Segurança da plataforma Xanadu

Última atualização: 19/11/2024

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Alguns exemplos e gráficos aqui representados são fornecidos somente para fins de ilustração.
Nenhuma associação ou conexão real com produtos ou serviços ServiceNow é intencional ou deve ser inferida.

ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países. Outros nomes de empresas e de produtos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Leia os Termos de Uso do Site do ServiceNow em www.servicenow.com/terms-of-use.html

Sede da empresa
2225 Lawson Lane
Santa Clara, CA 95054
Estados Unidos
(408) 501-8550

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países. Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

servicenow

Índice

Proteja sua instância 9
ServiceNow Vault 11
Segurança da plataforma 13
Security Center 14
Visão geral 16
Proteção de segurança 17
Security Scanner 23
Métricas de segurança 29
Ações do cliente 35
Práticas recomendadas de segurança 39
Aprendizado de segurança 46
Faixas de comunicados de segurança 46
Painéis de postura de segurança 47
Notificações de eventos de segurança 49
Central de segurança da instância 55
Migração da Central de segurança da instância para a ServiceNow Security Center 64
Monitorar eventos de segurança 67
Verificar a pontuação de conformidade diária e definir as configurações da propriedade de segurança 73
Verificar se há definições de segurança incorretas 83
Monitorar métricas de instância 84
Como ativar a interface do ISC Virtual Agent 97
Configurações de proteção de segurança da instância 98
Configurações de proteção 201
Linha de base das configurações de proteção 203
Controle de acesso 224
API e serviço Web 275
Arquitetura, design e modelagem de ameaças 290
Autenticação 300
Lógica de Negócios 329
Comunicação 332
Configuração 337
Proteção de dados 348
Manipulação de erros e registro em log 352
Arquivo e recursos 360
Código mal-intencionado 367
Gestão de sessões 369
Criptografia armazenada 384
Validação, limpeza e codificação 385

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países. Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Log de serviço de exportação (LES) 419
Funções Log de serviço de exportação 421
Origens de log 423
Criar uma configuração de fonte de log 423
Consumidor do Kafka 425
Consumidor do MID Server 429
Como revisar o relatório de logs 435
Logs 437
Logs do sistema 437
Registro em log, auditoria e erros 452
Gestão de segredos 453
Explorando a Gestão de segredos 453
Configurando segredos acessíveis ao cliente 458
Painel da Gestão de segredos 475
Assinatura de código 487
Explorando a assinatura de código 490
Configuração da assinatura de código 493
Usar a assinatura de código 515
Referência de assinatura de código 530
Varredura antivírus 536
Explorar a Varredura antivírus 537
Configuração do Varredura antivírus 539
Revisar arquivos em quarentena 540
Conhecer os atributos do Dicionário para Varredura antivírus 541
Limpador de HTML 542
Explorar o limpador de HTML 542
Configurar o limpador de HTML 545
Habilitar o limpador de HTML 546
Auditoria 548
Explorar a auditoria 548
Configurar auditoria para uma tabela 551
Visualizar tabelas de auditoria do sistema e de mudança de relacionamento de auditoria 553
Conhecer os conjuntos de históricos 555
Configurações de Alta Segurança 566
Explorar configurações de alta segurança 567
Configurar propriedade da área restrita de script 579
Ativar configurações de alta segurança 583
Rede virtual privada (VPN) 586
Explorar rede virtual privada (VPN) 586
Ativar um serviço VPN 589
Configurar um endereço para comunicação VPN 589

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Privacidade da plataforma 590
Privacidade de dados 590
Explorando a privacidade de dados 591
Domain separation e Privacidade de dados 592
Tipos de campos compatíveis para anonimização 593
Funções da Privacidade de dados 594
Privacidade de dados (Clássico) 595
Privacidade de dados 607
Descoberta de dados 612
Como explorar o Descoberta de dados 613
Como ativar o Descoberta de dados 615
Classificar dados na página de descobertas de Descoberta de dados 615
Trabalhos do Descoberta de dados 616
Funções Descoberta de dados 624
Resultados da tarefa do Descoberta de dados 626
Tipos de dados compatíveis com a Descoberta de dados 628
Como fazer verificações com a configuração granular 629
Data Classification 631
Explorando a classificação de dados 632
Instalando dados de demonstração do plug-in Data Classification 633
Criando classificações de dados 635
Atribuindo classificações de dados a entradas do dicionário 636
Análise das classificações de dados usando o painel de Visão geral 637
Domain Separation e Data Classification 639
Anonimização de dados 640
Criação de técnicas de anonimização 641
Criação de políticas de anonimização 644
Criação de trabalho de anonimização 648
Como ativar trabalhos paralelos para anonimização de dados 652
Criptografia 653
Estrutura de gestão de chaves 654
Pacote de assinatura do Gerenciamento de criptografia e chaves 655
Noções básicas sobre a estrutura de gerenciamento de chaves 656
Ações de gerenciamento de chave 688
Importação de uma chave do serviço web 691
Integridade do Key Management Framework 694
Preparação da sua instância para descontinuação de GlideEncrypter 696
Descontinuar o uso do GlideEncrypter do 3DES para campos Password2 697
Troca de recursos do Key Management Framework 700
Segurança de infraestrutura 708
Criptografia Password2 com o KMF (Key Management Framework, Estrutura de gestão de chaves) 710

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Certificados ... 713
Explorando certificados ... 714
Geração de certificado do cliente LDPA ... 715
Carregamento de certificados para uma instância ... 717
Criptografia em nível de coluna ... 719
Exploração da criptografia em nível de coluna ... 720
Configuração da criptografia em nível de coluna ... 723
Uso da Criptografia em nível de coluna ... 727
Criptografia em nível de coluna para empresas ... 756
Criptografia da nuvem com gerenciamento de chave ... 761
Operações de gerenciamento de chaves ... 763
Política de controle de quórum ... 771
Transações de gestão de chaves ... 776
Registro em log da Criptografia da nuvem ... 778
Detecção de adulteração ... 781
Criptografia completa de disco ... 784
Edge Encryption ... 784
Como explorar o Edge Encryption ... 785
Planejamento do Edge Encryption ... 798
Instalando o Edge Encryption ... 807
Atualizando o Edge Encryption ... 859
Configurando o Edge Encryption ... 867
Criptografia de banco de dados ... 925
Explorando a criptografia de banco de dados ... 925
Solicitar rotação de chaves do banco de dados ... 927
Criptografia de banco de dados com comutador controlado pelo cliente ... 928
Gestão de acessos ... 930
Zero Trust Access ... 931
Explorar o Zero Trust Access ... 932
Ativar Zero Trust Access ... 934
Configurar função de acesso à sessão ... 934
Propriedades do sistema de acesso Zero Trust ... 936
Tutorial: usar o acesso Zero Trust ... 938
Zero Trust Access para dispositivos móveis ... 943
Domain Separation para provedores de serviço ... 944
Explorando o Domain Separation ... 945
Compatibilidade de aplicações com o Domain Separation ... 964
Práticas recomendadas do Domain Separation para provedores de serviço ... 973
Suporte para Separação de domínios ... 1014
Configuração e administração do Domain Separation ... 1015
Central de Separação de domínios ... 1047
Autenticação ... 1055

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Autenticação adaptável....1056
Autenticação de API....1115
Política de acesso de API....1127
Autenticação baseada em certificados....1152
Associação de URLs personalizadas para sua instância....1160
Saídas de instalação....1168
Autenticação baseada no intervalo de IP....1170
Integração LDAP....1173
Limitar sessões simultâneas....1240
Autenticação local....1244
Autenticação multifator (MFA)....1269
Single Sign-on (SSO) de vários provedores....1319
Autenticação de entrada e saída do OAuth....1411
Registro automático na instância da ServiceNow....1451
Autenticação baseada em tokens (logins de usuários)....1462
Segurança de serviços da Web....1475
Regras da lista de controle de acesso....1480
Como explorar listas de controle de acesso....1480
Configuração de uma regra de ACL....1498
Contextual Security Manager....1504
Configuração de ACL avançada....1509
Atributos de segurança....1521
Fundamentos dos atributos de segurança....1521
Criar atributos de segurança....1522
Escopo dos Atributos de segurança....1524
Funções e restrições da consulta de campos....1525
Como configurar uma função de consulta de campo....1525
Como configurar restrições de consultas de campo....1526
Filtragem de dados....1526
Explorando a filtragem de dados....1527
Ativando filtragem de dados....1529
Criando regras de filtragem de dados....1530
Criando critérios de assunto....1533
Depuração de filtragem de dados....1537
Funções de segurança....1538
Funções explícitas....1538
Funções de privilégio elevado....1546
Conexões e credenciais....1549
Explorando credenciais, conexões e aliases....1549
Introdução às conexões....1565
Introdução às credenciais....1576
Algoritmos de autenticação....1662

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

ServiceNow® controle de acesso 1673
Explorar o controle de acesso do ServiceNow® 1674
Ativar o controle do acesso ao ServiceNow® 1677
Configurar o controle de acesso ao ServiceNow® 1679
Registro em log de Auditoria 1680
Identidade 1681
Análise de acessos 1681
Explorando o analisador de acesso 1682
Uso do Analisador de acesso 1683
Avaliação de permissão 1703
Perguntas frequentes 1705
Simulador de acesso 1711
Identidade global 1724
Explorando ID federado 1725
Acessando critérios de ID federado 1726
Atualização de campos de ID 1727
Central de identidade 1728
Explorando o Identity Center 1729
Ativando a Central de identidade 1729
Central de identidade para usuários 1730
Métricas de identidade para administradores 1733
Sistema de gerenciamento de usuários entre domínios (SCIM) 1733
Provedor de SCIM 1734
Cliente de SCIM 1752
Auditoria de identidade e acesso 1770
Explorar Auditoria de identidade e acesso 1771
Resultados da auditoria de identidade 1772
Campos auditáveis de segurança 1776
Campos compatíveis e não compatíveis com Auditoria de identidade e acesso 1780

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Proteja sua instância

A segurança da plataforma oferece recursos para proteger a instância.

ServiceNow Vault

Use o conjunto de produtos da ServiceNow Vault de ferramentas de segurança de dados que protegem informações confidenciais contra acesso não autorizado, corrupção ou roubo durante todo o seu ciclo de vida.

Segurança da plataforma

A segurança da plataforma oferece recursos para proteger a instância.

Privacidade da plataforma

A Privacidade da plataforma permite mascarar os dados confidenciais da instância.

Criptografia

Proteja seus dados confidenciais e mantenha a conformidade com os requisitos e padrões regulatórios.

Gestão de acesso

A Gestão de acesso permite que você acesse a instância da ServiceNow® com segurança.

Identidade

Saiba mais sobre as identidades na instância.

Assinatura de código

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A assinatura de código cria assinaturas digitais para que os dados que posteriormente serão verificados confirmem a autenticidade e a integridade dos dados.		

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

ServiceNow Vault

Use o conjunto de produtos da ServiceNow Vault de ferramentas de segurança de dados que protegem informações confidenciais contra acesso não autorizado, corrupção ou roubo durante todo o seu ciclo de vida. Aplique proteções como criptografia, gestão de segredos e privacidade de dados para a redação e a auditoria de informações confidenciais. A Página inicial do ServiceNow Vaultfornece um único local visível para encontrar e navegar até os produtos de segurança de dados do ServiceNow Vault.

ServiceNow Vault é um plug-in pago que a equipe da ServiceNow deve ativar em sua instância de produção. ServiceNow Vault inclui os componentes listados aqui.

Para adquirir uma assinatura, entre em contato com o seu gerente de contas ServiceNow. Quando você compra uma assinatura, determinados plug-ins são ativados automaticamente. Se um plug-in pago não for ativado automaticamente, você poderá ativá-lo manualmente na lista **Todas as aplicações** em sua instância.

Componentes do ServiceNow Vault

Criptografia

O Key Management and Criptografia em nível de coluna são um pacote de módulos de criptografia altamente configuráveis

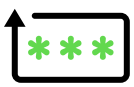
Gestão de segredos

Solução para substituir quaisquer segredos codificados, como senhas, certificados e chaves de API, na plataforma pela custódia dos segredos do cliente.

Assinatura de código

Ajude a melhorar a segurança validando scripts e dados de configuração de aplicação confidenciais antes que eles sejam usados.

Privacidade de dados



Use o plug-in Privacidade de dados para remover PII (personally identifiable information, informações de identificação pessoal) dos dados do usuário quando eles são migrados de uma instância de produção para uma instância de não produção.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países. Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Descoberta de dados

O plug-in Descoberta de dados permite localizar informações de identificação pessoal (PII) nos dados do usuário. Então, os dados podem ser classificados para medidas de segurança adicionais.

Logs

Melhore a segurança, o desempenho e a experiência do usuário importando dados de log do ServiceNow para a análise de log da empresa usando o serviço de exportação de log.

Zero Trust Access

O acesso à sessão da ServiceNow permite que as organizações reduzam dinamicamente o privilégio do usuário em uma sessão da Web

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países. Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Segurança da plataforma

A segurança da plataforma fornece recursos para proteger a instância.

Centro de segurança

Permita que os administradores mantenham continuamente o mais alto nível de postura de segurança e monitorem facilmente eventos e comportamentos inseguros.

Configurações de proteção

O conteúdo de configurações de proteção da Central de Segurança

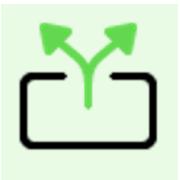
ServiceNow, Inc.

contém descrições detalhadas e valores de conformidade para as propriedades do sistema relacionadas à segurança e aos plug-ins em

Now Platform

. Você pode definir essas propriedades usando o app de configurações de proteção na Central de segurança.

Serviço de exportação de log

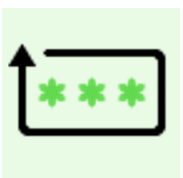


O LES (Log Export Service, Serviço de exportação de log) permite a exportação contínua dos logs de aplicação e sistema da sua instância para suas ferramentas de análise de segurança corporativa. O serviço oferece integração altamente escalonável e praticamente em tempo real com suas ferramentas de análise de fácil manutenção e configuração.

Logs

O módulo de Logs fornece uma variedade de logs que você pode usar para solucionar problemas e depurar transações e eventos que ocorrem na instância.

Gestão de segredos



Use a Gestão de segredos da ServiceNow para gerenciamento granular de acesso às suas senhas para atender às suas necessidades de negócio.

Assinatura de código

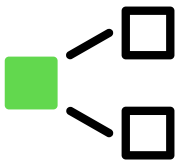
A assinatura de código cria assinaturas digitais para que os dados que posteriormente serão verificados confirmem a autenticidade e a integridade dos dados.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Capacidades de varredura antivírus

Use Varredura antivírus para ajudar a proteger sua instância contra infecções de vírus que podem ser introduzidas por anexos de arquivo aos registros do sistema, como incidentes, problemas e histórias.

Limpador de HTML

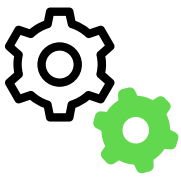


Remova o código indesejado e proteja-se contra problemas de segurança, como ataques de script entre sites, limpando a marcação HTML nos campos HTML e nos campos HTML traduzidos.

Auditoria

Rastreie mudanças de registro em tabelas habilitadas para auditoria. Por padrão, o sistema rastreia mudanças nas tabelas de incidentes, mudanças e problemas, entre outras.

Configurações de alta segurança



As Configurações de alta segurança se referem a várias opções de segurança disponíveis em sua instância.

Rede virtual privada (VPN)

Use uma VPN (virtual private network, rede virtual privada) para integrar sua instância com fontes de dados externas na Internet.

Outras configurações e recursos de segurança

Defina as propriedades de segurança fora da Central de segurança da instância, que também contém outros recursos relacionados à segurança.

Security Center

A ServiceNow Security Center é uma aplicação que consiste em um conjunto de ferramentas criadas para ajudar a sua organização a manter as suas implementações da ServiceNow seguras. Ao usar o Security Center, você pode melhorar sua postura de segurança e fortalecer seus níveis de conformidade, ao mesmo tempo que desfruta de uma experiência de usuário fluida.

A Central de segurança é uma aplicação gratuita que os administradores de sistema podem baixar na ServiceNow Store. Ele é instalado por padrão a partir da versão Vancouver. Ela também fica disponível na ServiceNow Store todos os trimestres, entre as versões da família, para facilitar a adoção mais rápida das novas funcionalidades.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Importante: A Central de segurança da instância (ISC) chegará ao fim das vendas em setembro de 2024. A SSC (ServiceNow Security Center, Central de segurança da ServiceNow) é a solução recomendada no futuro. Para obter mais informações, consulte Migração da Central de segurança da instância para a ServiceNow Security Center.

Página inicial Visualize sua pontuação de conformidade de proteção como uma porcentagem, analise as principais configurações de proteção não compatíveis que precisam de correção e veja os resultados das suas verificações de segurança.	**Proteção de segurança** Veja se as configurações de proteção estão em conformidade com as recomendações de segurança da ServiceNow	**Security Scanner** Faça uma varredura em um conjunto de verificações de segurança para identificar configurações incorretas e comportamento inseguro
Métricas de segurança Monitore mais de 50 métricas diferentes que ajudam a identificar possíveis ameaças à segurança.	**Antivírus** Exibe a tendência de quando os eventos ocorrem em arquivos potencialmente infectados.	**Aprendizado de segurança** Um repositório central de recursos de segurança que fornece acesso a documentos de segurança e conformidade da ServiceNow.

Funções de usuário

Para usar a Central de segurança, você deve ter a função de administrador ou sn_vsc.security_center_viewer.

Função necessária	Usuário	Benefícios
administrador	Essa função tem acesso a todos os recursos, funções e dados do sistema, já que os administradores podem substituir as regras de ACL (Access Control List, lista de controle de acesso) e	Utilize as ferramentas da Central de segurança para melhorar a postura de segurança da instância e monitorar os comportamentos relacionados à segurança.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Função necessária	Usuário	Benefícios
	ignorar todas as verificações de função. Evite atribuir esta função aos seus usuários quando houver funções mais específicas disponíveis.	
sn_vsc.security_center_viewer	Essa função permite que usuários não administradores acessem informações da Central de segurança, mas os impede de modificar as ferramentas da Central de segurança ou fazer mudanças na configuração da instância. Por exemplo, proprietários de plataforma, analistas de operações de segurança ou partes interessadas em conformidade podem precisar de acesso a determinados KPIs (Key Performance Indicators, principais indicadores de desempenho) de segurança, informações sobre segurança e materiais de aprendizado de segurança disponíveis na Central de segurança.	Obtenha visibilidade sobre as ferramentas da Central de segurança para monitorar a postura de segurança da instância e monitorar os comportamentos de segurança.

Iniciar

- Security Center está incluído em todas as versões da família a partir de Vancouver.
- Leia a documentação do produto, começando com a Visão geral.
- Conclua o curso TACO (Technical Training and Certification) da Central de segurança.

Visão geral

Obtenha um resumo rápido da postura de segurança da sua instância na página de visão geral. Exiba sua pontuação de conformidade de proteção como uma porcentagem, veja as tendências da sua pontuação de conformidade em gráficos, analise as principais configurações de proteção fora de conformidade que precisam de correção e acesse os resultados das suas verificações de segurança.

A pontuação de conformidade de proteção é uma porcentagem que representa o quanto suas configurações de segurança estão alinhadas com as configurações recomendadas. O resumo da pontuação de conformidade de proteção exibe essa porcentagem e dados a mudanças recentes na pontuação. Use o gráfico de tendência de pontuação de conformidade de proteção para ver como sua pontuação de conformidade mudou ao longo de um período de tempo.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Melhore sua pontuação de conformidade usando as principais configurações de proteção que estão fora de conformidade. Esta lista exibe as 10 configurações de proteção que mais afetam negativamente sua pontuação de conformidade de proteção. Essa visibilidade ajuda a priorizar quais configurações de proteção devem ser corrigidas.

A seção de resumo das varreduras de segurança exibe gráficos de barras que refletem o número de descobertas ao longo do tempo para cada uma das suas verificações de segurança.

1. Acesse o gráfico de tendências de pontuação da conformidade de proteção na página de visão geral ou navegando até **Proteção** > **Tendência de pontuação**.
2. Selecione o botão **Revisar tendência de pontuação** para personalizar o período de tempo e selecionar pontos de tendência para analisar.
3. Na seção de resumo da verificação de segurança, selecione uma barra para navegar até a página de resultados da verificação desse conjunto de verificação.

Proteção de segurança

Use a ferramenta de proteção da Central de Segurança para ver sua pontuação de conformidade de proteção, compará-la com pontuações anteriores e mudar as configurações para melhorar sua conformidade e postura de segurança.

A Configurações de proteção especifica valores recomendados para as propriedades e os plug-ins relacionados à segurança na NOW Platform. A ferramenta de proteção calcula a pontuação de conformidade da configuração de proteção como um percentual. Este número indica a conformidade da sua instância com as configurações de proteção da Central de Segurança.

A fórmula para calcular a pontuação de conformidade de proteção é a seguinte:

- Cada configuração de proteção tem uma pontuação de risco entre 0 e 10.
- A pontuação é igual à soma de todas as pontuações de risco em conformidade, dividida pela soma de todas as pontuações de risco.

Por exemplo, se a soma de todas as pontuações de risco em conformidade for 25,4 e o total de todas as pontuações de risco for 34,9, a pontuação de conformidade será (25,4 /34,9) × 100, o que equivale a 72,7. Este decimal é arredondado para o número inteiro mais próximo e, portanto, será igual a 73.

Este cálculo é realizado automaticamente no primeiro dia do mês ou após uma instalação ou reinstalação da Central de segurança ServiceNow.

Comparação da pontuação de proteção

Obtenha visibilidade da integridade das suas configurações de proteção e use esses dados para melhorar a postura de segurança de sua instância.

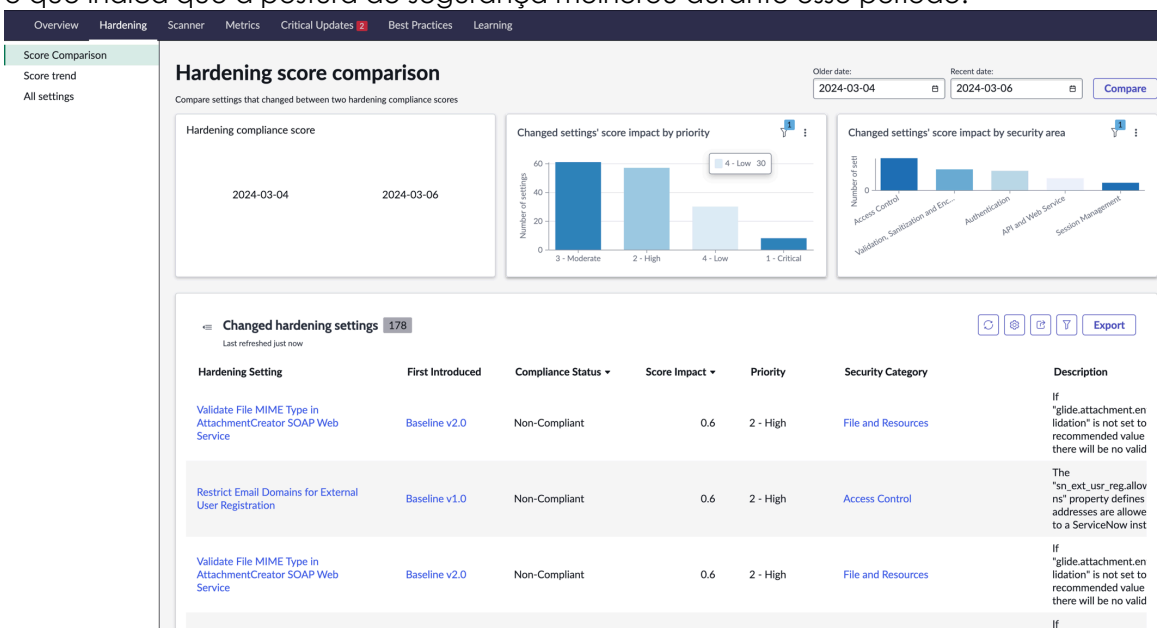
A página de comparação de pontuação de proteção exibe todas as configurações de proteção com mudanças no status de conformidade entre a primeira e a segunda datas e como elas afetaram a pontuação de conformidade de proteção. Por exemplo, se uma configuração mudasse de conforme para não conforme, a pontuação teria diminuído.

Para visualizar os resultados dessas mudanças, insira uma data mais Antiga e uma data Recente no seletor de datas no canto superior direito da página e clique em "Comparar". Veja a seguir está uma explicação de cada cartão:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países. Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Pontuação de conformidade de proteção: exibe a pontuação de conformidade da sua instância como uma porcentagem na primeira e na segunda data selecionadas por você.
- Impacto da pontuação das configurações alteradas por prioridade: mostra o número de configurações de proteção que mudaram seu status de conformidade entre as duas datas, organizadas por valor de prioridade.
- Impacto da pontuação das configurações alteradas por área de segurança: mostra o número de configurações de proteção que mudaram o status de conformidade entre as duas datas, organizadas pela área de segurança.
- Configurações de proteção alteradas: mostra a lista de configurações de proteção que mudaram os status de conformidade entre as duas datas. Você pode revisar as configurações que se tornaram não conformes e diminuíram sua pontuação de comparação de proteção para oportunidades para torná-las conformes e aumentar sua pontuação. Consulte Aumente a pontuação de conformidade de proteção.

Por exemplo, na captura de tela a seguir, a pontuação de conformidade aumentou, o que indica que a postura de segurança melhorou durante esse período.



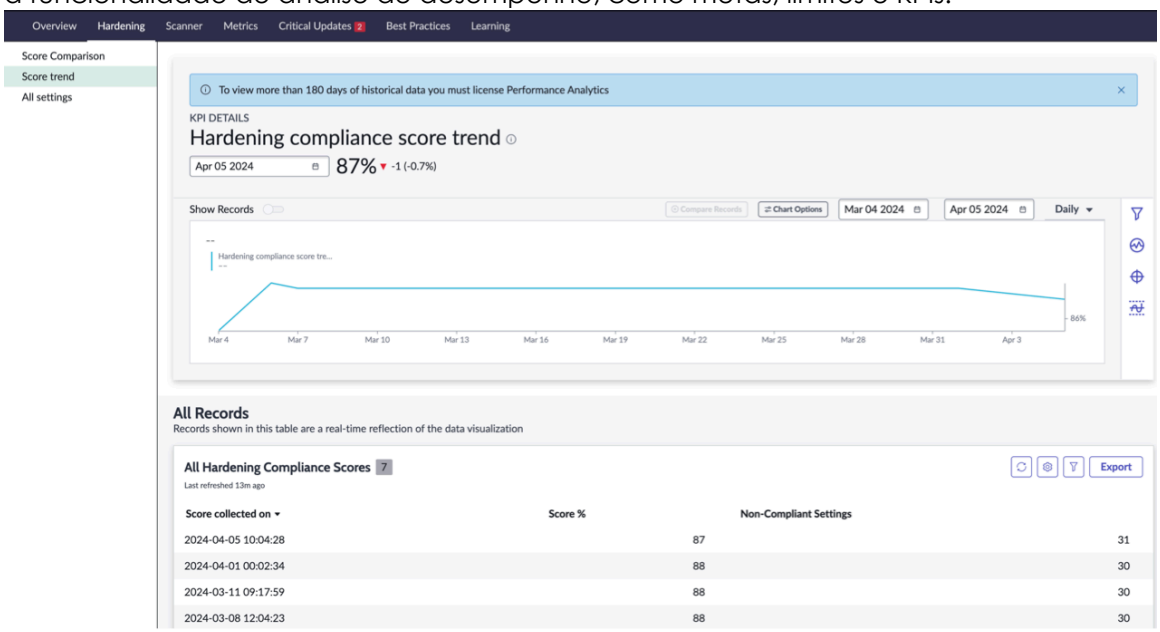
Tendência da pontuação de conformidade de proteção

Visualize as tendências da pontuação de conformidade de proteção em um gráfico ou tabela ao longo de um período de tempo.

Veja as tendências da sua pontuação de conformidade ao longo de um período de tempo. Use o seletor de data para selecionar um período de tempo para análise e obtenha informações mais detalhadas sobre os dados usando

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a funcionalidade de análise de desempenho, como metas, limites e KPIs.



Opções de gráfico: selecione **Opções de gráfico** para executar análises, exibir as séries temporais e exibir os dados em vários tipos de gráficos.

Análise

- Meta: objetivos que sua organização deseja alcançar. Consulte Performance Analytics metas.
- Limite: define um intervalo normal de pontuações para um indicador e alerta quando determinados eventos ocorrem. Consulte Performance Analytics limites.
- Previsão: descreve a capacidade de prever pontuações futuras com base no comportamento passado. Consulte Previsões de pontuações do Performance Analytics.
- Tendência: mostra como o valor de um ou mais itens muda ao longo do tempo.
- Anotações: exibe anotações em pontos de dados individuais.
- Rótulos: exibe pontuações relacionadas a visualizações.
- Estatísticas: exibe estatísticas relacionadas à sua pontuação de conformidade.

Série de tempo

- Pontuação: pontuação dos KPIs.
- Mudança: mudança da pontuações deste indicador.
- Mudança de porcentagem: porcentagem de mudança de pontuações.

Tipo de gráfico: veja Casos de uso do tipo de visualização da série temporal.

Tabela Todos os registros

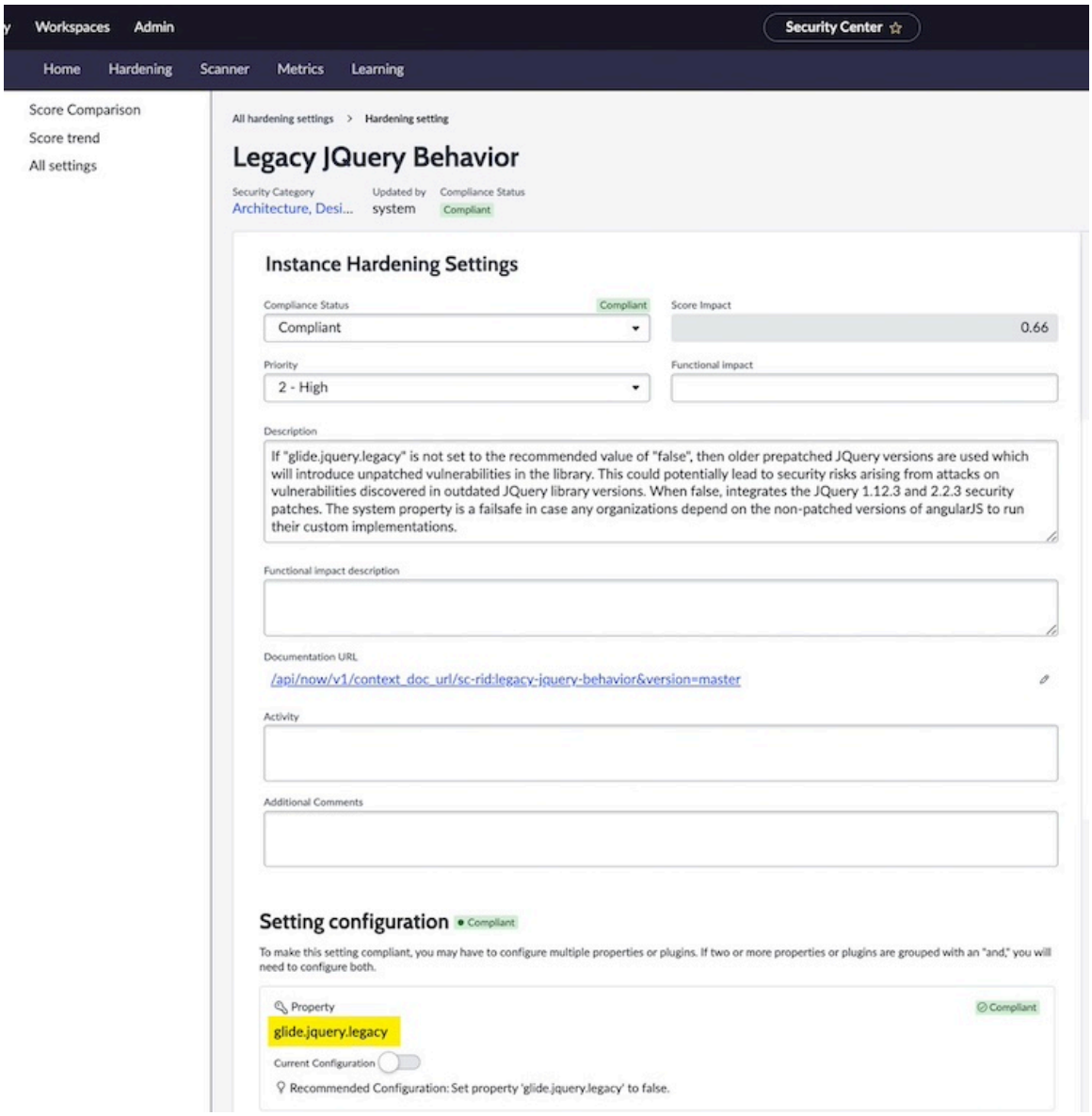
A tabela Todos os registros exibe a data em que as pontuações de conformidade foram coletadas, as porcentagens de pontuação e o número de configurações fora de conformidade. Você pode usar esta tabela como outra opção para analisar a postura de segurança da sua instância ao longo do tempo .

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Detalhes da configuração de proteção

Analise os detalhes de uma configuração de proteção selecionando o link dela na aplicação Central de segurança.

Navegue até **Proteção** > **Todas as configurações** e selecione uma configuração de proteção a ser redirecionada para uma página na ferramenta de configuração de proteção que exibe informações relacionadas à segurança.



Detalhes da configuração das configurações de proteção

Atributo da configuração	Descrição
Status de conformidade	Indica se a configuração de proteção é compatível ou não.
Impacto da pontuação	Percentual que indica quanto essa configuração de proteção afeta sua postura de segurança.
Prioridade	Um número no intervalo de 1 a 4, com 1 tendo o maior peso, que indica a força

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Detalhes da configuração das configurações de proteção

Atributo da configuração	Descrição
	do impacto que essa configuração de proteção tem sobre sua postura de segurança.
Impacto funcional	O impacto desta configuração de proteção sobre a operação da sua instância.
Descrição	Uma visão geral sobre a configuração de proteção.
URL da documentação	Link para a documentação da configuração de proteção.
Atividade	Notificações de atualizações relacionadas à configuração de proteção.
Definição de configuração	Detalhes relacionados ao status de conformidade da sua configuração de proteção junto com instruções sobre como torná-los compatíveis. **Nota:** Algumas configurações de proteção podem exigir que você configure várias propriedades e plug-ins para torná-los compatíveis.

Aumente a pontuação de conformidade de proteção

Aumente sua pontuação de conformidade de proteção garantindo que as configurações de proteção estejam em conformidade com as recomendações do sistema.

Antes de Iniciar

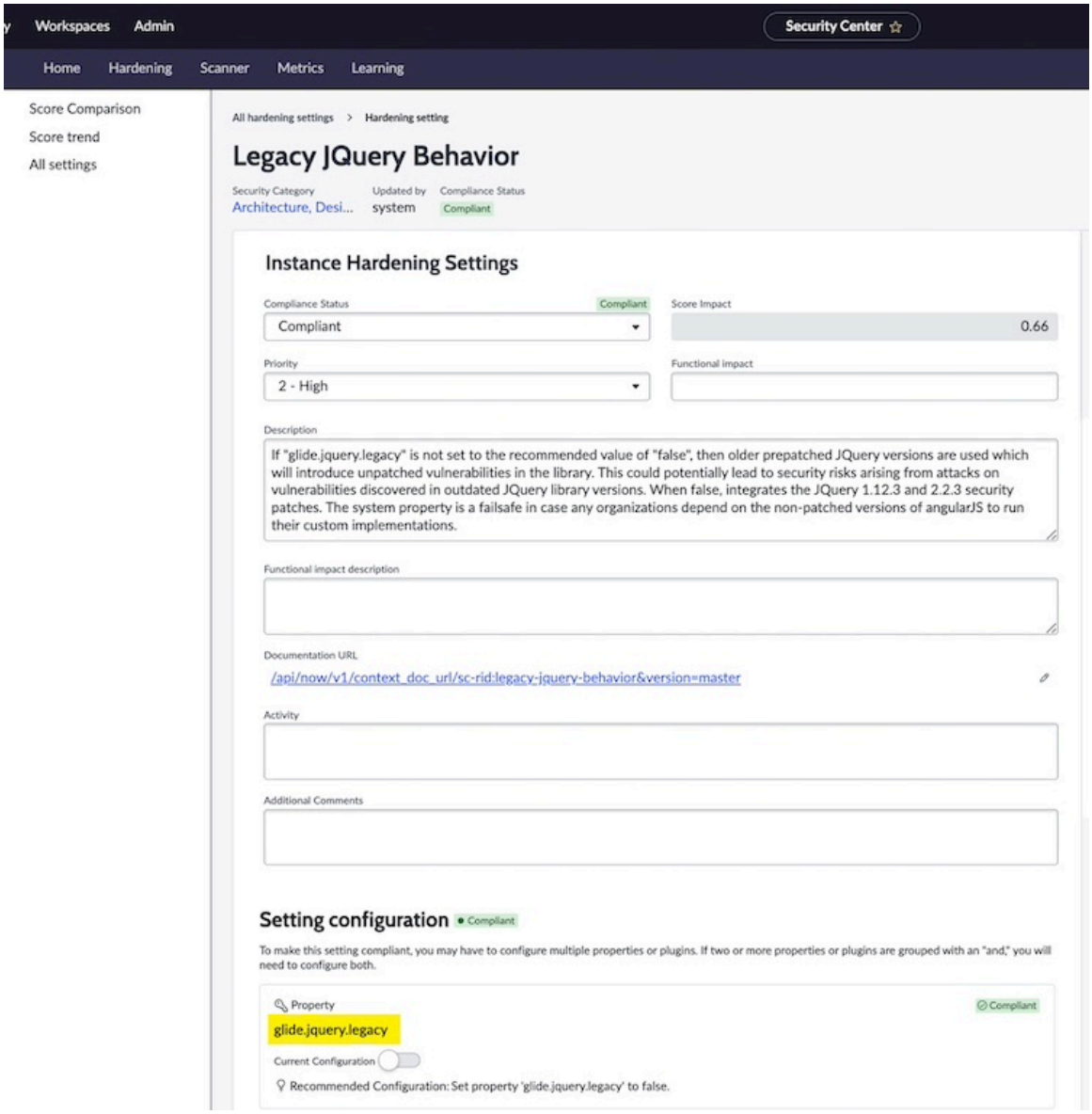
Função necessária: administrador

Identifique configurações de proteção fora de conformidade com o maior impacto de pontuação em sua instância. Revise-as para ver se você cumpre as recomendações do sistema e aumentar sua pontuação geral de conformidade.

Procedimento

1. Navegue para **Proteção** > **Todas as configurações**.
2. Filtre a coluna Status de conformidade para visualizar apenas configurações de proteção não compatíveis.
3. Selecione **Impacto da pontuação** para classificar do maior para o menor.
4. Selecione as configurações e revise os detalhes da configuração para decidir se deseja cumprir as recomendações.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Coloque a configuração de proteção em conformidade.
6. Se você atualizar uma pontuação de proteção fora de conformidade para torná-la compatível, vá para a Página inicial e selecione **Atualizar pontuação** para exibir a pontuação mais atualizada.
   A pontuação de proteção é arredondada para cima. Uma pontuação de 86,75% será arredondada para 87.

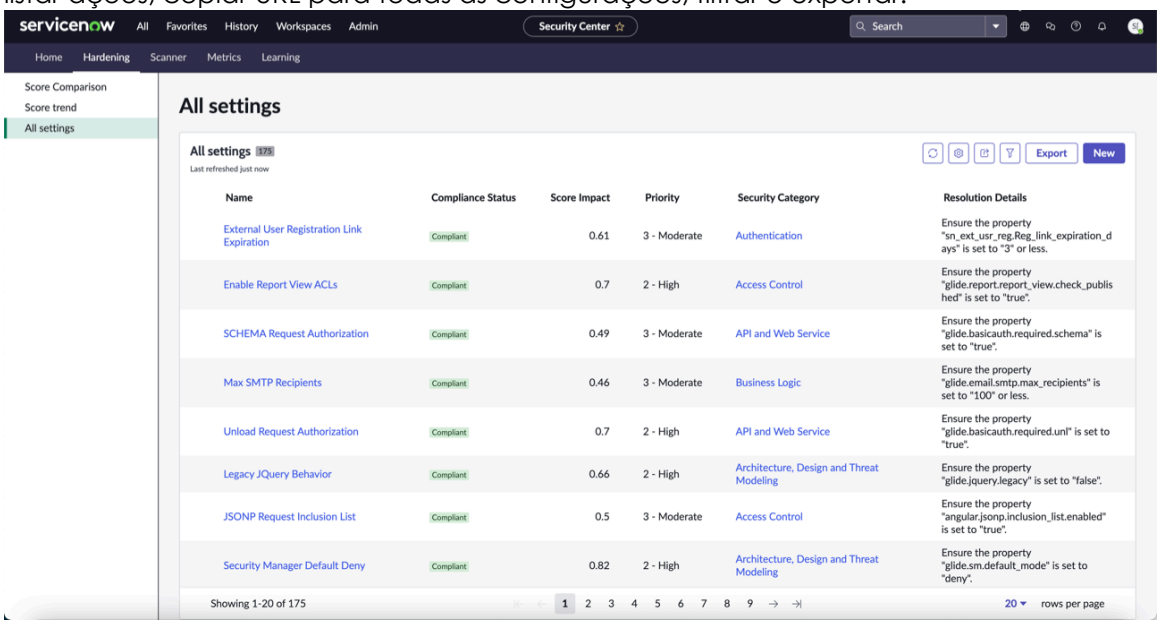
Todas as configurações

Exiba todas as configurações de proteção disponíveis na sua instância a partir de uma única página.

Uma tabela que exibe todas as configurações de proteção disponíveis na sua instância. Você pode aplicar as operações comuns de uma tabela selecionando ícones no canto superior direito da tabela: Atualizar lista,

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

listar ações, copiar URL para todas as configurações, filtrar e exportar.



- **Nome**: o nome da configuração de proteção da propriedade.
- **Status de conformidade**: **em conformidade** indica que a configuração de proteção está definida corretamente; **fora de conformidade** indica que a configuração de proteção da propriedade não está definida de acordo com a recomendação do sistema.
- **Impacto da pontuação**: valor percentual que corresponde ao impacto que esta configuração de proteção tem sobre a sua postura de segurança. Todos os impactos de pontuação somam 100%.
- **Prioridade**: valor que representa o nível de criticidade da configuração: Extrema, Alta, Moderada e Baixa. A relação entre o impacto da pontuação e a prioridade é que um impacto de pontuação mais alto indica um nível de criticidade mais elevado.
- **Categoria de segurança**: é a categoria de segurança da propriedade.
- **Detalhes da resolução**: etapas que você deve executar para corrigir a vulnerabilidade de segurança da configuração de proteção em questão.

Para saber como definir uma configuração de proteção de propriedade, consulte Aumente a pontuação de conformidade de proteção.

Security Scanner

Use a ferramenta para verificar sua instância em um conjunto de critérios de segurança para identificar configurações incorretas. A ferramenta simplifica o processo de criação de diferentes pacotes de verificação para diferentes casos de uso para que você possa analisar os resultados ao longo do tempo.

A varredura de segurança é um método para investigar sua instância em busca de configurações que indiquem problemas de integridade de segurança. Isso permite que você identifique oportunidades para implementar recomendações de segurança para sua organização.

Ao acessar a ferramenta de verificação, não haverá uma comparação disponível até que você selecione o pacote a ser comparado e pelo menos outros dois resultados de varreduras do pacote. Você pode usar o pacote e as verificações padrão ou pode criar suas próprias verificações e pacotes personalizados.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Comparação da pontuação de proteção

Alcance o controle da integridade das suas configurações de proteção e use esses dados para corrigir ameaças de segurança e melhorar a postura de segurança de sua instância.

A página de comparação de pontuação de proteção exibe as mudanças de segurança nas configurações de proteção entre a primeira e a segunda data. Para visualizar essas mudanças, insira uma data mais **Antiga** e uma data **Recente** no seletor de datas no canto superior direito da página e clique em **"Comparar"**. Abaixo você encontra uma explicação de cada cartão:

- **Pontuação de conformidade de proteção**: exibe a pontuação de conformidade da sua instância como uma porcentagem na primeira e na segunda data.
- **Pontuação do impacto das alterações das configurações por prioridade**: exibe o número de configurações que alteraram as prioridades.
- **Pontuação do impacto das alterações das configurações por área de segurança**: exibe o número de configurações que alteraram as prioridades. Por exemplo, passando de **Controle de acesso** para **Proteção de dados**.
- **Configurações de proteção alteradas**: exibe uma visualização consolidada das configurações que foram alteradas junto dos dados de segurança associados na lista. Além disso, pode aplicar funcionalidades comuns associadas a listas, como atualizar, listar ações de IU, copiar URL, filtros e exportar.

Por exemplo, na captura de tela a seguir, a pontuação de conformidade mudou de 71% para 73%, indicando que a postura de segurança melhorou durante esse período.

Foram quatro as configurações que alteraram a prioridade: duas altas e duas moderadas. Além disso, o número de configurações que alteraram a segurança foram quatro: duas de controle de acesso, uma de autenticação e uma de lógica de negócios. Os detalhes de segurança dessas quatro configurações também são exibidos na lista Configurações de proteção alteradas. Você pode exibir as configurações que não estão em conformidade e corrigi-las, o que recalculará a pontuação de conformidade de proteção.

Verificações do Security Scanner

Verificações são regras projetadas para detectar anomalias em uma instância e são executadas em tabelas, registros ou metadados.

É possível usar quatro tipos de verificações com a ferramenta scanner para identificar problemas e implementar recomendações de segurança para sua organização: verificações de tabela, verificações de tipo de coluna, verificações somente de script e verificações de linter.

Tipos de verificações

Nome da verificação	Descrição
Verificações de tabela	Use-a quando você souber as tabelas e as verificações específicas que deseja testar.
Verificações de coluna	Use-a para implementar a regra que você criou para fazer a iteração de todos os registros correspondentes ao tipo de campo da coluna de destino.
Verificações de script	Use-a para verificar metadados e configurações e executar verificações

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tipos de verificações

Nome da verificação	Descrição
	complexas escrevendo suas próprias verificações.
Verificações de linter	Use-a para identificar quaisquer problemas em um script. Quando há a execução de uma verificação de linter em um registro, é gerada uma árvore de sintaxe abstrata para o código dela. É possível usar essa árvore para analisar problemas com o código.

Criação de um novo pacote

Crie e programe um pacote personalizado para que você possa analisar a segurança da sua instância da sua organização.

Antes de Iniciar

Função necessária: administrador ou sn_vsc.security_center_viewer.

Um pacote é uma conjunto de verificações que podem ser usadas para uma varredura. Veja uma lista dos pacotes de verificação disponíveis em sua instância organizados em uma tabela, navegando até **"Varredura"** > **"Pacotes"**. Você pode criar seus próprios pacotes ou usar o pacote padrão, Auditor: esse é um pacote padrão pronto para uso que contém verificações de práticas de segurança recomendadas. Essas verificações consistem em propriedades do sistema, plug-ins e tabelas que podem afetar a postura de segurança da sua instância. As etapas a seguir mostram como criar um pacote e as várias opções disponíveis para configurá-los.

Procedimento

1. Navegue até **"Pacotes"** > **"Novo"**.
2. Dê um **nome** e uma **descrição** para o pacote e selecione **"Salvar"**.
3. **Verificações**
   É nesta etapa que você pode adicionar verificações ao seu pacote.
   a. Selecione **Editar**.
   b. Selecione as verificações que você deseja adicionar e clique em "Adicionar" (**>**) para colocá-las em seu pacote.
   c. **"Salvar"**.
4. **Pacotes secundários**
   É aqui que você adiciona pacotes secundários ou os pacotes que são colocados nos pacotes primários.
   a. Selecione **Editar**.
   b. Selecione os pacotes secundários que você deseja adicionar e clique em "Adicionar" (**>**) para colocá-los em seu pacote secundário.
   c. **"Salvar"**.
5. **Pacotes Primários**
   Aqui você deve adicionar os pacotes primários. Todos os pacotes secundários são executados quando um pacote primário é usado em uma varredura.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Selecione **Editar**.

b. Selecione os pacotes secundários que você deseja adicionar e clique em "Adicionar" (**>**) para colocá-los em seu pacote primário.

c. "Salvar".

6. Programação
Defina um horário para a execução do seu pacote.

a. Selecione **Novo**.

b. Insira os detalhes da varredura programada.
Os campos de hora estão no formato: hora:minutos:segundos.

c. "Salvar".

Como clonar o pacote de auditor de controles de acesso

Clone e personalize o pacote padrão de auditor de controles de acesso em sua instância para criar um pacote adaptado às práticas de segurança da sua organização.

Antes de Iniciar

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

Não é possível modificar o pacote padrão de auditor de controles de acesso fornecido com sua instância. No entanto, se você quiser adicionar, remover ou editar verificações para alinhá-las às práticas de segurança da sua organização, poderá duplicar os pacotes de auditor de controles de acesso. A cópia desses pacotes permite que você os personalize e crie um pacote com base no padrão. Os pacotes de auditor de controles de acesso incluem verificações relacionadas às práticas recomendadas de segurança, abrangendo propriedades do sistema, plug-ins e tabelas que afetam a postura de segurança da instância. As etapas abaixo demonstram como duplicar os pacotes padrão de auditor de controles de acesso para adaptá-los aos requisitos da sua organização.

Procedimento

1. Navegue até **"Todos"** > **"Verificação de instância"** > **"Pacotes"**.

2. Selecione **Novo** e digite um nome para seu pacote, junto com uma descrição opcional.

3. Clique com o botão direito no cabeçalho do formulário e selecione **Salvar**.

4. Adicione as verificações necessárias para sua análise.

a. Na guia **Verificações**, selecione **editar**.

b. Adicione as condições.
Por exemplo, para adicionar verificações de análise, aplique os seguintes campos, operadores, valores e condições:

[Campo][é][segurança] E [Aplicação][é][Global]

Para este exemplo, o resultado deve ser parecido com este: `Categoria é segurança e Aplicação é global`.

5. Selecione **executar filtro**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

6. Selecione as verificações de análise que você deseja adicionar da lista de coleções à check-list e selecione o botão de adição (>).
7. Selecione **salvar**.
   O pacote com as verificações personalizadas adicionadas foi criado.
8. Selecione **Executar verificação de pacote**.

Como exibir o pacote de auditor de controles de acesso

Veja as verificações disponíveis nos Pacotes padrão de auditor de controles de acesso para entender quais verificações são executadas quando esse pacote é executado.

Por Que e Quando Desempenhar Esta Tarefa

As etapas que você precisa concluir para acessar os pacotes padrão de auditor de controles de acesso em sua instância da ServiceNow.

Procedimento

1. Navegue até o pacote de auditor de controles de acesso selecionando **Scanner** > **Pacotes** > **Auditor de controles de acesso** (pacote). Em seguida, para revisar as verificações do pacote, selecione a guia **Verificações**.
   Você deve ver a lista de oito verificações disponíveis para o pacote.
2. Selecione o nome de uma verificação que você deseja analisar.
3. Analise os campos associados à verificação.

Nome	Descrição
Nome	Nome da verificação.
Aplicação	A aplicação à qual a verificação pertence (Central de segurança).
Categoria	Categoria associada à verificação.
Prioridade	O nível de urgência.
Versão	Número de versão da verificação.
Ativo	O status da verificação, por exemplo, ativa ou inativa.
Descrição resumida	Um breve resumo da verificação.
Descrição	Um resumo mais abrangente da verificação.
Detalhes das Resoluções	Possíveis incidentes de segurança mitigados.
URL da Documentação	Links para a documentação relacionada na documentação do produto ou em artigos da KB (Knowledge Base, Base de conhecimento).
Condição para execução	Condições que acionam o início das verificações.
Tabela	A tabela à qual a verificação pertence.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome	Descrição
Condições	Lógica condicional aplicada às verificações.
Avançado	Opções avançadas de configuração.

Resultados da varredura

Veja dados relacionados aos resultados da verificação em uma só exibição.

O resultado de uma verificação informa o status e o tipo da verificação. Também é possível ver todas as verificações executadas como parte da verificação e todas as outras informações relacionadas à verificação, como erros e logs. Selecione **Resultados** para navegar até o painel **Resultados da verificação**. Os resultados da verificação são listados na coluna **Resultado**. Clique em um resultado para aprofundar-se e exibir os detalhes:

- **Descobertas da verificação**: mostra todas as descobertas encontradas durante a execução das verificações.
- **Pacotes**: mostra todos os pacotes executados como parte da verificação.
- **Verificações**: mostra todas as verificações executadas como parte da verificação.
- **Falhas:** mostra todas as verificações que falharam durante a execução da verificação. Também mostra o motivo da falha na forma de uma mensagem de erro.
- **Log de verificação**: mostra as mensagens encontradas durante toda a verificação.
- **Estatísticas de varredura**: mostra as estatísticas relacionadas à verificação.
- **Destino**: mostra todos os destinos nos quais as verificações foram executadas.

Descobertas da varredura

Uma descoberta é uma referência a um registro que violou uma regra de uma verificação da instância. Você pode encontrar o registro de origem e o número de vezes que o registro acionou as regras de uma determinada verificação.

Navegue até **Descobertas** para exibir uma lista de descobertas de verificação da sua instância. Selecione um link na coluna **Criadas** para fazer uma busca detalhada e exibir os detalhes granulares relacionados a uma descoberta:

- **Verificação**: lista de verificações associadas à verificação.
- **Categoria**: categoria de segurança associada à verificação. Por exemplo, controle de acesso ou código malicioso.
- **Quantidade**: número de vezes que o registro violou as regras de verificação.
- **Prioridade**: severidade do risco de segurança (sendo 1 a prioridade mais alta e 4 a mais baixa).
- **Resultado**: o status e o tipo da verificação.
- **Versão da verificação**: versão da mudança da verificação.
- **Tabela de origem**: registro que violou uma regra da verificação.
- **Motivo do silenciamento**: motivo que levou ao silenciamento da descoberta.
- **Origem**: data em que a descoberta foi criada.
- **Tarefa**: usada para facilitar a atribuição de tarefas a partir da descoberta de um registro.
- **Domínio**: define o que você pode e não pode acessar.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- **Descrição resumida**: breve explicação da verificação.
- **Detalhes da resolução**: instruções sobre como resolver os problemas de verificação.

Métricas de segurança

Use a ferramenta Métricas para monitorar mais de 50 métricas de segurança diferentes para identificar possíveis ameaças à segurança ou comportamentos inseguros. Você pode definir limites para notificações por e-mail, visualizar e analisar os dados de várias formas, exportar os dados ou criar painéis com as métricas mais importantes para sua organização.

As métricas são implementadas como visualizações do Hub de análise que habilitam um conjunto avançado de recursos, incluindo o envio de alertas por e-mail quando os limites são excedidos, a visualização de metas e a exibição e filtragem de eventos subjacentes.

Meu painel de métricas de segurança

Exiba as métricas de segurança da sua instância em um único painel.

Para navegar até a página Métricas, selecione **Minhas métricas**. Esta página exibe o painel padrão, mas você também pode criar seu próprio painel selecionando **Editar**.

Você pode personalizar seu próprio painel adicionando visualizações, filtros, títulos, imagens, rich text e listas. Para saber mais sobre as diversas maneiras de personalizar seu painel, consulte Painéis no Análise da plataforma.

Como configurar métricas de segurança para enviar e-mails quando os limites forem acionados

Saiba como configurar métricas de segurança para que sua instância gere uma notificação por e-mail quando um limite for acionado.

Antes de Iniciar
Função necessária: administrador

Procedimento

1. Na Central de segurança, navegue até **métricas**.
2. Selecione uma métrica para a qual você deseja definir um limite em sua organização.

   Example
   Se você quiser gerenciar logins com falha, convém definir um limite para que, quando os logins com falha atingirem um número específico, os administradores ou os especialistas em segurança da organização recebam uma notificação. A métrica de segurança adequada nesse caso é **usuários** > **logins com falha**.
3. Selecione o ícone **Limites**.
4. Selecione o ícone **adição (+)** no painel de limites para configurar o formulário.
   As opções disponíveis são definir a visibilidade, o tipo de limite e o valor do limite.

   a. Para obter a visibilidade, selecione **para todos** se você quiser que todos recebam a notificação ou **para mim** se somente você quiser receber uma notificação.

   b. No tipo de limite, selecione **alta histórica**.
   Esse é o campo que aciona a notificação de limite.

   Nota: Somente é necessário inserir um valor de limite quando o **Tipo de limite** for definido como **Menor que** ou **Maior que**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Selecione **salvar** para criar o limite.
   Em seguida, é necessário configurar a notificação.
6. Selecione **todos** e insira a **notificação do sistema**.
7. Navegue até **e-mail** > **notificações**.
8. Na coluna **nome**, insira `*pa thre`.
   As notificações de limite se baseiam em eventos e são configuradas na tabela "Notificação de limites do PA".
9. Selecione **Notificação de limites do PA**.
   Há três guias nos resultados:
   - Quando enviar: especifica o que deve ocorrer para enviar a notificação por e-mail. Neste exemplo, o e-mail é acionado quando o limite que você definiu anteriormente é atingido.
   - Quem receberá: especifica quais usuários receberão a notificação. É possível adicionar usuários e grupos.
   - O que conterá: especifica a ação do script que um usuário pode modificar para personalizar a mensagem que os usuários e o grupo receberão. Para saber mais sobre como criar ações de script, consulte Ações de script.

Como personalizar o painel de métricas de segurança

Descubra a flexibilidade do painel de métricas de segurança, que pode ser personalizado com métricas de várias fontes, como gráficos e tabelas. Adapte o painel para atender aos requisitos específicos da sua organização.

Antes de Iniciar

Para personalizar o painel de métricas de segurança, verifique se você está no escopo da aplicação Central de segurança. Para alternar para esse escopo, selecione o **seletor de aplicações** > **Escopo da aplicação** e digite "central de segurança".

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

Implemente e personalize métricas de segurança usando o painel da Central de segurança. Adicione métricas e conteúdo ao seu painel a partir de várias fontes, como gráficos e diagramas gerados de um relatório. Aprenda as etapas necessárias para adicionar uma guia ao painel de métricas de segurança e, assim, poder personalizá-lo para atender às necessidades da sua organização.

Procedimento

1. No app Central de segurança, navegue até o painel de métricas de segurança selecionando **métricas**.
2. Entre no modo de edição selecionando **editar**.
3. Crie uma guia selecionando **+Adicionar uma guia**.

   Nota: Também é possível adicionar uma nova guia selecionando o ícone de **adição (+)** ao lado de uma guia existente.

4. Edite o título da guia recém-criada selecionando o ícone de lápis e digitando um nome.
5. Adicione um elemento à sua guia selecionando **adicionar um novo elemento**.
6. Selecione **Salvar**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

7. Opcional: Para compartilhar o painel com usuários, grupos e funções da sua organização, selecione o **menu Mais ações** > **Compartilhar**.
   a. Digite o nome de um usuário ao qual deseja conceder acesso.
   b. Selecione **confirmar**.

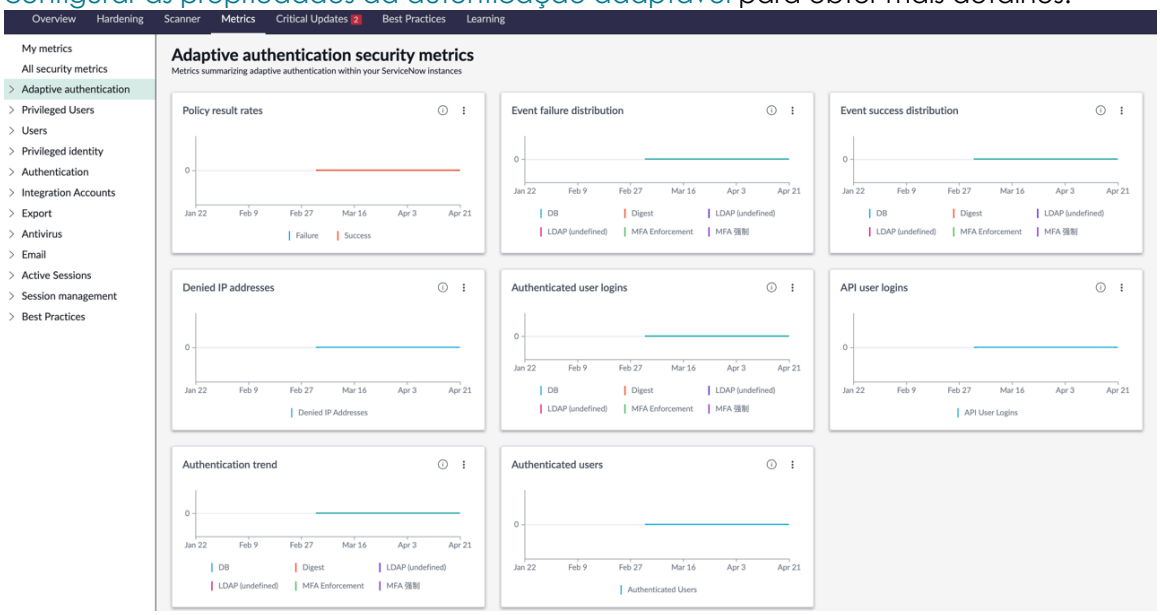
Todas as métricas de segurança

Navegue até **Todas as métricas de segurança** para exibir uma tabela com os dados relacionados às métricas de segurança da sua instância.

Métricas de segurança de autenticação adaptável

Use políticas de autenticação para avaliar as solicitações de autenticação e negar ou permitir o acesso à sua instância com base nas condições de política especificadas.

As métricas de autenticação adaptáveis permitem monitorar como a autenticação adaptável está sendo usada em sua instância. Você tem a opção de exibir um resumo de todas as suas métricas na autenticação adaptável ou pode detalhar e exibir métricas individuais, como taxas de resultado de política ou endereços IP negados. Esta página requer que o plug-in Adaptive Authentication (*com.snc.adaptive_authentication*) para autenticação adaptável esteja disponível em sua instância. Você também precisará habilitar a Política de autenticação para ver as métricas. Consulte Como ativar a autenticação adaptável e Como configurar as propriedades da autenticação adaptável para obter mais detalhes.



Nota: Este recurso foi lançado com a versão 1.2.

- Taxas de resultado de política: todos os eventos de autenticação adaptável bem-sucedidos e com falha.
- Distribuição de falha de eventos: todos os eventos com falha para cada tipo de evento.
- Distribuição de sucesso de eventos: os eventos bem-sucedidos associados a cada tipo de evento.
- Endereços IP negados: o número de endereços IP bloqueados pela instância, junto com os dados associados.
- Logins de usuários autenticados: o número de eventos contados para cada tipo de evento, excluindo o evento de pré-login.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Logins de usuários da API: o número de eventos associados às políticas de autenticação da API para cada tipo de evento.
- Tendência de autenticação: o número total de eventos registrados.
- Usuários autenticados: o número de usuários contados para cada tipo de evento, excluindo o evento de pré-login.

Usuários privilegiados

Exiba a linha de tendência dos usuários privilegiados (ativos e inativos) e suas atividades na Now Platform.

A seção de visão geral de Usuários privilegiados exibe a linha de tendência do total de usuários (ativos e inativos) e suas atividades em Now Platform. Usuários privilegiados são usuários aos quais foram atribuídas funções adicionais por administradores para acessar recursos como Configurações de alta segurança, Importação e Usuários do portal.

Abaixo você encontra uma explicação sobre usuários privilegiados:

- Total de usuários: a contagem total de usuários em sua instância.
- Usuários ativos: número total de usuários que iniciaram sessões em sua instância.
- Usuários inativos: usuários que não fizeram login recentemente em sua instância.
- Usuários inativos que não estão bloqueados: usuários que não fizeram login recentemente, mas que ainda têm acesso à conta.
- Usuários bloqueados: usuários que não têm permissão para autenticar em suas contas.
- Novos usuários: usuários que foram adicionados recentemente à sua instância.
- Logins bem-sucedidos: usuários que fizeram login.
- Logins com falha: tentativas de login malsucedidas.
- Logins locais não protegidos pela MFA: usuários que fizeram login sem MFA.
- Usuários que nunca fizeram login: usuários que nunca fizeram login em sua instância.
- Usuários que não fizeram login desde o mês passado: usuários que não fizeram login nos últimos 30 dias.
- Usuários que não fizeram login por 6 meses: usuários que não fizeram login nos últimos 6 meses.
- Usuários que não fizeram login há um ano: usuários que não fizeram login no último ano.
- Precisam redefinir a senha: usuários que precisam redefinir a senha.
- Falhas de redefinição de senha dos usuários: número de falhas de senha por usuário.

Usuários

Exiba a linha de tendência do total de usuários (ativos e inativos) e suas atividades em Now Platform.

A seção de visão geral de Usuários exibe a linha de tendência do total de usuários (ativos e inativos) e suas atividades em Now Platform.

Abaixo você encontra uma explicação sobre os tipos de usuários:

- Total de usuários: a contagem total de usuários em sua instância.
- Usuários ativos: número total de usuários que iniciaram sessões em sua instância.
- Usuários inativos: usuários que não fizeram login recentemente em sua instância.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Usuários inativos que não estão bloqueados: usuários que não fizeram login recentemente, mas que ainda têm acesso à conta.
- Novos usuários: usuários que foram adicionados recentemente à sua instância.
- Logins bem-sucedidos: usuários que fizeram login.
- Logins com falha: tentativas de login malsucedidas.
- Logins externos: autenticações que usam aplicações de terceiros.
- Logins locais não protegidos pela MFA: logins que não utilizam MFA.
- Usuários que não fizeram login desde o mês passado: usuários que não fizeram login nos últimos 30 dias.
- Usuários que não fizeram login por 6 meses: usuários que não fizeram login nos últimos 6 meses.
- Usuários que não fizeram login há um ano: usuários que não fizeram login no último ano.
- Precisam redefinir a senha: usuários que precisam redefinir a senha.
- Falhas de redefinição de senha dos usuários: número de falhas de senha por usuário.

Identidade privilegiada

Analise dados relacionados a métricas para usuários com identidade privilegiada.

Este painel exibe dados relacionados a usuários com identidade privilegiada e suas atividades na sua instância.

- Logins de administrador: quantidade total de logins com usuários que têm função de administrador.
- Representação: quantidade total de representações realizadas por usuários com a função de representação.
- Elevação: quantidade total de elevações de segurança realizadas por usuários com a função security_admin.
- Logins da ServiceNow: quantidade total de logins de funcionários da ServiceNow.
- Usuários administradores adicionados: número total de usuários com função de administrador

Métricas de autenticação

Exiba métricas relacionadas à autenticação na sua instância de um painel.

Exibe dados para métricas relacionadas a esquemas de autenticação, como uso de MFA, contas de serviço da Web e uso de leitor biométrico.

- Usuários inscritos na MFA: a quantidade total de usuários inscritos para usar a MFA.
- Usuários que estão ignorando a MFA: quantidade total de usuários que estão ignorando a autenticação multifator.
- Usuário com privilégios elevados que não usam a MFA: quantidade total de usuários com privilégios elevados que não usam a MFA.
- Usuários ativos da MFA: quantidade total de usuários ativos da MFA na sua instância.
- Usuários da MFA bloqueados: quantidade total de usuários da MFA bloqueados na sua instância.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Usuário da conta de serviço da Web: quantidade total de usuários que tem somente conta de serviço da Web.
- Certificados X509 expirando: quantidade total de certificados X509 que expiram nos próximos 30 dias.

Contas de integração

Exiba as tendências sobre as contas de integração criadas em Now Platform.

O painel das contas de integração exibe tendências sobre as contas de integração que são criadas em Now Platform.

Veja abaixo as explicações das métricas das contas de integração:

- Total de contas de integração: tendências relacionadas a contas de integração na sua instância.
- Contas de integração ativas: tendências relacionadas a contas de integração ativas na sua instância.
- Contas de integração inativas: tendências relacionadas à quantidade total de contas de integração inativas na sua instância.

Exportar

Descubra os dados que são normalmente exportados e quais usuários fazem a exportação.

- Total de exportações: quantidade total de registros de tabela exportados pelo usuário.
- Exportações classificadas: quantidade total de registros da tabela exportados, resumida pela classificação de dados atribuída a eles.

Antivírus

Exibe a tendência de quando os eventos ocorrem em arquivos potencialmente infectados. Veja quando eles são descobertos, colocados em quarentena, restaurados ou excluídos.

- Arquivos em quarentena: o número de arquivos que podem conter malware.
- Arquivos baixados: o número de arquivos baixados.
- Arquivos restaurados: o número de arquivos que foram restaurados.
- Arquivos excluídos: o número de arquivos excluídos.

E-mail

Exibe dados relacionados a e-mails de spam que estão sendo recebidos externamente.

E-mails de spam representam o número de lixo eletrônico recebido por dia.

Sessões ativas

Exiba a linha de tendência de usuários ativos em Now Platform.

A linha de tendência pode ser exibida para as seguintes métricas:

- Sessões de usuário: métricas relacionadas a sessões de usuário ativas na sua instância.
- Sessões de usuário privilegiado: métricas relacionadas a usuários privilegiados ou àqueles que receberam funções adicionais.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Gestão de sessões

Visualize métricas relacionadas às sessões do usuário e à frequência de bloqueios das sessões.

Classificação de dados

Acesse as métricas de segurança para classificação de dados de sua instância da ServiceNow.

A classificação de dados permite a aplicação de rótulos de classificação de dados às entradas de dicionário existentes em qualquer tabela para proporcionar visibilidade sobre os tipos de dados hospedados em suas instâncias. Ela também permite o cumprimento das leis de privacidade e o atendimento das exigências regulatórias do setor.

Consulte classificação de dados para obter mais informações.

- **Dados classificáveis**: tabelas ou colunas que podem ser classificadas.
- **Dados classificados**: entradas de dicionário, tabelas ou colunas que foram classificadas.

Os dados são exibidos graficamente em um gráfico personalizável que apresenta uma análise detalhada, como definição de metas, limites, tendências, estatísticas ou previsões. Eles também são organizados como registros em uma tabela. Para obter mais informações, consulte Hub de análise.

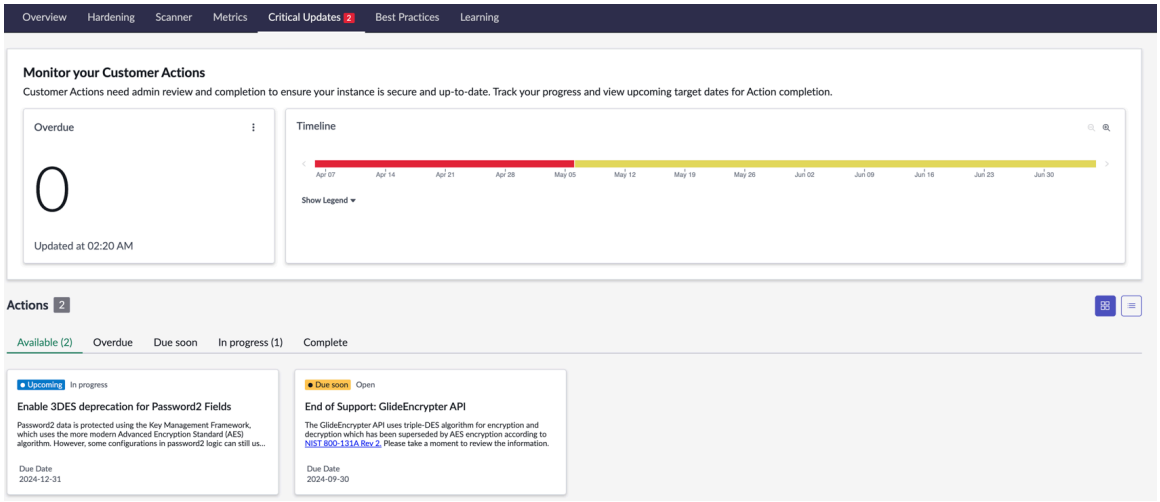
Ações do cliente

Aumente a postura de segurança da sua instância garantindo a implementação no prazo das Ações do cliente que o sistema recomenda.

Ações do cliente é uma ferramenta que ajuda os administradores a implementar atualizações importantes de segurança com base na própria instância e na configuração de plug-ins. Uma ação do cliente é uma mudança recomendada em uma instância que tem como objetivo ajudar você a entender a importância das mudanças relacionadas à segurança. A ferramenta ajuda você a implementar as etapas para verificar, atualizar e testar as atualizações de segurança na sua instância. Implemente uma ação do cliente para evitar a interferência na personalização da sua instância. As ações do cliente de implementação manual são diferentes das atualizações automáticas de códigos ou funcionalidades da ServiceNow que ocorrem na sua instância com as versões de família ou os patches.

Na página inicial de "Ações do cliente", é possível ver a linha do tempo das ações do cliente para priorizá-las ao implementar as etapas. A linha do tempo da captura de tela mostra as ações do cliente que venceram e as com vencimento em breve. Além disso, é possível rastrear o andamento de suas ações do cliente no rótulo "Atualizações". Selecione as guias para ver as ações do cliente disponíveis, vencidas, com vencimento em breve, em andamento ou concluídas.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Iniciar:

- Acesse essa ferramenta navegando até **Ações do cliente** na Central de Segurança.
- As Ações do cliente estão inclusas no app da Central de segurança a partir da versão Washington DC.

Implementação de etapas para ações do cliente

Aprenda a implementar ações do cliente em sua instância para aumentar a postura de segurança.

Antes de Iniciar

Função necessária: administrador

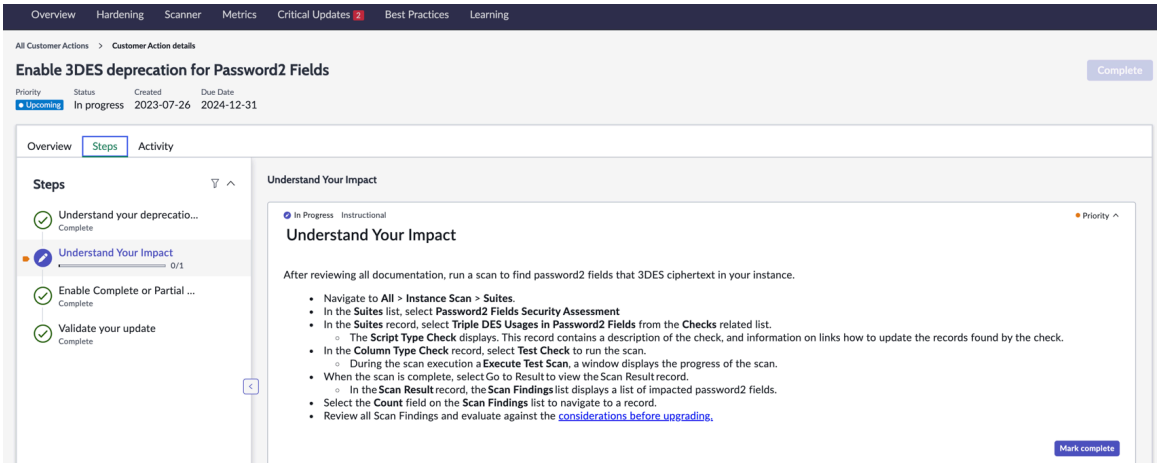
Por Que e Quando Desempenhar Esta Tarefa

As CA (Customer Actions) apresentam instruções passo a passo para implementar mudanças em sua instância para aumentar sua postura de segurança. Elas extraem conteúdo relevante da documentação do produto para guiar você durante todas as etapas do processo de implementação. Siga as etapas abaixo para saber como implementar uma ação do cliente.

Procedimento

1. Navegue até o app **Ações do cliente**.
2. Clique em uma ação do cliente para implementar.
   Na seção **Atualizações**, a guia "Disponível" listará todas as Ações do cliente de sua instância. Clique em uma ação do cliente nessa guia para exibir as instruções.
3. Leia a visão geral para saber por que a ação do cliente é necessária e para se preparar para implementar as etapas.
   Clique em **Ir para a próxima etapa** para avançar para os detalhes da implementação.
4. Implemente as etapas de atualização.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



a. Leia cada grupo de instruções e implemente-os em sua instância.

b. Clique em **Marcar como concluído** quando terminar de seguir um conjunto de instruções.

c. Repita as etapas a-b até concluir todas as etapas de atualização.

d. Clique em **Concluir**.
A ação do cliente não deverá mais estar disponível na seção "Atualizações" da página inicial de Ações do cliente.

Exibição de atividades das ações do cliente

Veja os detalhes de todas as atividades relacionadas às suas Ações do cliente.

Antes de Iniciar
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa
As atividades serão listadas da mais recente para a mais antiga para que você possa analisar a mais recente primeiro. Cada atualização de uma atividade tem um carimbo de data/hora, e você pode usar a pesquisa e o filtro para consultar informações específicas.

Procedimento

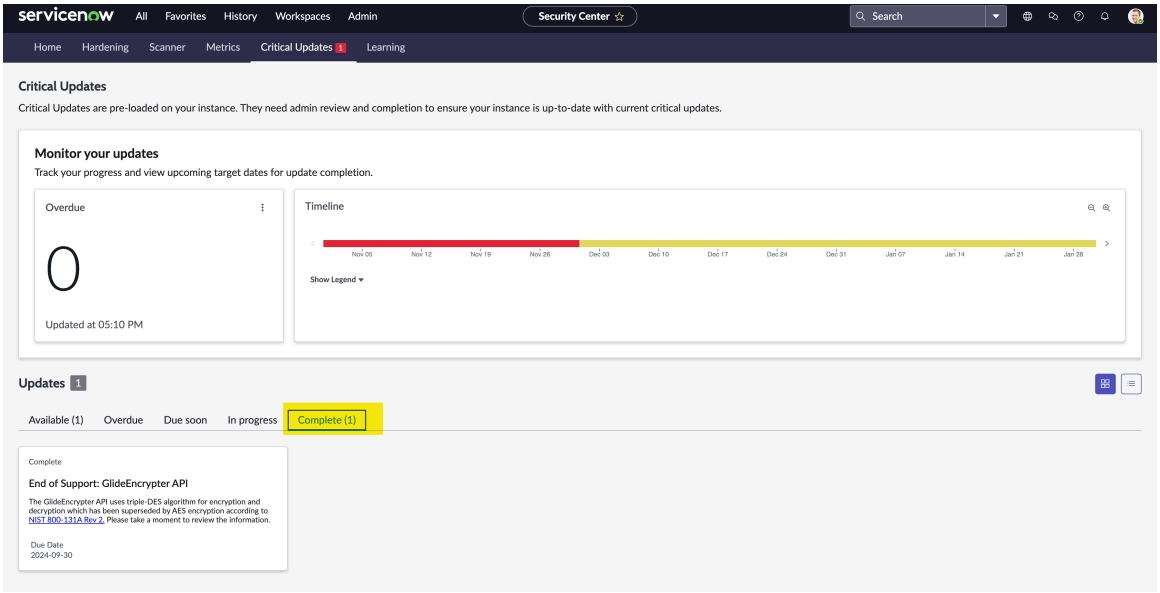
1. Navegue até o app **Ações do cliente** na Central de segurança.

2. Navegue até o rótulo **Atualizações** das Ações do cliente.

3. Clique em um estado e, depois, selecione uma ação do cliente desse estado.

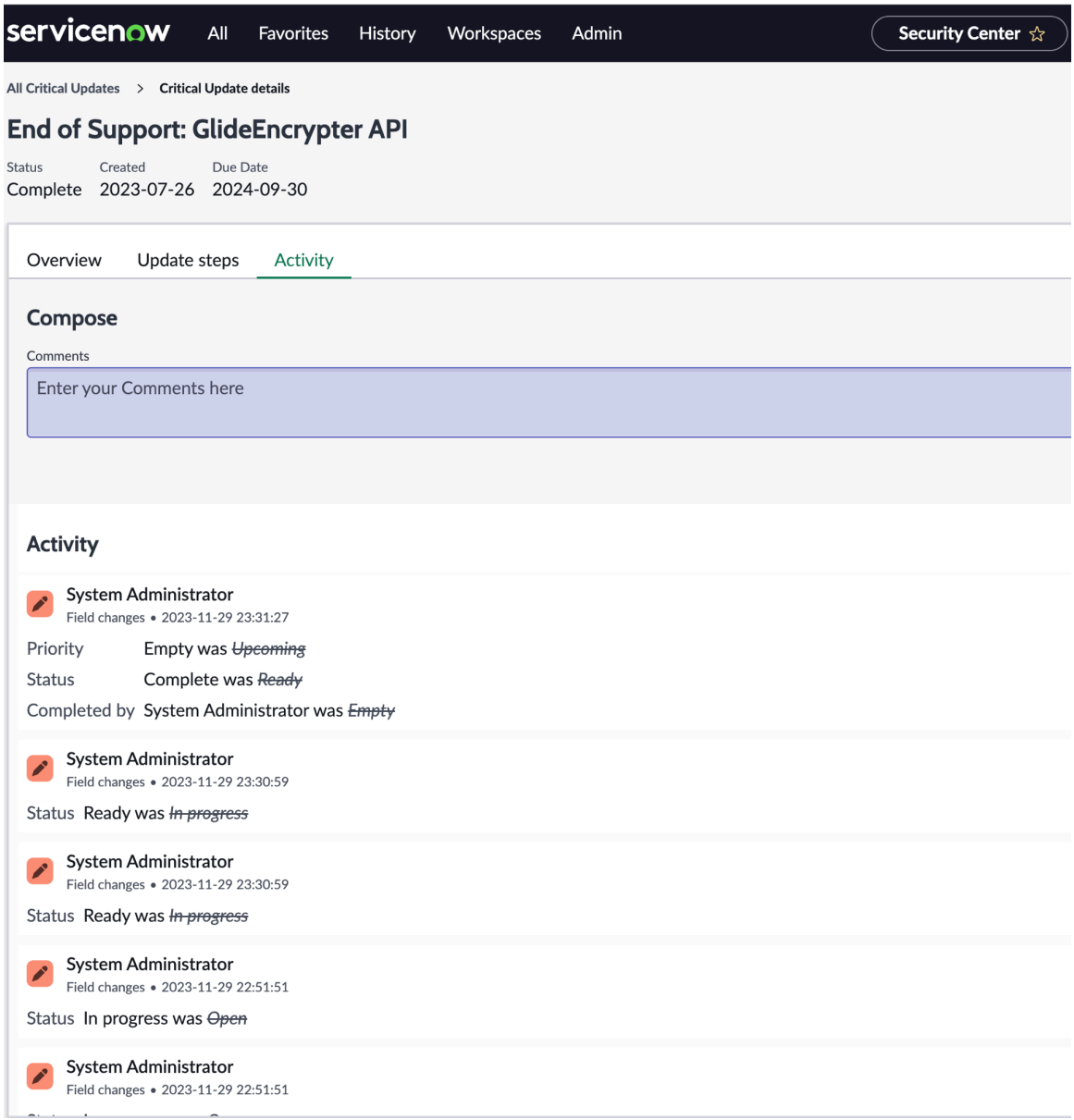
No exemplo abaixo, há a seleção do estado **Concluído** e, em seguida, a seleção da ação do cliente para **Fim do suporte: API GlideEncrypter**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Exiba a atividade da sua ação do cliente.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



A aplicação registra automaticamente todas as atividades relacionadas a uma ação do cliente. Além disso, você pode adicionar comentários adicionais às atividades.

Práticas recomendadas de segurança

Use as Práticas recomendadas de segurança para implementar tarefas de configuração de privacidade e segurança em sua instância da ServiceNow.

Use as Práticas recomendadas de segurança para analisar as sugestões de segurança da ServiceNow, identificar as que mais melhorariam sua postura de segurança e seguir as instruções passo a passo sobre como implementá-las.

As Práticas recomendadas de segurança apresentam as seguintes informações:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- A página inicial mostra uma visão geral do seu progresso na implementação das práticas recomendadas de segurança. Você também pode organizar e gerenciar listas de práticas recomendadas de segurança de acordo com os objetivos de sua organização.
- A página de visão geral apresenta detalhes de cada prática recomendada de segurança, as etapas para implementá-las e um registro de todas as atividades e todos os comentários.
- A página de etapas da tarefa apresenta instruções sobre como implementar as práticas recomendadas de segurança.
- A página de atividade rastreia o histórico das ações do sistema e do usuário relacionadas às suas práticas recomendadas de segurança.

Página inicial das Práticas recomendadas de segurança

A página inicial inclui gráficos que representam o número total de práticas recomendadas de segurança concluídas em geral, o número de práticas recomendadas concluídas por nível de maturidade e uma tabela com todas as práticas recomendadas de segurança disponíveis.

A tabela permite aplicar filtros para que você possa classificar e salvar listas filtradas e, depois, usá-las como listas de trabalho para diferentes casos de uso ou funções. Consulte Como salvar uma lista filtrada para obter mais informações.

Abaixo, há as explicações dos campos relacionados à tabela de práticas recomendadas de segurança.

Resumo dos campos usados na tabela de práticas recomendadas de segurança

Nome	Descrição
Nome	Palavra usada para identificar uma prática recomendada de segurança.
Nível de maturidade	Aplicações e recursos organizados pela ordem de impacto para apresentar resultados mensuráveis. Os valores dos níveis de maturidade são: • Criar uma base • Aprimorar a experiência • Otimizar a funcionalidade • Adicionar recursos avançados Também é possível pensar nos níveis como as fases de engatinhar, andar, correr e voar.
Status	Estado atual de uma prática recomendada de segurança: • Aberta • Em andamento • Concluído(a)

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resumo dos campos usados na tabela de práticas recomendadas de segurança

Nome	Descrição
Prioridade	Ordem de importância para implementar uma prática recomendada de segurança em sua organização: • Imediata • Mais tarde • Não aplicável
Objetivos	Categoria de segurança que uma prática recomendada de segurança aborda: • Abordar configurações iniciais de segurança • Proteger e-mails • Monitoramento de logs • Gerenciar controles de acesso • Proteger com criptografia • Manter instâncias atualizadas
Primeira introdução	Versão da Central de segurança em que a prática recomendada de segurança foi introduzida.
Alterada	Versão da Central de segurança em que a prática recomendada de segurança foi alterada pela última vez.
Removida	Versão da Central de segurança em que a prática recomendada de segurança foi removida.

Página de visão geral das Práticas recomendadas de segurança

Ao selecionar uma prática recomendada de segurança na tabela correspondente, haverá o direcionamento para uma página com as seguintes subguias: Visão geral, Etapas da tarefa e Atividade.

Na parte superior da página de visão geral, você pode exibir informações gerais sobre a prática recomendada de segurança, como prioridade, nível de maturidade e status.

O menu suspenso **Prioridade** permite especificar as práticas recomendadas de segurança que são importantes para você no momento e quais não são aplicáveis.

A seção de detalhes apresenta conteúdo sobre os recursos associados à prática recomendada de segurança, e a seção de documentação apresenta um ou mais links onde você pode encontrar informações adicionais.

O cartão **Andamento** à direita mostra o número de etapas concluídas em comparação com o número total de etapas incluídas. Selecione **Ir para a próxima etapa** para navegar até a próxima etapa incompleta.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O cartão de **histórico de atualizações de prática recomendada** apresenta uma visão geral das informações de versão da prática recomendada. Você pode rastrear em qual versão da Central de segurança da ServiceNow a prática recomendada de segurança foi lançada e em quais versões ela foi atualizada pela última vez.

Página de etapas da tarefa das Práticas recomendadas de segurança

Ao selecionar a subguia **etapas da tarefa**, haverá o direcionamento para uma página que apresenta instruções passo a passo sobre como implementar a prática recomendada de segurança. Consulte Como concluir uma prática recomendada de segurança para obter mais informações.

Página de atividade das Práticas recomendadas de segurança

As atividades são listadas da mais recente para a mais antiga para que você possa analisar a mais recente primeiro. Cada atualização de uma atividade tem um registro de data/hora, e você pode usar a pesquisa e o filtro para consultar informações. Consulte Como aplicar filtros à tabela de práticas recomendadas de segurança para obter mais informações.

Como concluir uma prática recomendada de segurança

Saiba como concluir uma prática recomendada de segurança em sua instância da ServiceNow.

Por Que e Quando Desempenhar Esta Tarefa

Siga as etapas abaixo para implementar práticas recomendadas de segurança em sua instância da ServiceNow.

Procedimento

1. Acesse as Práticas recomendadas de segurança selecionando **Todos** na sua instância da ServiceNow e inserindo a **prática recomendada**.
2. Aplique um filtro para exibir as práticas recomendadas de segurança para implementação.
   a. Navegue até a tabela **Práticas recomendadas** na IU.
   b. Selecione o menu de opções ou o item com três pontos verticais (⋮) na coluna **Status**.
   c. Selecione as opções **Aberto** e **Em andamento** e selecione **Aplicar**.
3. Selecione o nome de uma prática recomendada de segurança para implementação.
4. Selecione **Ir para a próxima etapa**.
5. Selecione uma etapa da tarefa na lista **etapas da tarefa**.
6. Selecione o ícone de seta para baixo (v) para exibir as instruções de implementação dessa etapa.
7. Leia as instruções e as implemente em sua instância da ServiceNow.
8. Quando terminar a tarefa, selecione **Marcar a etapa como concluída**.

   Nota: É possível ignorar a tarefa caso você queira retornar a ela mais tarde ou se ela não se aplicar aos objetivos da sua organização. Além disso, é possível reabrir uma etapa da tarefa concluída selecionando-a e, em seguida, selecionando **Reiniciar etapa**.

9. Selecione **Concluir prática recomendada**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

É possível concluir uma prática recomendada de segurança a qualquer momento. Você não precisa concluir todas as etapas, já que pode ignorá-las. No entanto, ao concluir uma prática recomendada sem ter concluído todas as etapas, considere inserir um comentário na subguia "Atividade" para referência de auditoria.

Como exibir a atividade de uma prática recomendada

Rastreie o histórico cronológico e com carimbo de data/hora relacionado a uma prática recomendada de segurança que você está concluindo em sua instância da ServiceNow, junto com o usuário que iniciou a atividade.

Procedimento

1. Acesse o Gerenciador de práticas recomendadas de segurança selecionando **Todos** na sua instância da ServiceNow e, depois, inserindo a prática recomendada.
2. Na tabela "Práticas recomendadas", na coluna **Nome**, selecione uma prática recomendada de segurança cuja atividade você deseja exibir.
3. Selecione a guia **Atividade**.

   Alguns exemplos de atividades que você pode exibir são mudanças de campo, como quando o status de uma prática recomendada de segurança muda de aberto para concluído ou quando uma etapa da tarefa é concluída ou ignorada. Além disso, é possível inserir informações adicionais relacionadas a uma atividade digitando um comentário na caixa de texto.

Como exibir dados de práticas recomendadas concluídas

Veja representações visuais da quantidade total de práticas recomendadas concluídas ou uma segmentação delas por nível de maturidade.

Por Que e Quando Desempenhar Esta Tarefa

Conclua as ações para ver gráficos que apresentam tendências visuais de práticas recomendadas de segurança que foram concluídas em geral e por nível de maturidade.

Procedimento

1. Acesse o app Central de segurança e navegue até a guia **Práticas recomendadas**.
2. No cartão **Gerenciar suas práticas recomendadas**, selecione o gráfico **Concluído em geral**.
3. Exiba o gráfico para ver as tendências relacionadas às configurações de práticas recomendadas de segurança que foram concluídas.
4. Selecione **Concluído por nível de maturidade** para ver um gráfico que exibe as tendências das práticas recomendadas concluídas por nível de maturidade.

Como aplicar filtros à tabela de práticas recomendadas de segurança

Aplique filtros para exibir resultados mais relevantes para suas práticas recomendadas de segurança.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Acesse o Gerenciador de práticas recomendadas de segurança selecionando **Todos** na sua instância da ServiceNow e inserindo a prática recomendada.
2. Navegue até a tabela **Práticas recomendadas** e selecione um campo ao qual você deseja aplicar um filtro, selecionando seu menu de opções ou o menu de três pontos verticais (⋮).

Campos	Filtro
Nome	Combine um operador condicional com uma cadeia de caracteres de texto para exibir as práticas recomendadas de segurança que correspondem ao nome que você digitou.
Nível de maturidade	Aplique um filtro para exibir as práticas recomendadas de segurança que correspondem a um ou mais dos seguintes níveis de maturidade: ◦ Criar uma base ◦ Aprimorar a experiência ◦ Otimizar a funcionalidade ◦ Adicionar recursos avançados
Status	Aplique um filtro para exibir as práticas recomendadas de segurança que correspondem a um ou mais dos seguintes status: ◦ Vazio ◦ Abertos ◦ Em andamento ◦ Concluído(a)
Prioridade	Aplique um filtro para exibir as práticas recomendadas de segurança que correspondem às seguintes prioridades: ◦ Vazio ◦ Imediato ◦ Mais tarde ◦ Não aplicável
Objetivos	Aplique um filtro para exibir as práticas recomendadas de segurança que correspondem a um ou mais dos seguintes objetivos:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campos	Filtro
	◦ Configurações de segurança iniciais do endereço ◦ Manter instâncias atualizadas ◦ Gerenciar controles de acesso ◦ Monitoramento de logs ◦ Proteger com criptografia ◦ Proteger e-mails **Observação**: por padrão, aplicam-se os filtros avançados aos objetivos. Para modificá-los, selecione **Fazer mudanças** > **Exibição avançada** > **Selecionar objetivos de campo** e, em seguida, crie o restante das condições e selecione **Atualizar**.
Primeira introdução	Combine um operador condicional com uma cadeia de caracteres de texto para exibir as práticas recomendadas que foram introduzidas pela primeira vez com a versão que você digitou.
Alterado	Combine um operador condicional com uma cadeia de caracteres de texto para exibir as práticas recomendadas de segurança que mudaram na versão que você digitou.
Removido	Combine um operador condicional com uma cadeia de caracteres de texto para exibir as práticas recomendadas de segurança que foram removidas na versão que você digitou.

Como salvar um filtro para uso futuro

Descubra as etapas para salvar filtros em suas práticas recomendadas de segurança e poder reutilizá-los posteriormente.

Por Que e Quando Desempenhar Esta Tarefa

Depois de criar filtros na tabela de práticas recomendadas de segurança, é possível salvá-los para usá-los na próxima vez que você se autenticar em sua instância. Se você quiser mais flexibilidade sobre o tipo de filtros que pode criar, poderá aplicar um filtro avançado.

Procedimento

1. Selecione o ícone de painel "Mostrar filtro" ( ).
2. No painel de diálogo **Filtro**, role a tela para baixo e selecione **Exibição avançada**.
3. Crie um filtro adicionando condições que contenham um campo, um operador e valores.
4. Selecione **Salvar filtro**
5. Digite o nome do filtro.
6. Selecione uma permissão.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

7. Selecione **Salvar**.
8. Selecione **Atualizar** para aplicar o filtro salvo à tabela de práticas recomendadas de segurança.

Como usar um filtro salvo

Descubra as etapas para usar os filtros que você salvou para suas práticas recomendadas de segurança.

Por Que e Quando Desempenhar Esta Tarefa
Depois que você faz logout da instância, os filtros são redefinidos às configurações padrão. As etapas abaixo mostram como recuperar um filtro salvo para que você possa reaplicá-lo na tabela de práticas recomendadas de segurança.

Procedimento

1. Selecione o ícone de painel "Mostrar filtro" ( ).
2. No painel de diálogo "Filtro", role a tela para baixo e selecione **Exibição avançada**.
3. Selecione **Usar filtro existente** e selecione um filtro salvo na lista suspensa.
4. Selecione **Atualizar** para aplicar o filtro salvo.

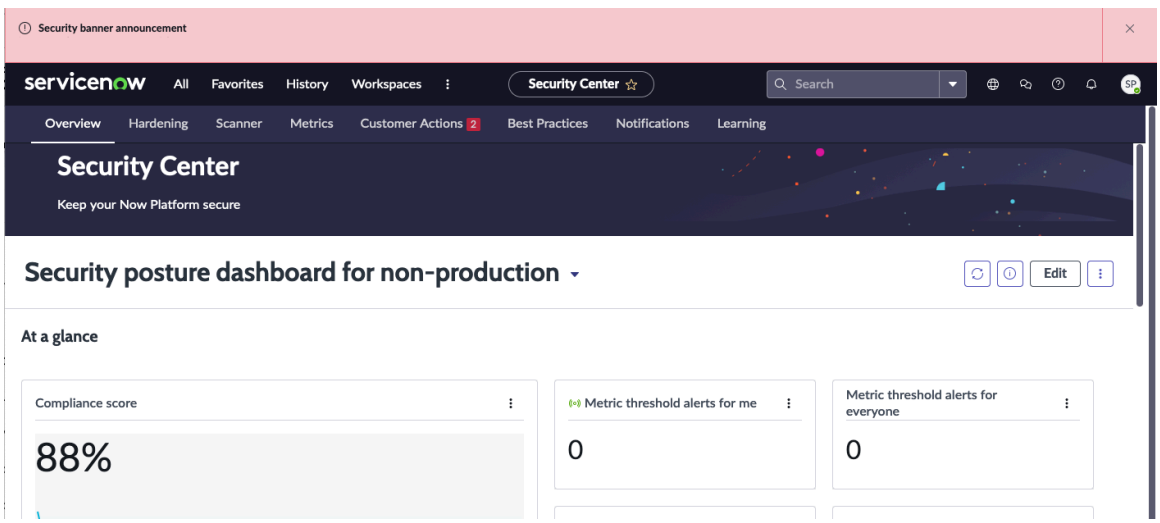
Aprendizado de segurança

Acesse materiais de aprendizado de segurança em uma só página.

Leia white papers de segurança, e-books, artigos da base de conhecimento (KB), documentação do produto e discussões da comunidade em uma exibição consolidada, navegando até **Aprendizado**. O conteúdo é organizado por títulos e cartões de IU descritivos para agilizar a identificação do recurso correto.

Faixas de comunicados de segurança

Ative as faixas de comunicados de segurança para notificar alertas de segurança urgentes e críticos exibindo faixas de alta visibilidade para os administradores na IU da instância.



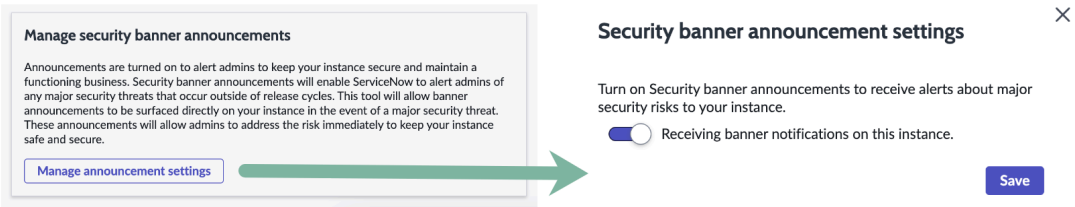
As faixas de comunicados de segurança são comunicados exibidos para os administradores do cliente, enviados pela ServiceNow, para mantê-los informado sobre correções de possíveis ameaças à segurança que foram descobertas recentemente. Esses alertas contêm

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

um resumo do risco à segurança e incluem um link onde é possível saber mais e agir para proteger sua instância.

Como ativar ou desativar faixas de comunicados de segurança

O recurso de faixa de segurança é ativado por padrão. Para ativar ou desativar as faixas de comunicados de segurança, navegue até **Segurança do sistema** > **Centro de segurança** > **Notificações**. Nessa página, selecione o botão **Gerenciar configurações de comunicados**.



Painéis de postura de segurança

Use os painéis personalizáveis de postura de segurança com uma ou várias instâncias para monitorar os KPIs de segurança. Esses painéis consolidam as informações importantes sobre a segurança das suas instâncias em um só local e incluem vários widgets de painel do sistema principal.

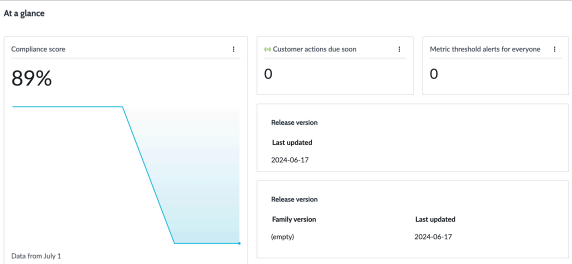
Como acessar os Painéis de postura de segurança

Acesse o Painel de postura de segurança navegando até **Todos** > **Centro de segurança**. O conteúdo do Painel de postura de segurança está localizado na guia **Visão geral**.

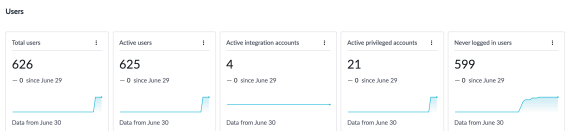
Componentes do painel

O painel é dividido em várias seções que contêm widgets relacionados a um aspecto de segurança da sua instância. Selecione qualquer widget no painel para exibir mais detalhes sobre um aspecto.

A seção **Resumo** exibe uma visão geral da segurança de uma instância, como uma pontuação de conformidade, ações pendentes do cliente e informações de atualizações e versões da instância.

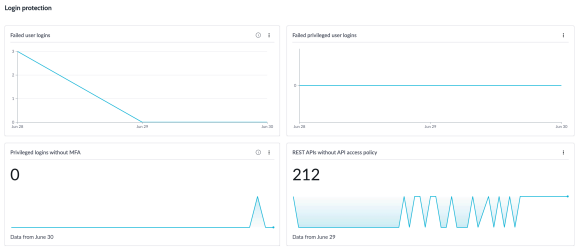


A seção **Usuários** apresenta informações sobre os usuários da sua instância. Os widgets dessa seção mostram informações do usuário e um gráfico de linhas que apresenta as mudanças nessas informações ao longo do tempo. Selecione um widget para exibir mais detalhes

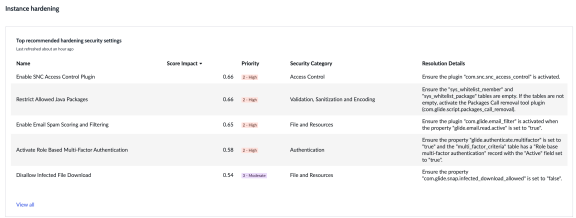


© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

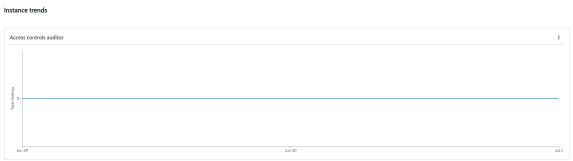
A seção **Proteção de login** inclui informações sobre falhas de login, inclusive tentativas de login com falha de usuários privilegiados.



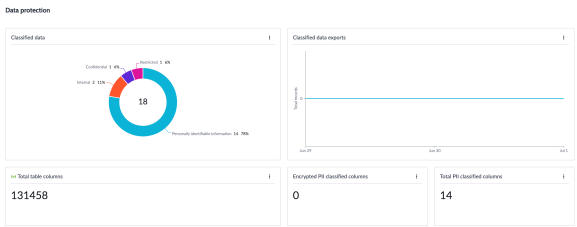
A seção **Proteção da instância** contém configurações recomendadas de proteção que você pode mudar para melhorar a segurança da instância. Use essa seção para ver a prioridade e o possível impacto dessas mudanças.



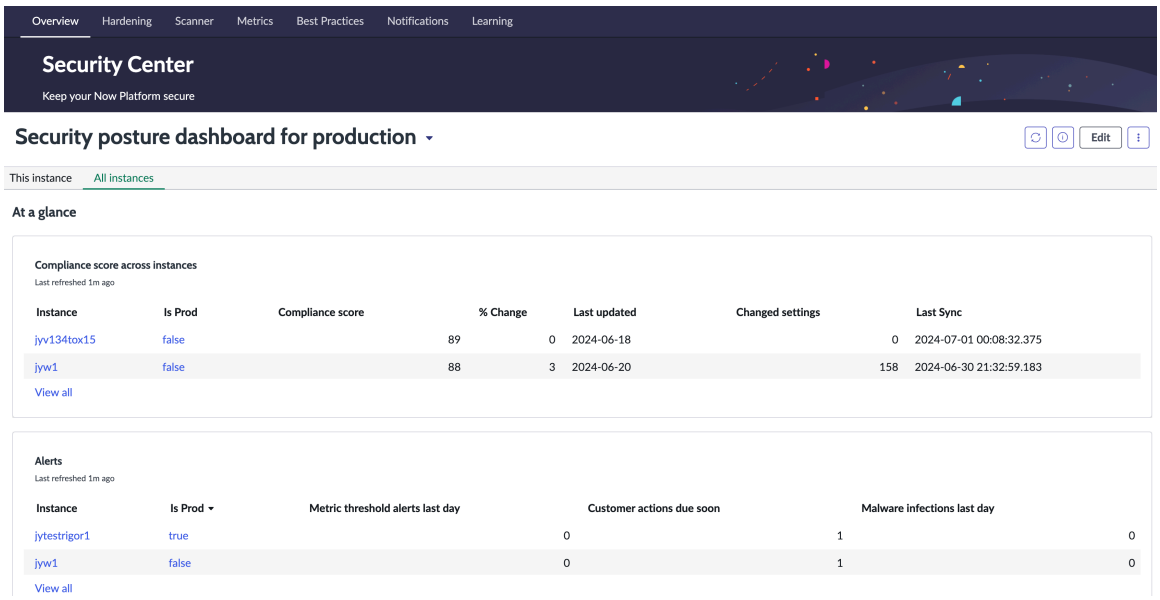
O painel **Tendências da instância** exibe os resultados do pacote de verificação do auditor de controles de acesso.



Use a seção **Proteção de dados** para obter uma visão geral dos dados confidenciais, como PII (Personally Identifiable Information, informações de identificação pessoal). O painel também rastreia exportações de dados confidenciais.



Revisão de várias instâncias

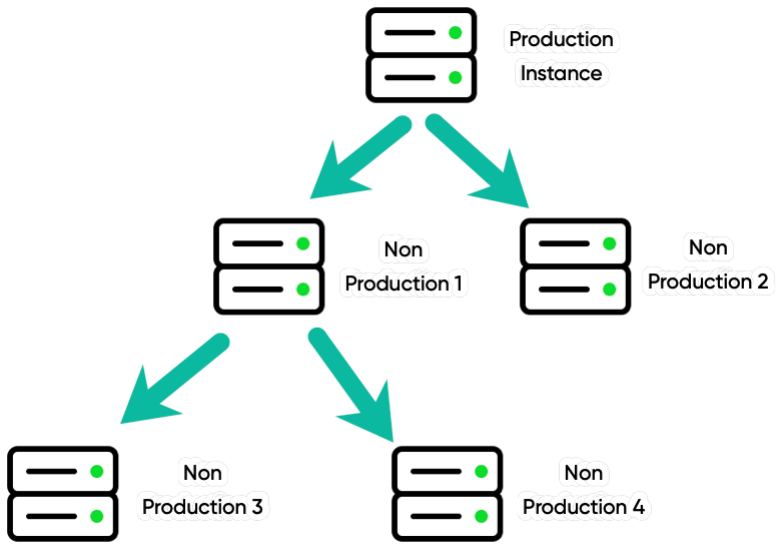


Usando a guia **Todas as instâncias** na parte superior do painel, veja a postura de segurança de suas instâncias de não produção sem sair da instância de produção. A guia **Todas as instâncias** exibe uma versão resumida das mesmas informações da guia **Esta instância**, mas também inclui dados de todas as suas instâncias de não produção.

Por padrão, a guia **Todas as instâncias** exibe informações sobre a instância de produção, todas as instâncias clonadas da produção e todas as instâncias clonadas das instâncias

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

clonadas. Neste exemplo, duas instâncias são clonadas da produção e duas instâncias adicionais são clonadas de um desses clones. Todas as cinco instâncias aparecem na guia **Todas as instâncias**.



Personalização do painel

Não é possível personalizar o painel de postura de segurança, mas é possível duplicá-lo selecionando o ícone **Mais ações** (⋮) e selecionando **Duplicar**. Em seguida, é possível mudar o painel duplicado.

Notificações de eventos de segurança

Veja, gerencie e analise as políticas padrão de notificações de eventos de segurança de sua instância da ServiceNow. Acesse também a funcionalidade para criar novas políticas personalizadas.

Personalize e crie facilmente políticas de notificação que acionam notificações por e-mail quando os usuários realizam ações na Now Platform que podem ser inseguras ou que exigem monitoramento do administrador.

As notificações de eventos de segurança são compostas por duas partes: configuração das políticas de segurança e configuração das notificações. A configuração de políticas permite que você especifique a combinação de eventos e ações que acionam as notificações. A configuração de notificações permite que você especifique os formatos e os destinatários dos e-mails.

Os administradores podem personalizar os valores das políticas padrão, clonar e editar as políticas padrão ou criar suas próprias políticas personalizadas.

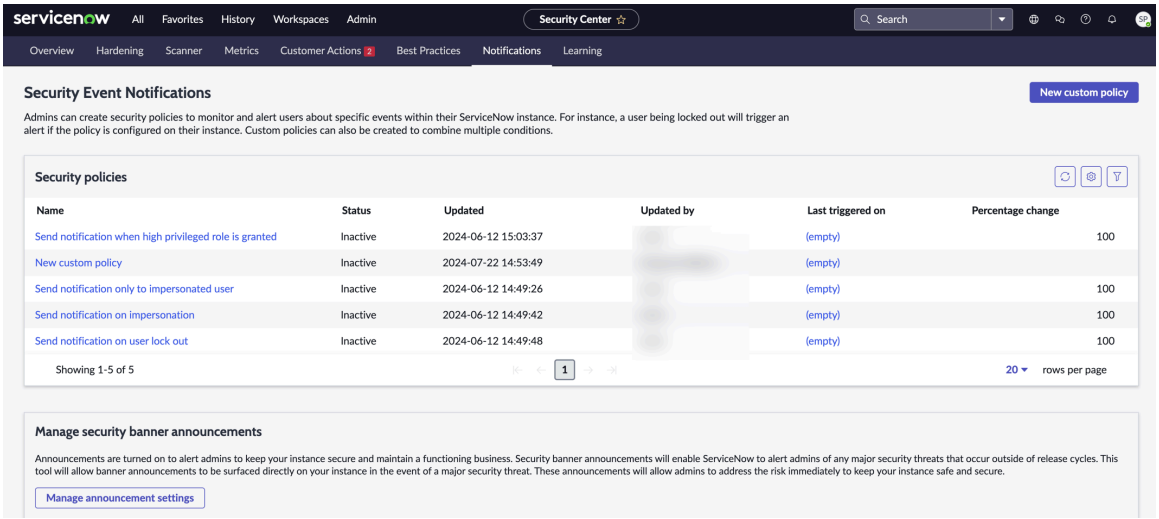
Visão geral das Notificações de eventos de segurança

Na visão geral das Notificações de evento de segurança, você pode ver uma tabela que organiza todas as políticas de segurança disponíveis em sua instância.

Essa tabela inclui colunas que exibem o nome da política, o status (ativa ou inativa), a data e hora da última atualização, o usuário que fez a atualização, a data e hora do último gatilho e a mudança percentual (ou a taxa de mudança dos gatilhos semanais calculada como uma porcentagem). Por exemplo, se essa política aciona uma média de cinco

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

notificações por semana e foi acionada dez vezes na semana passada, isso representaria um aumento percentual de 100%.



Além disso, você pode selecionar o botão **Nova política personalizada** para criar uma nova política personalizada adaptada aos casos de uso de sua organização.

Página de visão geral das Notificações de eventos de segurança

Navegue até a página inicial das Notificações de eventos de segurança e selecione qualquer uma das políticas que você deseja revisar ou personalizar. A guia "Visão geral" apresentará um quadro geral da política. Para personalizar a política, selecione a guia **Configurações da política**.

Não é possível mudar o gatilho nem a lógica de condição das políticas padrão. Se você quiser fazer essas mudanças, primeiro é necessário duplicar a política selecionando o botão "Duplicar" no canto superior direito da página.

Nota: para exibir o botão "Duplicar", é necessário selecionar o ícone do menu de opções (menu de três pontos) à direita do botão "Atualizar", no canto superior direito.

Depois de concluir as mudanças, lembre-se de selecionar o botão "Atualizar". E lembre-se de desativar a política até que você esteja pronto para começar a acionar notificações. É possível ativar e desativar a política com o botão no canto superior direito, ao lado do botão "Atualizar".

Acesse um quadro geral das políticas de notificações de eventos de segurança em sua instância, onde os dados são organizados em cartões de IU. Analise os detalhes e as seções de atividade, e use a funcionalidade para incluir informações adicionais às políticas de segurança, como por meio de comentários.

Campos e funcionalidade da tabela de visão geral

Rótulo	Descrição
Nome	O nome da política de notificações de eventos de segurança.
Status	O status de uma política pode ser "Ativa" ou "Inativa".
Atualizada em	A data e hora da última atualização da política.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campos e funcionalidade da tabela de visão geral

Rótulo	Descrição
Atualizada por	O usuário que atualizou uma política.
Último acionamento	A data e hora em que a política foi executada pela última vez.
Número de acionamentos na última semana	O número de gatilhos que uma política gerou nos últimos sete dias.
Mudança percentual	A taxa de mudança dos gatilhos semanais calculada como uma porcentagem.

Como criar políticas personalizadas de notificações de eventos de segurança

Saiba como criar notificações personalizadas de eventos de segurança específicas para as necessidades da sua organização. Com elas, você pode monitorar as ações que usuários e grupos realizam em sua instância e gerar notificações de possíveis riscos à segurança.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Navegue até o app Central de segurança e selecione **Notificações** .
2. Selecione **Nova política personalizada**.
3. Selecione um dos três tipos de evento que acionarão o início da política e selecione **Criar**.
4. Configure a política.
   Consulte Como configurar preferências para políticas de notificação de eventos de segurança para saber como configurar sua nova política personalizada de notificações de eventos de segurança.

Modificação das políticas de notificações de eventos de segurança

Saiba como modificar as configurações de suas políticas de notificações de eventos de segurança.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Navegue até a página inicial de **Notificação** de eventos de segurança e selecione qualquer uma das políticas que você deseja modificar.

   Nota: Não é possível modificar o gatilho nem a lógica de condição das políticas padrão. Para modificar essas configurações, primeiro você deve duplicar a política. Faça isso selecionando a seta para baixo ao lado de **Atualizar** e, em seguida, selecionando **Duplicar**.

2. Selecione as **configurações da política** para mudar as configurações.
3. Selecione **Atualizar** para salvar suas mudanças.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Opcional: Selecione **desativar** até que você esteja pronto para começar a acionar notificações.
5. Opcional: Para começar a acionar notificações, selecione **Ativar**.
   Consulte Como configurar preferências para políticas de notificação de eventos de segurança para saber como configurar sua nova política personalizada de notificações de eventos de segurança.

Como configurar preferências para políticas de notificação de eventos de segurança

Descubra como personalizar as políticas de notificação de eventos de segurança na Security Center para alinhá-las às necessidades específicas da sua organização.

Antes de Iniciar

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

Na página **Configurações de política**, é possível personalizar as configurações de uma política de notificação de eventos de segurança. Aqui, é possível ajustar opções relacionadas a quando a política é executada, à lógica condicional e às notificações enviadas.

Procedimento

1. Na Central de segurança, selecione **Notificações**.
2. Na tabela "Políticas de segurança", selecione uma política de notificação de eventos de segurança que você deseja configurar.
   Por exemplo, **Enviar notificação quando a função de privilégio alto for concedida**.
3. Selecione **Configurações de política**.
4. Defina as configurações da política.

Opções de definição das configurações de política

Rótulo	O que configurar
Quando executar	**Gatilho**: o evento que inicia a política.
Condições	A lógica condicional e as condições que serão aplicadas às suas políticas. ◦ **Lógica de condição**: duas opções ▪ **É necessário atender a todas as condições para acionar esta política**: todas as condições precisam ser válidas para que a política envie notificações. ▪ **É necessário atender a qualquer uma das condições para acionar esta política**: as notificações serão enviadas se qualquer uma das condições for válida. ◦ **Adicionar condição**: selecione "Adicionar condição" e informe os valores adequados.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Rótulo	O que configurar
	É possível remover uma condição selecionando **Remover condição**.
Notificações	O corpo e os destinatários do e-mail: ◦ **Notificação**: selecione um dos modelos de notificação predefinidos. Para obter mais informações, consulte Como criar um e-mail personalizado para notificações de eventos de segurança. ◦ **Adicionar notificação**: selecione "Adicionar notificação". ◦ **Grupos**: selecione o grupo que deve receber a notificação. ◦ **Usuários**: selecione os usuários que devem receber a notificação. É possível remover uma notificação selecionando **Remover notificação**.

Nota: Se você quiser tornar uma política inativa, selecione **Desativar**. Se você quiser replicar uma política, selecione a seta para baixo ao lado do botão **Atualizar** (

).

5. Selecione **Atualizar** para salvar suas configurações.

Como criar um e-mail personalizado para notificações de eventos de segurança

Saiba como criar um e-mail personalizado para notificações de eventos de segurança configurando novas notificações, definindo gatilhos, estabelecendo destinatários e criando conteúdo de e-mail com campos de evento dinâmicos.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Selecione **notificações do sistema** > **notificação**.
2. Selecione **novo**.
3. Digite um **nome** para o campo de notificação.
4. Selecione o campo ao lado de **tabela** e insira a notificação da política de segurança (*sn_vsc_security_policy*).
5. Configure o novo registro.
   O registro contém três guias que exigem configuração: **Quando enviar**, **Quem receberá** e **O que conterá**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia	Descrição
Quando enviar	Selecione o campo ao lado do rótulo **Enviar quando** e selecione **Acionado**.
Quem receberá	◦ Selecione o ícone local ao lado de **Usuários/grupos em campos** e selecione **Usuários** e **Grupos**. Selecione o ícone **Adicionar item** (>) para mover os campos ao campo de texto **Selecionado**. ◦ Clique com o botão direito na faixa de cabeçalho e clique em **Salvar**.

O que conterá	Crie um modelo de e-mail.
	
	Para obter mais informações, consulte Criar um modelo de e-mail.
	
	Insira os campos do evento em **Mensagem HTML**. Você pode fazer isso usando `${event_id.FIELD_NAME}`. Veja um exemplo:
	
	`Role: ${event_id.role.URI_REF}`
	`Granted to:`
	`${event_id.granted_to.URI_REF}`
	`Granted by:`
	`${event_id.user.URI_REF}`
	`Logged at:`
	`${event_id.sys_created_on}`
	`Security Center Notification:`
	`${execution.policy.name}`

6. Selecione **Enviar**.
7. Adicione uma notificação personalizada ao modelo de e-mail em "Notificações de eventos de segurança".
   a. Na Central de segurança, selecione **Notificações** > **Configurações de política**.
   b. Navegue até o rótulo **Notificações**.
   c. Digite o nome da notificação personalizada que você criou no campo **Notificação**.

Histórico de notificações de eventos de segurança

Explore o histórico completo das notificações de eventos de segurança em sua instância.

A página **Notificações** apresenta uma visão geral do histórico de notificações de todas as políticas de notificações de eventos de segurança em sua instância. É possível exibir os dados em gráficos, apresentando-os graficamente e aplicando funcionalidades de análise de desempenho, como metas, limites e sinais de KPI. Outra opção é exibir os dados em formato de tabela, o que permite o uso de funcionalidades padrão, como pesquisa, classificação, filtro e consulta.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Central de segurança da instância

Monitore o nível de conformidade de controles de segurança da instância, visualize as métricas de monitoramento de eventos de segurança e configure e mantenha todas as configurações de segurança da instância de dentro da Central de segurança da instância. A Central de segurança da instância consolida vários componentes de segurança de chave em um único console de controle que ajuda a detectar, proteger e responder a eventos de segurança baseados em instância.

Visão geral da Central de segurança da instância

Importante:

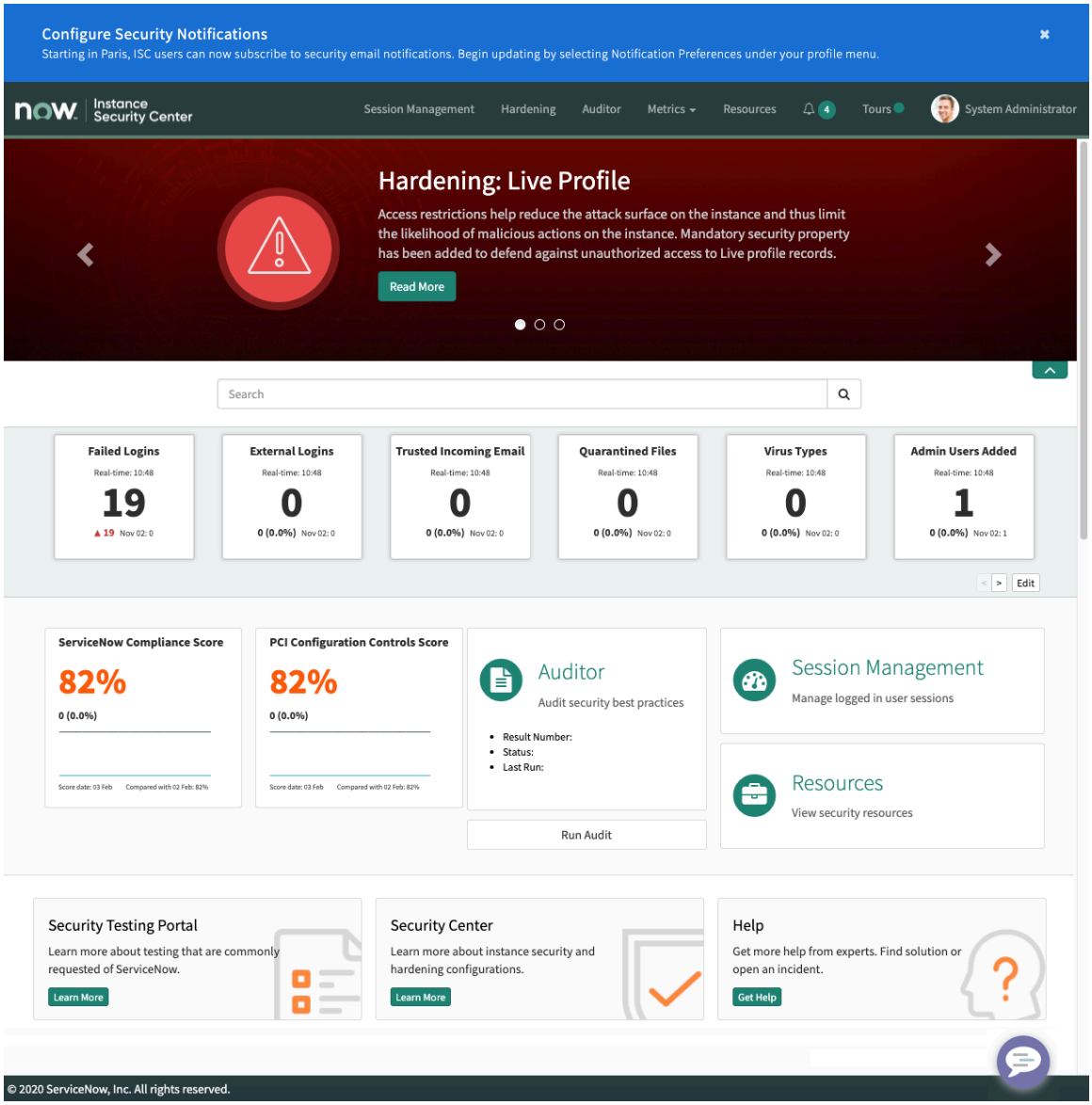
A Central de segurança da instância (ISC) atingiu o fim das vendas em setembro de 2024 e não é mais compatível ou disponível para nova ativação.

A SSC (ServiceNow Security Center, Central de segurança da ServiceNow) é a solução recomendada no futuro. Para obter mais informações, consulte Migração da Central de segurança da instância para a ServiceNow Security Center.

Componentes da Central de segurança da instância

Para acessar a Central de segurança da instância, navegue até **Segurança do sistema** > **Central de segurança da instância** ou a página inicial de Administração do sistema.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



A página inicial da Central de segurança da instância contém os seguintes componentes de segurança:

- Mensagens do administrador
- Faixa de segurança rotativa
- Pesquisar
- Faixa de opções de eventos de segurança
- Pontuação de conformidade diária
- Pontuação de controles de configuração de PCI
- Gestão de sessões
- Proteção
- Auditor
- Métricas (usuário, e-mail e antivírus)
- Recursos
- Notificações de segurança
- Tours

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Portal de teste de segurança
- Central de segurança
- Ajuda
- Acesso ao Virtual Agent

A partir da página inicial da Central de segurança da instância, você pode exibir a pontuação de conformidade de segurança da instância e monitorar a integridade geral da segurança. Em seguida, você pode configurar ou atualizar as propriedades do sistema que estão relacionadas à segurança da sua instância para que elas estejam em conformidade com os requisitos de segurança.

Nota: A Central de segurança da instância não é compatível com Domain Separation.

Funções de usuário

Para usar a Central de segurança da instância, você deve ter a função de administrador ou security_dashboard_user.

Para saber mais sobre como gerenciar assinaturas por usuário, consulte Como gerenciar assinaturas por usuário no Gestão de assinaturas e entre em contato com o representante da sua conta.

funções

Função necessária	Usuário	Benefícios
administrador	Essa função tem acesso a todos os recursos, funções e dados do sistema porque os administradores podem substituir as regras da lista de controle de acesso (ACL) e passar em todas as verificações de função. Evite atribuir esta função a seus usuários quando houver mais funções direcionadas disponíveis.	Aproveite as ferramentas Security Center para melhorar a postura de segurança da instância e monitorar os comportamentos relacionados à segurança.
sn_vsc.security_center_viewer	Essa função permite que usuários que não são administradores exibam as informações em Security Center, mas não façam mudanças nas ferramentas Security Center ou alterem as configurações de instância com as ferramentas Security Center. Por exemplo, proprietários de plataforma, analistas de operações de segurança	Obtenha visibilidade das ferramentas Security Center para monitorar a postura de segurança da instância e monitorar os comportamentos de segurança.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

funções

Função necessária	Usuário	Benefícios
	ou partes interessadas de conformidade podem querer ou precisar exibir alguns dos KPIs e informações de segurança e material de aprendizado disponíveis em Security Center.	

Aviso: Para garantir que a Central de segurança da instância receba informações de segurança atualizadas com cada upgrade, não personalize este módulo. Se você alterar qualquer configuração de segurança em sua instância, certifique-se de testá-la em um ambiente de não produção primeiro.

Mensagens do administrador

Mensagens e lembretes, destinados principalmente a administradores, aparecem acima da faixa de segurança rotativa.

Por exemplo, uma mensagem `Configurar notificações de segurança` é exibida para lembrar os administradores de configurar preferências para notificações de segurança, caso ainda não tenham feito isso. Ela também mostra a página apropriada para fazer isso.

Nota: A faixa de mensagens do administrador não é exibida para usuários que não sejam administradores ou se não houver itens acionáveis para usuários administradores.

Faixa de segurança rotativa

Para ajudá-lo a monitorar a integridade da segurança de sua instância, mensagens de segurança de instância crítica aparecem na faixa rotativa.

- Duas a três mensagens de segurança normalmente são alternadas em intervalos regulares.
- Os pontos na parte inferior da faixa mostram o número total de mensagens de segurança atuais.
- Para navegar por eles, selecione os pontos ou as setas que aparecem em cada lado das mensagens.

As cores do plano de fundo da faixa indicam a gravidade relativa das mensagens.

Cor	Descrição
Vermelho	Situação crítica de segurança que requer uma resposta oportuna ou uma recomendação sobre como proteger ou responder a eventos de segurança críticos.
Cinza escuro	Mensagem de aviso não crítica.
Azul	Mensagem de informações gerais

Para recolher ou minimizar o conteúdo de texto na faixa, selecione . Para maximizar o conteúdo do texto, selecione-o novamente.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Quando você usar a Central de segurança da instância novamente, o conteúdo de texto aparece como recolhido ou expandido, dependendo de como você o usou durante a sessão anterior.
- Se o próprio conteúdo de texto mudar, ele aparecerá como maximizado para todos os usuários.

Pesquisar

Use a barra de pesquisa para pesquisar recursos de segurança em toda a Central de segurança da instância que ajudam você a entender e resolver problemas de segurança. Você pode pesquisar os seguintes recursos relacionados à segurança:

- Artigos da Now Support Base de conhecimento
- Páginas da Central de segurança da instância
- Links externos do Now Support
- Widgets de segurança de PA, como Pontuação de conformidade diária e E-mails de entrada externos
- Conteúdo da faixa

Faixa de opções de eventos

Use a faixa de opções de eventos para exibir as principais métricas de monitoramento de eventos de segurança para a instância atual.

- Para rolar manualmente pelas métricas, selecione as teclas de seta para a direita ou para a esquerda.
- Para configurar a faixa de opções de eventos, selecione **Editar**.

Para saber mais sobre a faixa de opções de evento e como configurá-la, consulte Monitorar eventos de segurança e Configurar a faixa de opções de eventos de segurança.

Pontuação de conformidade diária

A seção Pontuação de conformidade diária contém os blocos **Pontuação de conformidade diária**, **Gestão de sessões**, **Proteção**, **Auditor**e **Recursos**.

Você usa a Pontuação de conformidade diária para medir a integridade da sua instância do ponto de vista da segurança.

A Pontuação de conformidade diária é uma pontuação percentual. É baseada no quanto as configurações atuais das propriedades de segurança de sua instância estão em conformidade com os valores de conformidade publicados em Configurações de proteção de segurança da instância.

- Para saber mais sobre os cálculos da Pontuação de conformidade diária e como as configurações de proteção a afetam, consulte Verificar a pontuação de conformidade diária e definir as configurações da propriedade de segurança.
- O botão **Atualizar** permite que um administrador recalcule instantaneamente a Pontuação de conformidade diária. Para saber mais, consulte Como a pontuação de Conformidade diária e os dados de tendência e do gráfico são atualizados.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Proteção

Use este processo para ajustar as propriedades de configuração de segurança específicas que afetam a Pontuação de conformidade diária:

1. Para acessar a página Configurações de conformidade de proteção e executar a proteção da Segurança da instância, selecione o bloco **Pontuação de conformidade diária** ou no link **Proteção**.
2. Especifique se você deseja exibir todos ou somente os controles de segurança recomendados. Em seguida, selecione a categoria na qual você deseja trabalhar.
3. Defina cada propriedade de configuração de segurança na categoria selecionada. Clique em **Mais informações** para exibir informações detalhadas de uma propriedade.

Para saber mais sobre como proteger e otimizar as propriedades de configuração de segurança para aumentar ainda mais a conformidade, consulte Ajuste as configurações de segurança da instância para aumentar a conformidade.

Para saber mais sobre como os dados de tendência e gráfico são atualizados, consulte Como a pontuação de Conformidade diária e os dados de tendência e do gráfico são atualizados.

Auditor

Execute o Auditor para verificar sua instância e encontrar definições de segurança incorretas. Ele fornece descobertas que você pode corrigir para ajudar a melhorar a postura de segurança da sua instância.

Para acessar a página Auditor, selecione o bloco **Auditor** ou o link **Auditor**. Para saber mais, consulte Verificar se há definições de segurança incorretas.

Gestão de sessões

Use o Gestão de sessões para:

- Exibir e gerenciar sessões de login do usuário.
- Veja a sessão de login do usuário do nó atual ao qual você está conectado.
- Ver informações detalhadas sobre cada sessão, como o nome de usuário e o endereço IP.
- Isolar e bloquear sessões de usuário específicas que representam riscos à segurança.

Para acessar a página Gestão de sessões, selecione o link ou o bloco **Gestão de sessões**.

Campo	Descrição
Usuário	Nome do usuário associado a esta sessão de login. • Para localizar uma sessão de usuário específica, selecione o ícone de pesquisa em destaque ( ) para pesquisar por usuário, palavra-chave do agente do usuário ou endereço IP. Por exemplo, se você quiser encontrar todos os logins atuais de um tipo específico de navegador, insira o nome do navegador como uma palavra-chave no campo **Agente do usuário**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	• Clique em um nome de usuário para acessar o registro de perfil de usuário. Você pode modificar o perfil de usuário somente se tiver uma função de administrador atribuída. **Nota:** Para saber mais sobre perfis de usuário, consulte Criar um usuário.
MFA	Marque a caixa de seleção que indica se a MFA (Multi-factor Authentication, autenticação multifator) está habilitada para o usuário conectado. Para saber mais sobre a MFA, consulte Autenticação multifator (MFA).
Ativo	Marque a caixa de seleção que indica se o usuário conectado está ativo ou inativo.
Agente do Usuário	Tipo de navegador e sistema operacional do dispositivo para a sessão de login do usuário.
Endereço IP	Endereço IP do usuário conectado.
Último acesso	Data e hora em que esta sessão do usuário acessou a instância pela última vez. **Nota:** Para exibir informações detalhadas de uma sessão de login específica ou para bloquear a própria sessão, selecione os campos **Agente do usuário**, **Endereço IP** ou **Último acesso**.

Métricas

Exibir detalhes dos seguintes tipos de métrica:

Tipo de métrica	Descrição
Usuário	Métricas de segurança associadas à atividade do usuário na instância. Para acessar a página Métricas do usuário, selecione o link **Métricas** e, em seguida, **Métricas do usuário**.
Exportar	Métricas de segurança associadas aos dados exportados da instância. Para acessar a página Exportar métricas, selecione o link **Métricas** e, em seguida, **Exportar métricas**.
Autenticação	Métricas de segurança relacionadas à autenticação, como endereços IP usados com pouca frequência, logins com falha e tipos de esquemas de autenticação usados por seus usuários. Para acessar a página Exportar métricas, selecione o link **Métricas** e, em seguida, **Métricas de autenticação**.
E-mail	Métricas de segurança associadas a comportamentos anormais relacionados aos e-mails de entrada para sua instância.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tipo de métrica	Descrição
	Para acessar a página Métricas de e-mail, selecione o link **Métricas** e, em seguida, **Métricas de e-mail**.
Antivírus	Métricas de segurança associadas à atividade de evento de antivírus na instância. Para acessar a página Métricas de antivírus, selecione o bloco **Antivírus** ou o link **Métricas** e, em seguida, **Antivírus**.

Nota: Para saber mais sobre como monitorar cada tipo de métrica, consulte Monitorar métricas de instância.

Recursos

Acesse artigos da Now Support Base de conhecimento, recursos e blogs relacionados à segurança da instância. Esses recursos incluem configurações de segurança, codificação, conformidade, correções e tópicos relacionados. Para acessar a página Recursos:

1. Clique no bloco ou no link **Recursos**.
2. Na página Recursos, selecione uma categoria:

Categoria	Descrição
Diretrizes recomendadas	Acesso às diretrizes de segurança recomendadas, incluindo os artigos Configurações de proteção de segurança da instância e Guia de codificação segura [KB0623354].
Recursos de Segurança	Acesso a recursos relacionados à segurança na Base de conhecimento, incluindo: ◦ Teste de segurança da instância do cliente ◦ Artigos da base de conhecimento de Segurança na nuvem, Centro de conformidade e de confiança

Notificações de segurança

Um ícone de sino de notificações ( ) aparece na Central de segurança da instância, com uma contagem total de notificações de segurança não lidas. As notificações são mantidas e incluídas nesta contagem até que você as marque como lidas.

1. Clique no ícone de sino para exibir as primeiras cinco notificações de segurança não lidas.

   Uma notificação é exibida quando os eventos **Login de administrador**, **Administrador desbloqueado**, **Falha de login**, **Função de alto privilégio**, **Representação**, **Elevação de segurança**e **Resumo semanal** ocorrem em sua instância. Para saber mais sobre esses eventos de segurança, consulte Monitorar eventos de segurança.

2. Para exibir informações detalhadas de um evento de segurança específico, selecione a notificação.

   Por exemplo, se você selecionar uma notificação de Função de alto privilégio, poderá exibir a tabela Funções (sys_user_role). Use esta tabela para ver quais usuários foram

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

atribuídos a funções privilegiadas durante o dia do calendário. Usar este histórico ajuda a determinar se as funções foram atribuídas corretamente.

3. Se houver mais de cinco notificações não lidas, selecione **Exibir todas as notificações** para acessar a página Todas as notificações com uma lista de todas as notificações não lidas.
   - Para exibir informações detalhadas de um evento de segurança específico, selecione a notificação.
   - Para marcar todas as notificações listadas como lidas, selecione **Marcar todas como lidas**.

Nota: Como administrador, você também pode configurar preferências para enviar tipos específicos de notificações para cada tipo de evento de segurança. Para saber mais, consulte Definir preferências para notificações de eventos de segurança.

Tours

Clique no link **Tours** para exibir um tour visual guiado da Central de segurança da instância.

- O tour guiado inclui somente as funções de monitoramento de segurança listadas na página inicial.
- Ele não inclui as funções de segurança que você acessa ao selecionar os blocos ou links na página inicial.

Portal de testes de segurança, centro de segurança e ajuda

O Now Support Portal de serviços é um recurso central usado para gerenciar instâncias, tarefas e contas. Você também pode acessar recursos úteis que podem ser usados para diagnosticar e resolver problemas técnicos e de segurança em sua instância.

Para acessar esses recursos, selecione **Saiba mais** ou **Obter ajuda** nos seguintes blocos:

Lado a Lado	Descrição
Portal de Teste de Segurança	Acesso ao painel de segurança no Portal de testes de segurança do Now Support.
Central de segurança	Acesso à Conformidade de segurança no Portal de segurança do Now Support.
Ajuda	Acesso aos seguintes recursos de ajuda no Portal de segurança do Now Support: • Pergunte a um especialista para encontrar respostas para perguntas comuns. • Relate um problema ou uma indisponibilidade ao Suporte técnico global da ServiceNow abrindo um caso. • Recursos de autoatendimento de suporte, incluindo: ◦ Vídeos ◦ Documentação ◦ ServiceNow Community ◦ Base de conhecimento

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Lado a Lado	Descrição
	◦ Portal de erros conhecidos ◦ Banco de dados de segurança RFX • Perguntas da ServiceNow Community que são recomendadas para seu uso.

Acesso ao Virtual Agent

O Virtual Agent é uma plataforma para fornecer assistência ao usuário por meio de conversas em uma interface de envio de mensagens.

Com os plug-ins associados instalados, os administradores podem acessar as funções Virtual Agent e Compreensão da linguagem natural (NLU) selecionando o ícone do Virtual Agent:

Ele permite que você execute as seguintes tarefas:

- Faça perguntas relacionadas à segurança e obtenha respostas de resumo rápido e links de referência para saber mais.
- Obtenha respostas relacionadas a processos como:
  - Central de segurança da instância
  - Segurança da plataforma
  - Políticas de segurança da ServiceNow
  - Confiança, governança e risco
- Pesquise recursos relacionados à segurança, como tópicos da Base de conhecimento no Portal de segurança do Now Support.

Nota: Para saber mais sobre como usar e ativar o Virtual Agent, consulte:

- Virtual Agent
- Como ativar a interface do ISC Virtual Agent

Migração da Central de segurança da instância para a ServiceNow Security Center

Aprenda as principais diferenças ao migrar da ISC (Instance Security Center, Central de segurança da instância) para a SSC (ServiceNow Security Center, Central de segurança da ServiceNow).

Importante:

A Central de segurança da instância é um produto legado que chegará ao fim das vendas em setembro de 2024. A Central de segurança da ServiceNow é a solução recomendada para os clientes adotarem no futuro. Para obter mais informações, consulte o artigo processo de descontinuação (KB0867184) na base de conhecimento do Now Support.

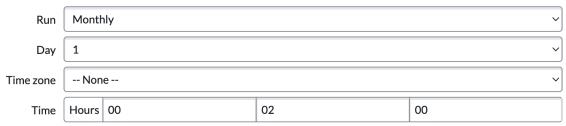
A SSC (ServiceNow Security Center, Central de segurança da ServiceNow) é uma aplicação de segurança que consiste em um conjunto de ferramentas criadas para ajudar as

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

organizações a suas implantações da ServiceNow seguras. Usando a SSC, as organizações podem aprimorar sua postura de segurança, reforçar seus níveis de conformidade e fazer tudo isso com uma experiência do usuário ininterrupta.

Use este documento para aprender sobre os aprimoramentos de funcionalidade da SSC e a executar tarefas na SSC que, antes, eram feitas na ISC.

Proteção de segurança

Aprimoramentos do recurso	ISC vs SSC
Atualizações das interações do usuário	• Revise a pontuação mais recente navegando até "Visão geral" ou a página de comparação de proteção. • Atualize manualmente a pontuação mais recente navegando até "Visão geral" e selecionando "Atualizar pontuação". • Mude a configuração de segurança selecionando o link de um nome de configuração em qualquer uma dessas páginas e, em seguida, faça edições na página **Detalhes de configurações**: ◦ Visão geral ◦ **"Proteção"** > **"Todas as configurações"** ◦ **"Proteção"** > **"Comparação"**
Definir um cronograma para recalcular sua pontuação de conformidade	Usando a SSC, é possível definir quando o sistema atualizará sua pontuação de conformidade: **1.** Navegue até a tabela "Execuções de script agendadas" [sysauto_script]. **2.** Localize e abra o registro `SC - Calcular conformidade mensalmente`. **3.** Use os campos **Executar**, **Dia**, **Fuso horário** e **Hora** para definir seu cronograma preferencial.  **4.** Selecione **Atualizar** para salvar suas mudanças.

KPIs e métricas de segurança

Aprimoramentos do recurso	ISC vs SSC
Melhorias dos KPIs	Usando a SCC, é possível: • Ver a tendência da pontuação ao longo do tempo. • Monitorar todos os KPIs e métricas usando a mesma interface e recursos analíticos.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países. Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Aprimoramentos do recurso	ISC vs SSC
Melhorias das métricas	A SCC inclui estas melhorias de métricas: • Adição de mais de 65 métricas. • Monitoramento e análise de KPIs e métricas em uma só interface do usuário. • Criação de metas e limites para as métricas.
Atualizações das interações do usuário	Acesse "Métricas" na SSC navegando até **Visão geral** > **Métricas**e selecionando a métrica no menu de navegação. Como alternativa, você pode navegar até **"Todas as métricas"**.

Security Scanner

Aprimoramentos do recurso	ISC vs SSC
Novo recurso	A SCC inclui estas funções: • Execute varreduras manualmente ou programe-as para serem executadas em horários específicos. • Crie suas próprias verificações de varredura. • Crie seu próprio pacote de varredura. • Compare os resultados de duas varreduras.
Aprimorar a funcionalidade do e-mail	Configure notificações por e-mail para se manter informado sobre eventos de segurança em sua instância.
Atualizações das interações do usuário	• Para executar a varredura de Auditor, navegue até **Visão geral** > **Varredura** > **Pacotes** e selecione **Pacote de auditor** na lista. • Para ver os resultados da varredura, navegue até **Visão geral** > **Varredura** > **Resultados**.

Recursos extras de segurança

Aprimoramentos do recurso	ISC vs SSC
Recurso de monitoramento de sessões	• Visualize as atividades da sessão usando o Hub de análise. • Monitore a atividade da sessão navegando até **Métricas** > **Sessões**.
Encontrar recursos	Acesse todos os recursos de aprendizado em uma só página em **Visão geral** > **Aprendizado**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Monitorar eventos de segurança

Analise as métricas de evento em sua instância para que você possa identificar e evitar possíveis eventos de segurança.

Importante:

A Central de segurança da instância (ISC) atingiu o fim das vendas em setembro de 2024 e não é mais compatível ou disponível para nova ativação.

A SSC (ServiceNow Security Center, Central de segurança da ServiceNow) é a solução recomendada no futuro. Para obter mais informações, consulte Migração da Central de segurança da instância para a ServiceNow Security Center.

Na faixa de opções de eventos, que está na página inicial de Segurança da instância, você pode analisar essas métricas e os detalhes que as acompanham para identificar possíveis eventos de segurança na instância.

- Para cada métrica de evento, uma contagem de pontuação única em tempo real aparece, indicando quantas vezes o evento ocorreu durante o dia nesta instância. Esses relatórios de pontuação única são atualizados automaticamente conforme os eventos correspondentes ocorrem.
- Cada métrica de evento também contém tendências de conformidade e informações de gráfico em um intervalo de datas. Essas informações são atualizadas diariamente quando você executa o trabalho de análise de desempenho. Para saber mais, consulte a seção **Analisar detalhe de tendência de evento**.

Tipos de eventos

Você pode monitorar pelo menos seis dos seguintes tipos de eventos. Para mais de seis eventos, use as setas para a esquerda ou para a direita abaixo da faixa de opções de eventos para rolar por eles. Para saber como configurar a faixa de opções de eventos, consulte Configurar a faixa de opções de eventos de segurança.

Preferência de notificação	Descrição
Logins de Administrador	Número de tentativas de login nesta instância, durante o dia do calendário, por usuários que têm uma função de administrador atribuída.
Usuários Administradores Adicionados	Número de usuários com função de administrador que foram adicionados a esta instância durante o dia do calendário. Por exemplo, sua instância pode ter um problema de segurança se a contagem for 10, mas 4 usuários são conhecidos por terem uma função de administrador atribuída.
E-mails de Entrada Externos	Para saber mais, consulte Métricas de e-mail.
Logins Externos	Número de usuários com uma função snc_external atribuída que fizeram login nesta instância durante o dia do calendário. Esses logins normalmente ocorrem para fins de manutenção, suporte, consultoria ou auditoria. O monitoramento desta métrica

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Preferência de notificação	Descrição
	permite que você verifique se as tentativas de login externo são legítimas e não são possíveis problemas de segurança. Para saber mais sobre como atribuir funções de usuário externo, consulte Funções explícitas.
Logins com falha	Número de tentativas de login que falharam nesta instância durante o dia do calendário. Esta métrica pode indicar que estão sendo feitas tentativas de fazer login e comprometem a segurança da instância.
Representações	Número de logins de representação nesta instância durante o dia do calendário. Para saber mais sobre como representar usuários, consulte Representar um usuário.
Arquivos em quarentena	Número de arquivos que foram colocados em quarentena quando você executou o Varredura antivírus nesta instância durante o dia do calendário. Para saber mais sobre arquivos em quarentena e o Varredura antivírus, consulte Métricas de antivírus e Varredura antivírus.
Elevações de Segurança	Número de vezes que um administrador de segurança elevou a segurança para usuários padrão, alterando sua função de usuário atribuída para uma função de segurança de alto privilégio durante o dia do calendário. Essas funções de segurança de alto privilégio incluem oauth_admin, admin, security_admin e representante. • Esta métrica indica que alguém pode ter tentado elevar a segurança de um usuário não autorizado. Não use esta métrica por si só para detectar um comprometimento de segurança específico. Em vez disso, trate esta métrica como uma indicação de que você deve verificar outra métrica para ver se ocorreu um comprometimento da segurança. • Para saber mais sobre como elevar a segurança do usuário, consulte Elevação para uma função privilegiada e Funções de privilégio elevado.
Logins SNC	Número de funcionários de Suporte e atendimento ao cliente que fizeram login nesta instância usando a técnica de hi-hopping durante o dia do calendário Esses

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Preferência de notificação	Descrição
	logins normalmente ocorrem para fins de manutenção, suporte, consultoria ou auditoria. Para obter informações sobre como controlar o acesso de funcionários corporativos da ServiceNow, consulte Controle de acesso da ServiceNow.
Spam	Para saber mais, consulte Métricas de e-mail.
E-mails Recebidos Confiáveis	Para saber mais, consulte Métricas de e-mail.
E-mails Recebidos Não Confiáveis	Para saber mais, consulte Métricas de e-mail.
Tipos de Vírus	Número de diferentes tipos de eventos de antivírus que ocorreram nesta instância durante o dia do calendário. Para saber mais sobre os tipos de evento de antivírus, consulte Métricas de antivírus.

Analisar detalhe de tendência de evento

Para exibir os detalhes da tendência de uma métrica de evento, clique na contagem de eventos para acessar a página do Hub de análise. Os detalhes que aparecem para a instância dependem do tipo de métrica.

Por exemplo, para exibir uma lista de cada tentativa com falha na página Logs de eventos do painel de segurança:

- Selecione a métrica **Logins com falha**.
- Na página Hub de análise, clique em **Mostrar registros**.
- Clique em uma das tentativas de login com falha.
- Os detalhes incluem o nome do usuário que tentou fazer login, o endereço IP e o nome da tabela que ele tentou acessar.

Você pode configurar gatilhos de limite de evento em Hub de análise para fornecer alertas quando um determinado evento ocorrer dentro de um intervalo de pontuações para um indicador. Você também pode definir metas que permitem visualizar a diferença entre a pontuação desejada e a pontuação real de um evento.

Por exemplo, você pode definir um limite de `10` para a métrica **Logins com falha**. Quando ocorrem dez ou mais tentativas de login com falha durante o dia, um alerta é enviado para a equipe de segurança específica. Você também pode definir um destino semelhante que forneça um destaque visual no Hub de análise quando ocorrerem 10 falhas de login durante um dia.

Os dados e os gráficos de tendência que aparecem no bloco da faixa de opções de evento e o Hub de análise são atualizados após a execução do trabalho de análise de desempenho às 2h hora local. Para saber mais, consulte Como a pontuação de Conformidade diária e os dados de tendência e do gráfico são atualizados.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Informações relacionadas

- Central de segurança da instância
- Now Intelligence
- Hub de análise
- Metas e limites do Performance Analytics

Configurar a faixa de opções de eventos de segurança

Configure a faixa de opções de evento de segurança na página inicial da Central de segurança da instância para incluir somente os eventos que são relevantes para rastrear a segurança da instância em suas operações. Você também pode mudar a ordem na qual os blocos de eventos de segurança aparecem na faixa de opções.

Antes de Iniciar

Função necessária: security_dashboard_user ou administrador

Por Que e Quando Desempenhar Esta Tarefa

A faixa de opções de eventos de segurança é preenchida inicialmente com um conjunto completo de eventos de segurança padrão. Você pode personalizá-la removendo os eventos que não são relevantes para a sua organização.

- Por exemplo, se você suspeitar que os problemas de segurança se devem às ações do pessoal interno, inclua os Logins de administrador, os Usuários administradores adicionados e os indicadores de evento de Elevações de segurança.
- Esses indicadores monitoram quantas vezes os usuários com funções de administrador tentaram fazer login e, se usuários administradores foram adicionados, quais tentativas foram feitas para elevar as funções de segurança.

Nota: Para saber mais sobre os tipos de eventos de segurança que aparecem na faixa de opções de eventos, consulte Monitorar eventos de segurança.

Procedimento

1. Navegue até **Todos** > **Segurança do sistema** > **Central de segurança da instância**.
2. Na faixa de opções do evento, clique em **Editar** (< > Edit).
   No formulário Editar eventos, a coluna **Selecionado** contém os eventos que já estão listados.
3. Para adicionar eventos de segurança à faixa de opções de eventos, mova-os da coluna **Disponível** para a coluna **Selecionado**.
   Para mudar a ordem em que os eventos aparecem na faixa de opções, selecione um evento e clique na seta para cima ou para baixo para movê-lo para a posição correta.
   - Coloque os eventos na mesma ordem sequencial em que devem aparecer na faixa de opções de eventos da Central de segurança da instância.
   - Os eventos que você coloca na parte superior da coluna **Disponível** aparecem sequencialmente, começando no lado esquerdo da faixa de opções de eventos da Central de segurança da instância. Os eventos colocados na parte inferior da coluna aparecem à direita na faixa de opções de eventos.
4. Para remover eventos de segurança da faixa de opções de eventos:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Na coluna **Selecionado**, selecione os eventos de segurança que você deseja remover da faixa de opções de eventos.
- Mova-os da coluna **Selecionado** para a coluna **Disponível**.

5. Clique em **Salvar**.

Informações relacionadas

Central de segurança da instância

Definir preferências para notificações de eventos de segurança

Configure preferências para os tipos de notificações que você deseja receber para ocorrências de eventos de segurança específicos. Para cada tipo, você determina se deseja receber notificações por e-mail, por notificação por push no Now Mobile ou em aplicações de envio de mensagens de terceiros, como Slack ou Microsoft Teams.

Antes de Iniciar

Para habilitar aplicações de envio de mensagens de terceiros para enviar notificações de eventos de segurança, você deve ativar o plug-in Notificações de envio de mensagens (com.glide.notification.messaging). Usuários individuais devem definir suas próprias configurações. Para obter detalhes, consulte Notificações em aplicações de envio de mensagens.

Função necessária: administrador.

Procedimento

1. Na página inicial da Central de segurança da instância, clique no menu do perfil e em **Preferências de notificação**.

Preferências de notificação

Preferência de notificação	Descrição
Login de administrador	Envie o tipo de notificação selecionado sempre que outros usuários com funções de administrador atribuídas fizerem login nesta instância a partir de um endereço IP diferente.
Desbloqueio de administrador	Envie o tipo de notificação selecionado sempre que uma conta de um usuário de privilégios altos tiver sido desbloqueada.
Falha de login	Envie o tipo selecionado de notificação sempre que outros usuários não conseguirem fazer login nesta instância em um número menor do que o de tentativas definido na propriedade *glide.user.max_unlock_attempts*. Se você não configurar esta propriedade, o valor padrão será 5. Para saber mais sobre esta propriedade, consulte Especificar bloqueio para tentativas de login com falha.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Preferência de notificação	Descrição
Função da HP adicionada	Envie o tipo de notificação selecionado sempre que uma função de segurança de alto privilégio (incluindo as funções oauth_admin, admin, security_admin e representante) for concedida a outro usuário. Para saber mais sobre como elevar a segurança do usuário, consulte Elevação para uma função privilegiada e Funções de privilégio elevado.
Representação	Envie o tipo de notificação selecionado sempre que outro usuário estiver representando você. Para saber mais sobre como representar usuários, consulte Representar um usuário.
Elevação de segurança	Envie o tipo de notificação selecionado sempre que outros usuários forem elevados a uma função de administrador de segurança nesta instância.
Resumo semanal	Envie um resumo semanal do tipo de notificação selecionado. Ele inclui: ◦ Um resumo de todas as atividades de segurança realizadas nesta instância ao longo da semana. ◦ A pontuação de conformidade diária atual da instância.

2. Para cada tipo de evento de segurança, marque as caixas de seleção apropriadas para designar o tipo de notificação a ser enviado a você.
Você pode selecionar vários métodos de notificação para cada um.

Caixa de seleção	Descrição
E-mail	Envie um e-mail para este tipo de evento de segurança.
Slack	Envie notificações para este tipo de evento de segurança por meio de Slack. **Nota:** Esta coluna aparecerá somente se você tiver configurado a integração de Slack para a Now Platform.
Equipes	Envie notificações para este evento de segurança por meio de Microsoft Teams.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Caixa de seleção	Descrição
	Nota: Esta coluna aparecerá somente se você tiver configurado a integração de Microsoft Teams para a Now Platform.
Envio por Push	Envie notificações por push em Now Mobile para esse tipo de evento de segurança. **Nota:** Esta coluna aparecerá somente se você fizer login em Now Mobile pela primeira vez.
Selecionar tudo	Selecione um tipo específico de notificação para todos os tipos de eventos de segurança. Por exemplo, clique em **Selecionar tudo** localizado acima de **E-mail** se quiser receber notificações por e-mail para cada tipo de evento de segurança.

3. Clique em **Salvar**.

Verificar a pontuação de conformidade diária e definir as configurações da propriedade de segurança

Revise a métrica de Pontuação de conformidade diária e as propriedades de configuração de segurança para ver se sua instância está em conformidade com os requisitos de segurança sugeridos. Você pode afetar a pontuação de conformidade diária atualizando as propriedades de segurança fora de conformidade na página Configurações de conformidade de proteção.

Importante:

A Central de segurança da instância (ISC) atingiu o fim das vendas em setembro de 2024 e não é mais compatível ou disponível para nova ativação.

A SSC (ServiceNow Security Center, Central de segurança da ServiceNow) é a solução recomendada no futuro. Para obter mais informações, consulte Migração da Central de segurança da instância para a ServiceNow Security Center.

A Pontuação de conformidade diária é uma pontuação percentual. É baseada no quanto as configurações atuais das propriedades de segurança de sua instância estão em conformidade com os valores de conformidade publicados em Configurações de proteção de segurança da instância.

Revise a pontuação de conformidade diária da sua instância regularmente. Siga estas diretrizes ao avaliar sua pontuação de conformidade diária:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Maior ou igual a 90% indica que a instância está em conformidade com os controles de segurança críticos.
- Maior ou igual a 50% e menor que 90% indica um nível moderado de conformidade de segurança.
- Menor que 50% indica um baixo nível de conformidade de segurança.

Ajuste as configurações de segurança da instância para aumentar a conformidade

Usando a página Configuração de conformidade de proteção, proteja e otimize as propriedades de segurança não compatíveis que afetam a pontuação de conformidade diária de sua instância. Seu uso garante que sua instância esteja em conformidade com os padrões de proteção de segurança publicados, ao mesmo tempo em que atende aos requisitos de segurança da sua empresa.

Antes de Iniciar

Função necessária: security_dashboard_user ou administrador.

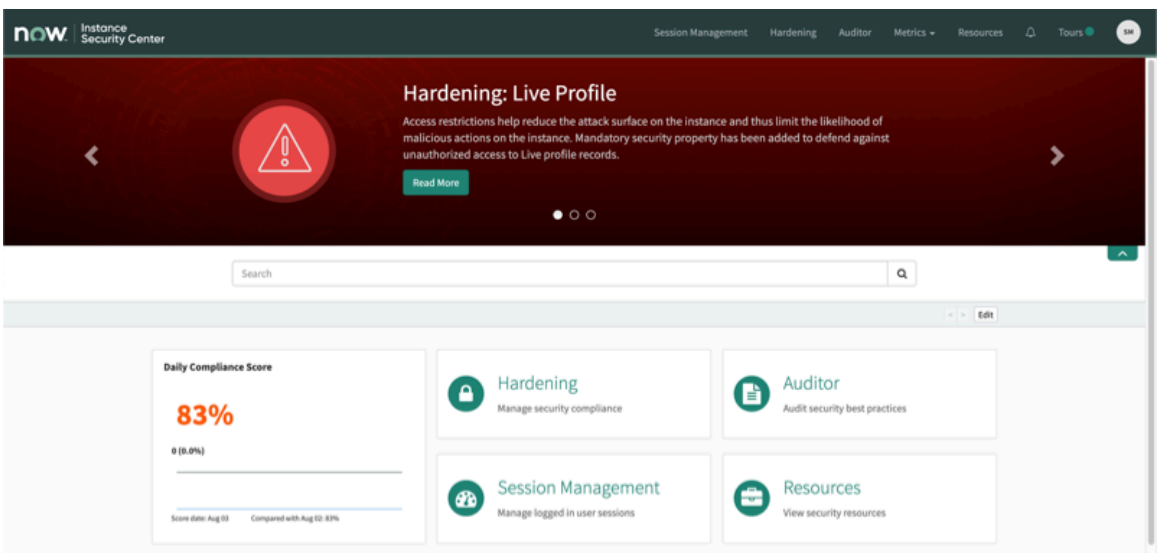
Consulte o conteúdo de Configurações de proteção de segurança da instância para obter descrições detalhadas e valores de conformidade para as propriedades do sistema relacionadas à segurança e plug-ins em Now Platform.

- Consulte as configurações de proteção de segurança da instância sempre que você definir ou atualizar propriedades relacionadas à segurança, mesmo que alguns dos valores de conformidade possam não ser adequados para sua instância.
- Ao atualizar essas propriedades, certifique-se de que a instância continua a se comportar conforme o esperado. Consulte o pessoal interno apropriado que tenha experiência para determinar os impactos na segurança.

Nota: Se você tiver uma função de administrador, poderá exibir e editar os controles de segurança. Se você tiver uma função security_dashboard_user, poderá exibir os controles de segurança, mas não poderá editá-los.

Procedimento

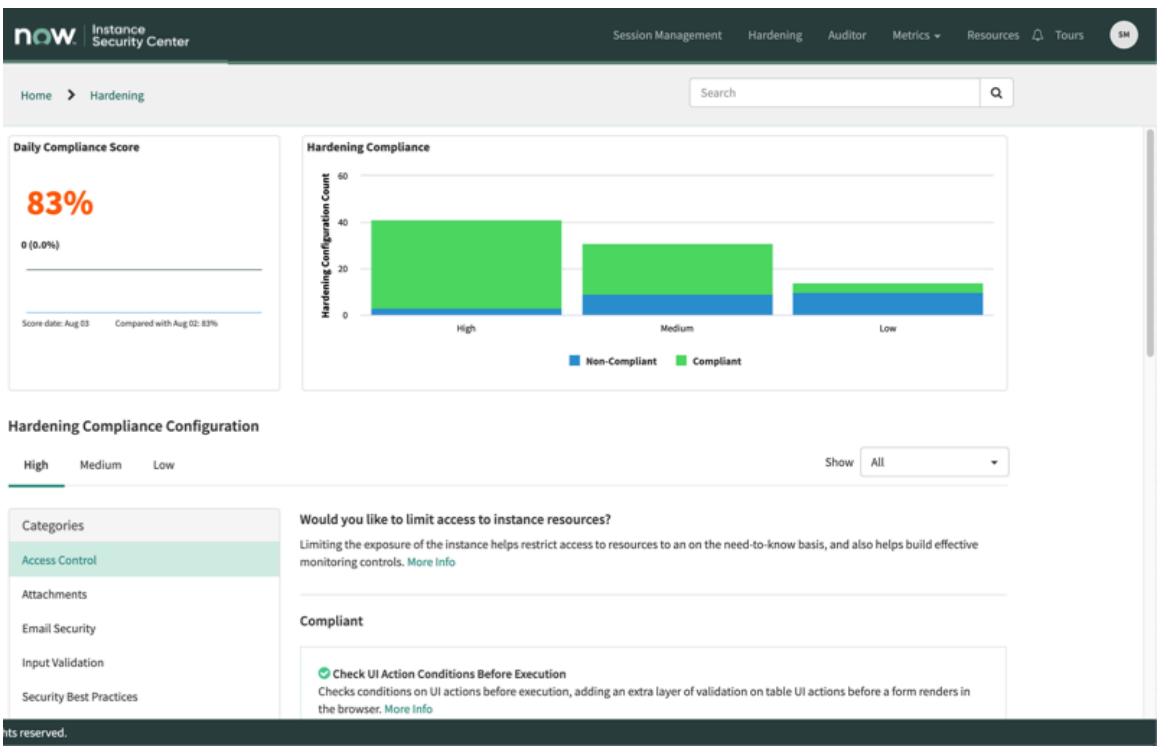
1. Navegue até **Todos** > **Segurança do sistema** > **Central de segurança da instância**.
2. Clique no bloco de **Pontuação de conformidade diária** ou no link **Proteção** para acessar a página de Configuração de conformidade de proteção.



© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. No gráfico de Conformidade de proteção, visualize as estatísticas das propriedades de configuração de segurança em conformidade e fora de conformidade.

Opção	Descrição
Conforme	Número de propriedades de configuração de segurança que estão em conformidade com os valores de conformidade nas Configurações de proteção da Segurança da instância. **Nota:** Não é possível alterar as configurações das propriedades de segurança compatíveis na Configuração de conformidade de proteção. Se quiser fazer isso, você deve atualizá-las em Propriedades do sistema. Para saber mais, consulte Adicionar uma pro-
Fora de Conformidade	Número de propriedades de configuração de segurança que não estão em conformidade com os valores de conformidade nas Configurações de proteção da Segurança da instância. Você pode atualizar as configurações de propriedades não compatíveis.

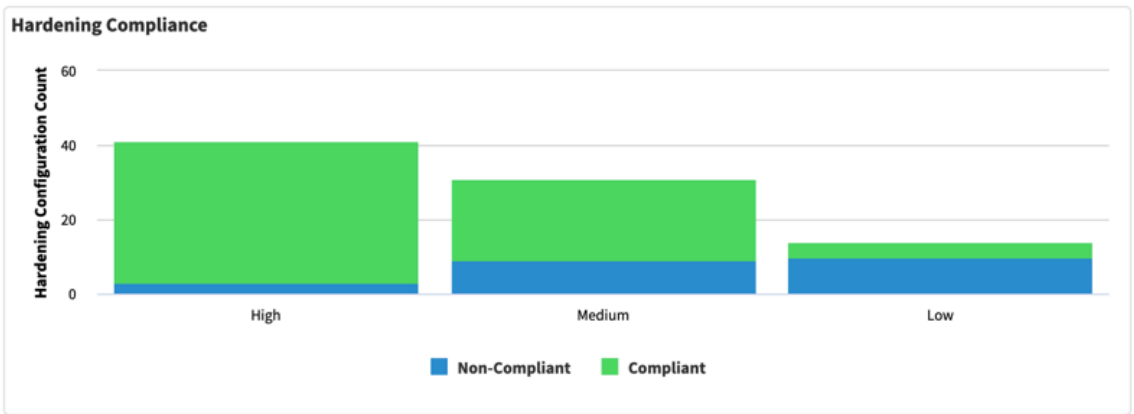


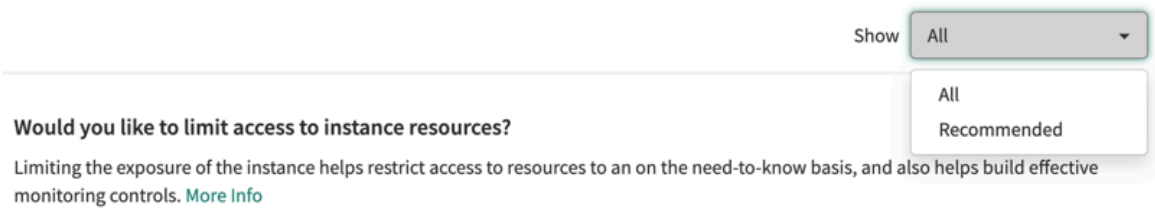
Nota: Para visualizar o número de pontuações de segurança em conformidade ou não em um intervalo de datas, mova o ponto azul no controle deslizante abaixo de Pontuação de conformidade diária.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Na lista **Mostrar**, abaixo do gráfico, especifique se deseja acessar todas as propriedades de configuração de segurança ou apenas as recomendadas.

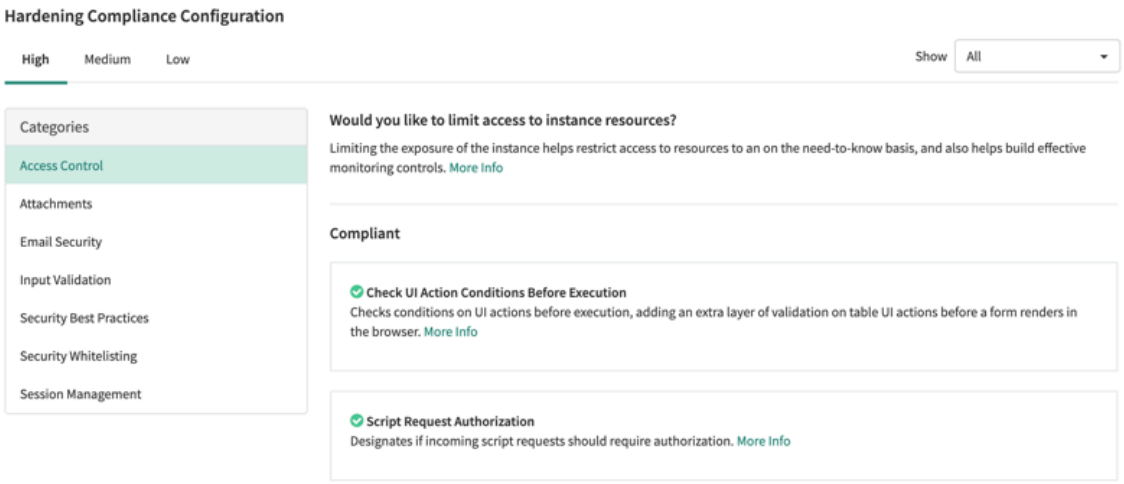
Opção	Descrição
Todos	(Padrão) Todas as propriedades de configuração de segurança em conformidade e fora de conformidade em cada categoria selecionada.
Recomendado	Somente as propriedades de configuração de segurança aparecerão em cada categoria selecionada. Essas propriedades de configuração de segurança são um subconjunto selecionado das mais críticas usadas para proteger o Now Platform. Considere essas propriedades de configuração de segurança como o número mínimo de configurações que você deve definir para proteger Now Platform. **Nota:** Para proteger totalmente sua instância, use a opção **Todos**. A opção contém também todas as propriedades de configuração de segurança recomendadas.





5. Em **Categorias**, selecione a categoria que contém as propriedades de configuração de segurança que você gostaria de acessar:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Opção	Descrição
Controle de Acesso	Os controles de acesso determinam se deve ser concedido ou negado o acesso do usuário a um recurso específico com base em quem tem permissão para usar os recursos. Para saber mais, consulte Controle de Acesso nas Configurações de proteção de segurança da instância.
Anexos	Os controles de segurança de anexo permitem a validação de anexos de entrada para proteger sua instância contra arquivos mal-intencionados enviados por invasores. Para saber mais, consulte Anexos nas Configurações de proteção de segurança da instância.
Segurança de e-mail	A segurança de e-mail abrange as propriedades de configuração de segurança que um administrador pode configurar para garantir que as políticas de segurança apropriadas estejam em vigor para todos os e-mails de entrada. Para saber mais, consulte Segurança de e-mail (proteção de segurança da instância) nas Configurações de proteção de segurança da instância.
Validação de entrada	A validação de entrada inclui propriedades relacionadas à segurança que um administrador pode configurar para minimizar a entrada de dados malformados, independentemente da origem. Para saber mais, consulte Validação de entrada nas Configurações de proteção de segurança da instância.
Comunicações seguras	Propriedades de comunicações seguras são as que um administrador pode configurar para proteger o transporte de tráfego HTTP. Para saber mais, consulte Comunica-

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	ções seguras nas Configurações de proteção de segurança da instância.
Práticas recomendadas de segurança	As práticas recomendadas de segurança abrangem tarefas de segurança que um administrador deve executar periodicamente, dentro de determinado intervalo de tempo e incluem propriedades de configuração relacionadas. Para saber mais, consulte Práticas recomendadas de segurança nas Configurações de proteção de segurança da instância.
Lista de inclusões de segurança	A lista de inclusões de segurança inclui propriedades relacionadas à segurança que um administrador pode configurar para restringir o comportamento a listagens de inclusão conhecidas. Para saber mais, consulte Lista de inclusões de segurança nas Configurações de proteção de segurança da instância
Gestão de sessões	Gerenciamento de sessão inclui propriedades relacionadas à segurança que um administrador pode configurar para garantir o gerenciamento seguro da sessão em Now Platform. Para saber mais, consulte Gestão de sessões nas Configurações de proteção de segurança da instância

6. Configure as propriedades de segurança que estão fora de conformidade na categoria selecionada.
   - A menos que seja especificado de outra forma, deslize o botão para mudar uma propriedade de segurança para a configuração recomendada. Por exemplo, a maioria dos controles é definida como verdadeiro ou falso, mas alguns exigem a entrada de um valor, ou valores, como uma lista de valores separados por vírgula.
   - Para acessar o tópico dedicado Configurações de Proteção de Segurança da Instância do controle de segurança e saber mais sobre ele, clique em **Mais informações**.

Resultados

A pontuação diária de conformidade aumenta ou diminui dependendo das mudanças que são feitas que fazem com que as configurações de controle de segurança que estão fora de conformidade.

Informações relacionadas

Central de segurança da instância

Como a pontuação de Conformidade diária e os dados de tendência e do gráfico são atualizados

Os dados de tendências e gráficos na Central de segurança da instância são atualizados depois que o trabalho de análise da performance é executado às 2h, horário local. Isso aparece no bloco de Pontuação de conformidade diária, nos blocos da faixa de opções de Evento e nos detalhes da página Hub de análise quando você clica em um dos blocos de evento.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O trabalho da Gestão de dados diários [AppSec] é um trabalho agendado regularmente que é executado todas as noites e realiza as seguintes tarefas:

1. Verifica se usuários válidos foram atribuídos aos trabalhos da Gestão de dados diários [AppSec] e Coleta de dados diários [PA AppSec] ao programá-los pela primeira vez.
   - Se você inseriu um usuário válido no campo **Executar como**, o trabalho continuará sendo processado. Um usuário válido é aquele que não está bloqueado na instância e tem uma função de administrador atribuída.
   - Se você inseriu um usuário inválido, uma mensagem de erro será exibida acima da faixa de segurança rotativa na Central de segurança da instância.

     Nota: Para saber mais sobre como atualizar o usuário atribuído ao executar trabalhos agendados, consulte Criar ou programar um trabalho de coleta de dados.

2. Executa a lógica de negócios para definir o estado de conformidade das propriedades de segurança que você configura na página Configuração de conformidade de proteção. Para saber mais, consulte Verificar a pontuação de conformidade diária e definir as configurações da propriedade de segurança.
3. Executa o trabalho de Análise de desempenho de Coleta de dados diários [PA AppSec] para coletar dados de conformidade e atualizar a pontuação de conformidade diária.

Atualização manual da Pontuação de conformidade diária

Como alternativa, se você tiver uma função de administrador atribuída, poderá atualizar e recalcular a Pontuação de conformidade diária a qualquer momento clicando em **Atualizar**.

Nota: O botão **Atualizar** não aparece para usuários com uma função security_dashboard_user atribuída.

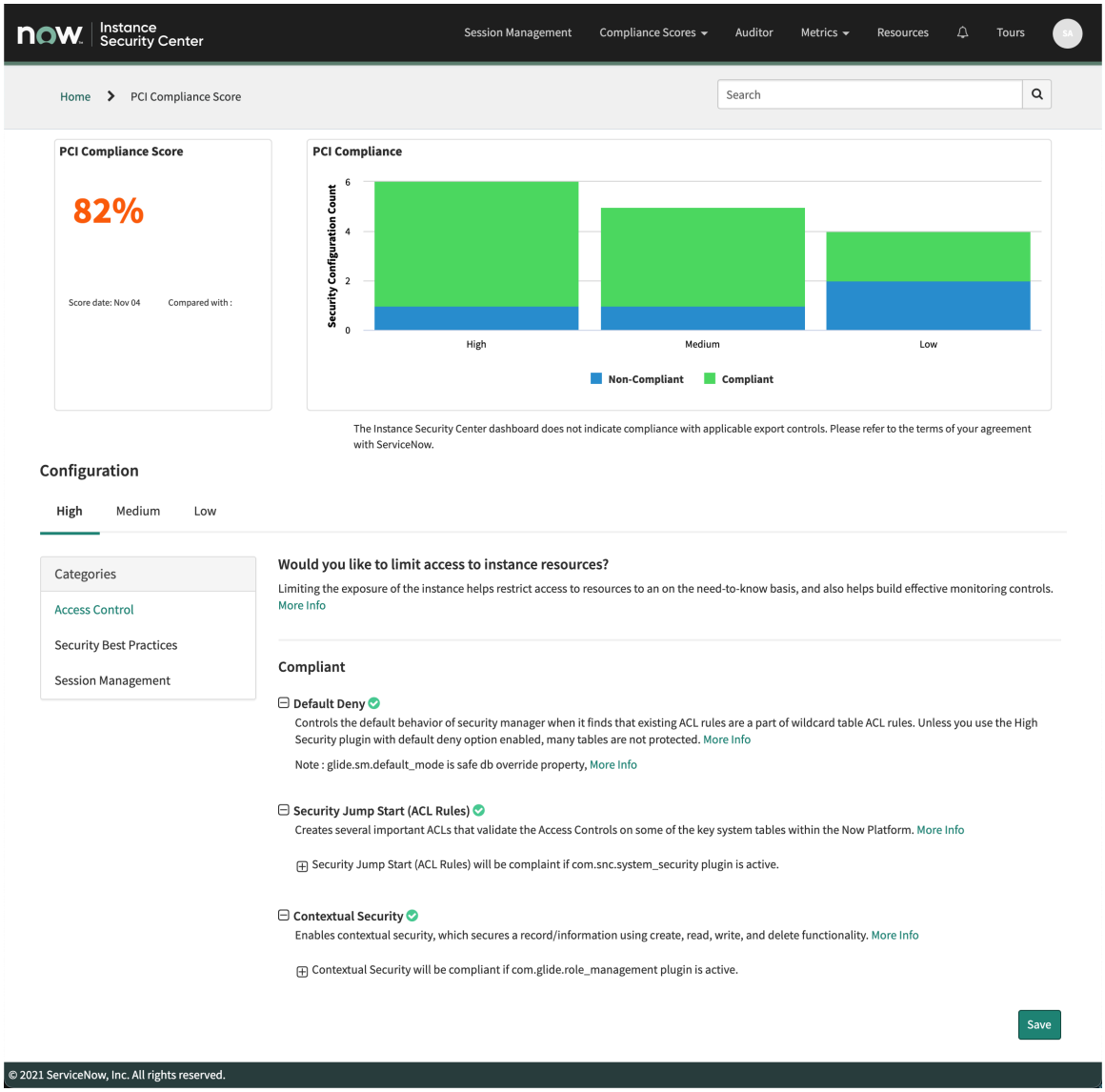
- A função Atualizar executa as mesmas tarefas que o trabalho de Análise de desempenho de Coleta de dados diários, mas o faz em tempo real, em vez de em um processo em lote.
- Você normalmente o usa quando deseja executar atualizações na Pontuação de conformidade diária para exibir imediatamente o impacto das atividades de segurança da instância.
- Pode haver um pequeno atraso antes que a pontuação atualizada seja exibida.

Nota: Quando você executa um upgrade (por exemplo, de London para Xanadu), o plug-in Central de segurança da instância (ISC) é ativado automaticamente. Um script de correção fornecido atribui automaticamente um usuário personalizado sem funções atribuídas.

Painel de pontuação de conformidade de PCI

O painel de pontuação de conformidade de PCI mostra como sua instância está em conformidade com os padrões de segurança do PCI (payment card industry, setor de cartão de pagamento). Use o painel para exibir sua pontuação de conformidade e modificar sua configuração para melhorar a segurança.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Funções necessárias de Now Platform

security_dashboard_user ou admin, necessário para exibir o painel de pontuação de conformidade de PCI.

Acessar o painel de pontuação de conformidade de PCI

Para abrir o painel, navegue até **Segurança do sistema** > **Central de segurança da instância**. na Central de segurança da instância, clique em **Pontuações de conformidade** no cabeçalho e selecione **Pontuação de conformidade de PCI**.

Casos de uso

Para obter exemplos de como diferentes pessoas de sua organização podem usar este painel, consulte estes casos de uso.

Usuário	Uso do painel
Usuário do painel de segurança (security_dashboard_user)	Monitore e gerencie continuamente a conformidade da Segurança da instância.

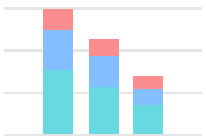
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Usuário	Uso do painel
Administrador (administrador)	Monitore continuamente a conformidade da Segurança da instância para detectar e responder a ameaças à segurança.

Indicadores

Indicador	Descrição
Pontuação de conformidade de PCI	Exibe a pontuação de conformidade da sua instância como uma porcentagem. Esta porcentagem de representa a porcentagem de configurações de segurança em sua instância que atendem aos padrões de conformidade. O indicador também exibe a data em que a pontuação de conformidade foi calculada e uma comparação com a pontuação calculada anteriormente.

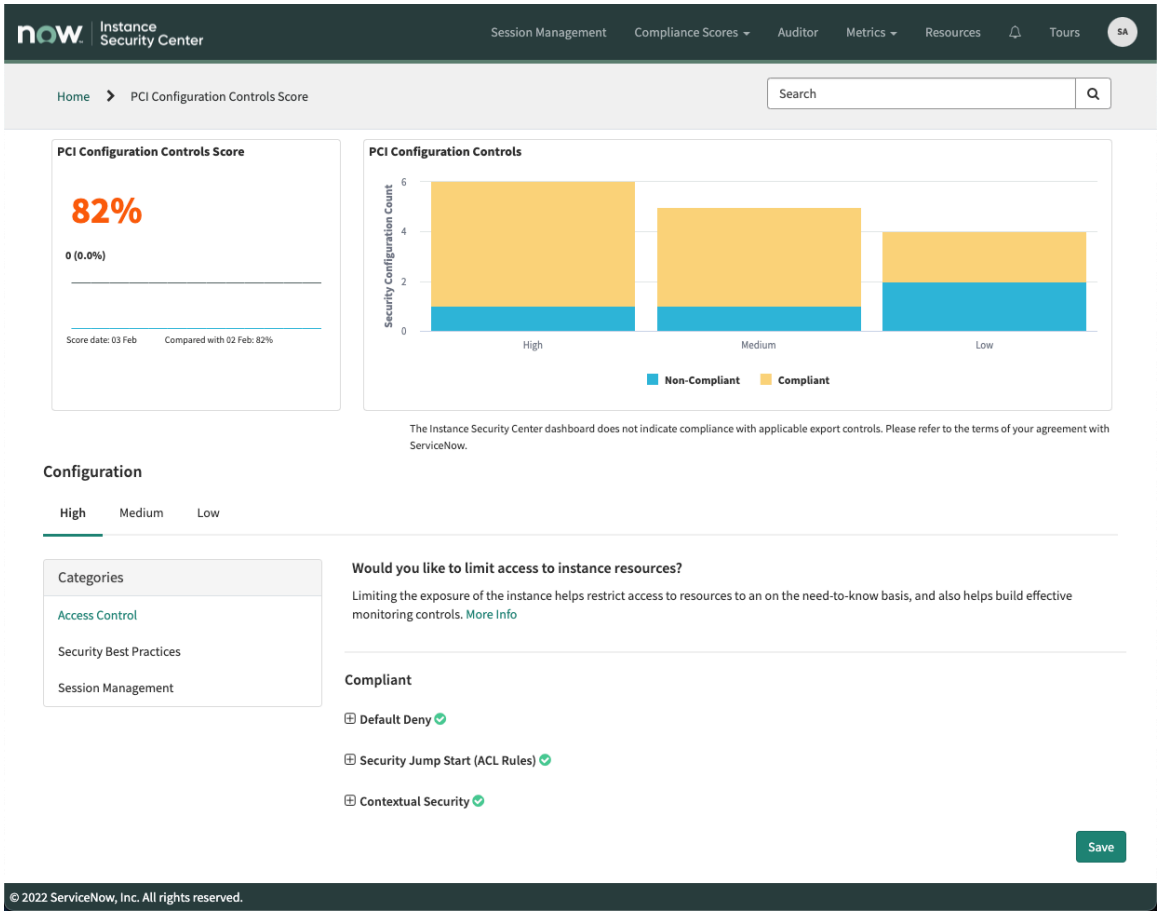
Visualização de dados

Título	Tipo	Tabela de origem	Descrição
Conformidade de PCI	 Gráfico de barras empilhadas	Configurações de segurança [isc_security_configurations]	Exibe configurações de segurança compatíveis e não compatíveis nas categorias alta, média e baixa. Clique em uma área do relatório para exibir as configurações de segurança correspondentes.

Painel de pontuação de controles de configuração de PCI

Use o painel de pontuação de controles de configuração de PCI para revisar sua configuração de PCI e determinar quais verificações de segurança não estão em conformidade. Você pode mudar a configuração das verificações de segurança fora de conformidade da Central de segurança da instância.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Funções necessárias de Now Platform

A função security_dashboard_user ou admin é necessária para visualizar o painel de pontuação de conformidade de PCI.

Acessar o painel de pontuação de controles de configuração de PCI

Para abrir o painel, navegue até **Segurança do sistema** > **Central de segurança da instância**. na Central de segurança da instância, clique em **Pontuações de conformidade** no cabeçalho e selecione **Pontuação de controles de configuração de PCI**.

Casos de uso

Para obter exemplos de como diferentes pessoas de sua organização podem usar este painel, consulte estes casos de uso.

Usuário	Uso do painel
Usuário do painel de segurança (security_dashboard_user)	Monitore e gerencie continuamente a conformidade dos controles de configuração de PCI em sua instância. Modifique a configuração de PCI para garantir a conformidade e melhorar a segurança da instância.
Administrador (administrador)	Monitore continuamente a conformidade dos controles de configuração de PCI para

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

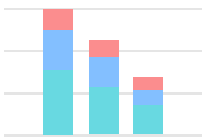
Usuário	Uso do painel
	detectar e responder a possíveis ameaças à segurança.

Indicadores

Pontuação de controles de configuração de PCI

Exibe a pontuação dos controles de configuração de PCI da sua instância como uma porcentagem. Essa porcentagem representa a porcentagem de configurações de controle de PCI de segurança na sua instância que atendem aos padrões de conformidade. O indicador também exibe a data em que a pontuação de conformidade foi calculada e uma comparação com a pontuação calculada anteriormente.

Visualização de dados

Título	Tipo	Tabela de origem	Descrição
Controles de configuração de PCI	 Gráfico de barras empilhadas	Configurações de segurança [isc_security_configurations]	Exibe configurações de controle de PCI compatíveis e não compatíveis nas categorias alta, média e baixa. Clique em uma área do relatório para exibir as configurações de segurança correspondentes.

Verificar se há definições de segurança incorretas

Execute o Auditor para verificar sua instância e encontrar definições de segurança incorretas. Ele fornece descobertas que você pode corrigir para ajudar a melhorar a postura de segurança da sua instância.

Importante:

A Central de segurança da instância (ISC) atingiu o fim das vendas em setembro de 2024 e não é mais compatível ou disponível para nova ativação.

A SSC (ServiceNow Security Center, Central de segurança da ServiceNow) é a solução recomendada no futuro. Para obter mais informações, consulte Migração da Central de segurança da instância para a ServiceNow Security Center.

O Auditor realiza uma avaliação de "corpo todo" da integridade da instância que analisa a configuração do sistema. Para verificações de segurança, ele compara sua configuração de segurança atual com as definições de práticas recomendadas e com os valores de conformidade da propriedade de segurança.

Do ponto de vista de segurança da instância, ele fornece informações e recomendações sobre o que você deve continuar fazendo e onde pode melhorar. Essas informações e recomendações ajudam a responder às seguintes perguntas:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- As propriedades relacionadas à segurança apropriadas estão definidas?
- O plug-in High Security está habilitado?
- Existem as regras de controle de acesso corretas?

Executar o Auditor e analisar os resultados da verificação

1. Para executar o Auditor, clique em **Auditoria** na página inicial da Central de segurança da instância.
2. Quando terminar, abra os resultados da verificação para revisar e analisar as descobertas de segurança.
3. Para revisar os detalhes de um resultado de verificação específico, clique duas vezes no número do resultado. Essas informações incluem seu status, tipo de verificação, tempo de execução e mensagens de erro.
4. Cada uma das descobertas do Auditor contém detalhes de resolução e um URL para o conteúdo do produto sobre como resolvê-los. Siga as diretrizes documentadas para resolver os problemas em cada uma das descobertas.

Informações relacionadas

Configurações de proteção de segurança da instância

Plug-in High Security

Regras da lista de controle de acesso

Monitorar métricas de instância

Monitore métricas de usuário, exportação, autenticação, e-mail e antivírus para sua instância. Por exemplo, você pode monitorar sua segurança de e-mail verificando as métricas de spam, e-mails externos e e-mails de entrada de domínios não confiáveis e confiáveis para sua instância. Analise essas métricas para procurar comportamentos anormais de segurança relacionados a atividades que ocorrem em sua instância.

Importante:

A Central de segurança da instância (ISC) atingiu o fim das vendas em setembro de 2024 e não é mais compatível ou disponível para nova ativação.

A SSC (ServiceNow Security Center, Central de segurança da ServiceNow) é a solução recomendada no futuro. Para obter mais informações, consulte Migração da Central de segurança da instância para a ServiceNow Security Center.

Métricas do usuário

Analise as métricas do usuário para procurar comportamentos anômalos relacionados a tipos específicos de atividade do usuário em sua instância.

Não conectado no último mês/nos últimos seis meses/no último ano

Indica o número de usuários que não fizeram login na instância no último mês, nos últimos seis meses e no último ano civil. Para exibir detalhes do usuário para uma métrica específica:

- Clique na métrica para exibir uma lista de usuários que não fizeram login na instância durante o período de tempo indicado.
- Clique em um nome de usuário para exibir mais detalhes sobre ele.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Usuários com funções de alto privilégio

Indica o número de usuários com os seguintes tipos de função de privilégio alto:

Função do usuário	Descrição
admin	Função de administrador primário que tem acesso a todos os recursos, funções e dados do sistema, independentemente das restrições de segurança.
ais_high_security_admin	Função de privilégio elevado que permite ao usuário acessar as configurações de Alta segurança para Pesquisa com IA. Para saber mais, consulte Atribuir funções a administradores e usuários do Pesquisa com IA.
password_reset_admin	Função de administrador que permite ao usuário exibir o status das atividades de redefinição de senha, identificar possíveis ameaças à segurança e monitorar a conformidade com as políticas de segurança de senha. Para saber mais, consulte Redefinição de senha e Relatórios e registros em log de mudança de senha.
script_include_admin	Função de administrador que também tem acesso a inclusões de script.
security_admin	Função de privilégio elevado que permite ao usuário criar e alterar controles de acesso e configurações de Alta segurança. Para saber mais, consulte Função security_admin..
user_admin	Função de administrador que também pode gerenciar usuários, funções, grupos de usuários, funções e atribuições de departamento.

Nota: Para saber mais sobre esses tipos de funções administrativas, consulte Funções administrativas especiais.

Para exibir detalhes do usuário para uma métrica de função do usuário específica:

- Clique na métrica de função de contagem de usuários para exibir uma lista de usuários com esse tipo de função de alto privilégio.
- Clique em um nome de usuário para exibir mais detalhes sobre ele. Você pode então determinar se essas funções críticas de segurança foram atribuídas ao pessoal apropriado.

Tendência de usuários

Mostra informações de tendência de contagem ao longo de um período para os seguintes tipos de usuários:

Tipo de contagem	Descrição
Usuários ativos	Número de usuários marcados como Ativos na instância.
Usuários inativos	Número de usuários marcados como Inativos na instância.
Bloqueado	Número de usuários que estão bloqueados fora da instância.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para exibir detalhes do usuário para uma contagem de usuário específica (por exemplo, Usuários bloqueados):

- Clique na métrica **Usuários bloqueados**.
- Na página Hub de análise, clique em **Mostrar registros**.
- Clique em um nome de usuário para exibir mais detalhes sobre ele. Você pode determinar se há um motivo pelo qual essa pessoa está bloqueada e corrigir a situação.

Tendência de eventos

Mostra informações de tendência de contagem para tipos específicos de eventos, durante um período de tempo:

Tipo de evento	Descrição
Login de administrador	Número de usuários com funções de administrador de privilégios altos que fizeram login em um dia específico.
Login externo	Número de usuários com uma função snc_external atribuída que fizeram login nesta instância durante o dia do calendário. Esses logins normalmente ocorrem para fins de manutenção, suporte, consultoria ou auditoria. O monitoramento desta métrica permite que você verifique se as tentativas de login externo são legítimas e não são possíveis problemas de segurança.
Falha de login	Número de tentativas de login com falha em um dia específico.
Representação	Número de usuários conectados em um dia específico que estão representando outros usuários.
Elevação de segurança	Número de vezes que um administrador de segurança elevou a segurança para usuários padrão, alterando sua função de usuário atribuída para uma função de segurança de alto privilégio durante o dia do calendário. Essas funções de segurança de alto privilégio incluem oauth_admin, admin, security_admin e representante.
Login SNC	Número de funcionários da Suporte e atendimento ao cliente que fizeram login nesta instância usando a técnica de hi-hopping durante um dia específico.

Para exibir os detalhes do usuário para uma contagem de eventos específica (por exemplo, Representação):

- Clique na métrica de contagem de usuário. A página Registros em log de eventos do painel de segurança lista os registros em log de eventos para esse tipo de evento.
- Clique em um nome de usuário para exibir mais detalhes sobre esse evento.

Informações relacionadas

Hub de análise

Métricas de exportação

Analise as métricas de exportação para ver quais dados são exportados com mais frequência e quais usuários exportam mais dados.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

1. Gráfico de exportação

   Cada relatório exibe o número de eventos de exportação por data, usando uma legenda codificada por cores para indicar quais usuários realizaram a exportação. Clique em uma seção colorida de uma coluna para ver a lista de registros de **Eventos de exportação** [isc_export_event] correspondentes a essa entrada.

2. Legenda do relatório

   A legenda na parte inferior do relatório indica quais cores identificam quais usuários ou tabelas.

3. Pop-up de visualização

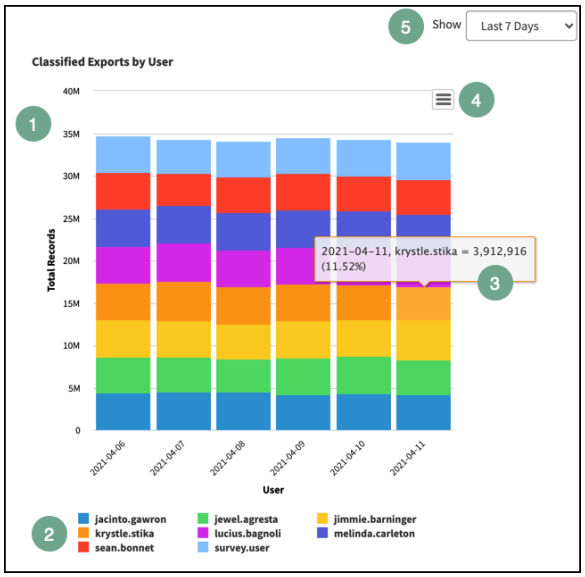
   Aponte para uma entrada no gráfico para ver uma visualização em pop-up. Esta visualização mostra o nome do usuário ou da tabela, bem como uma contagem de exportações e uma porcentagem do total nessa coluna.

4. Exportação de imagem

   Clique no ícone para salvar o relatório como uma imagem. Você pode salvar o relatório no formato PNG ou JPEG.

5. Intervalo de datas do relatório

   Use a lista **Exibir** para exibir as exportações nas últimas 24 horas ou nos últimos 7 dias.



Relatórios de métricas de exportação

A página de métricas de exportação exibe quatro relatórios.

Exportações por usuário

Use o relatório **Exportações por usuário** para ver quais usuários estão exportando a maioria dos dados.

Exportações classificadas por usuário

Use o relatório **Exportações classificadas por usuário** para ver quais usuários estão exportando a maioria das classificações correspondentes de dados, como informações confidenciais, restritas ou pessoais. Os administradores podem definir quais classificações este relatório usa na guia **Configurações**.

Exportações por tabela

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Use o relatório **Exportações por tabela** para ver quais tabelas são exportadas com mais frequência.

Exportações classificadas por tabela

Use o relatório **Exportações classificadas por tabela** para ver de quais tabelas são exportadas com mais frequência que correspondem a classificações como informações confidenciais, restritas ou pessoais com mais frequência. Os administradores podem definir quais classificações este relatório usa na guia **Configurações**.

Nota: Os relatórios de métrica de exportação rastreiam somente os eventos de exportação. As exportações de outras origens, como REST APIs ou fluxos de trabalho, não são rastreadas como parte deste recurso.

Configurações de métricas de exportação

Use as opções de configuração na guia Configurações para restringir os resultados de emissão de relatórios.

Acesse as configurações das suas métricas de exportação clicando na guia **Configurações**.

Campos de ajuste de configurações

Configurações de métricas de exportação

Configuração	Descrição
Classificações de métricas	Adicione classificações a este campo ou as remova para determinar quais exportações estão incluídas nos relatórios **Exportações classificadas por usuário** e **Exportações classificadas por tabela**. Esses relatórios são compatíveis com as seguintes classificações: • Informações de identificação pessoal • Confidencial • Restrito • Interno • Público(a) Para obter mais detalhes sobre classificações de dados, consulte Classificações de dados.
Classificações de alertas	Adicione ou remova classificações deste campo para determinar quais exportações acionam notificações de segurança de instância. As classificações compatíveis com o campo **Classificações para métricas** são compatíveis aqui. Para obter mais detalhes sobre esses alertas, consulte a seção de notificações de segurança na página Central de segurança da instância. O campo **Limite de registro** define o número de registros exportados antes de sua instância ser acionada e alertada.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configurações de métricas de exportação

Configuração	Descrição
Limite de registro	Número de registros que um usuário deve exportar para acionar um alerta. Para acionar um alerta, esses registros também devem corresponder às classificações listadas no campo **Classificações de alertas**.

Use o botão **Salvar (⌘ + s)** para salvar suas configurações.

Métricas de autenticação

Analise as métricas de autenticação para ver informações relacionadas à autenticação, como endereços IP usados com pouca frequência, logins com falha e tipos de esquemas de autenticação usados por seus usuários.

Use a página **Métricas de autenticação** para exibir relatórios relacionados à sua configuração de autenticação. Os relatórios a seguir são exibidos nesta guia.

Nota: A página de métricas de autenticação requer o plug-in **REST API Access Policy** (com.glide.rest.policy). Para obter mais detalhes sobre este recurso, consulte Políticas de acesso da REST API.

APIs sem políticas de autenticação

Exibe uma contagem em tempo real de todas as APIs sem uma política de acesso

Proteção: fluxo de recuperação de conta

Proteção: configuração relacionada ao recurso da MFA baseado em função

Contas do serviço da Web somente de acesso

Mostra a contagem de todos os registros do usuário com a opção de acesso ao serviço da Web habilitada na tabela *User* [sys_user].

Certificados X509 que expiram em 30 dias

Exibe uma contagem de todos os certificados X.509 da tabela *X.509 Certificates* [sys_certificate] que expiram em 30 dias.

Métricas de autenticação adaptável

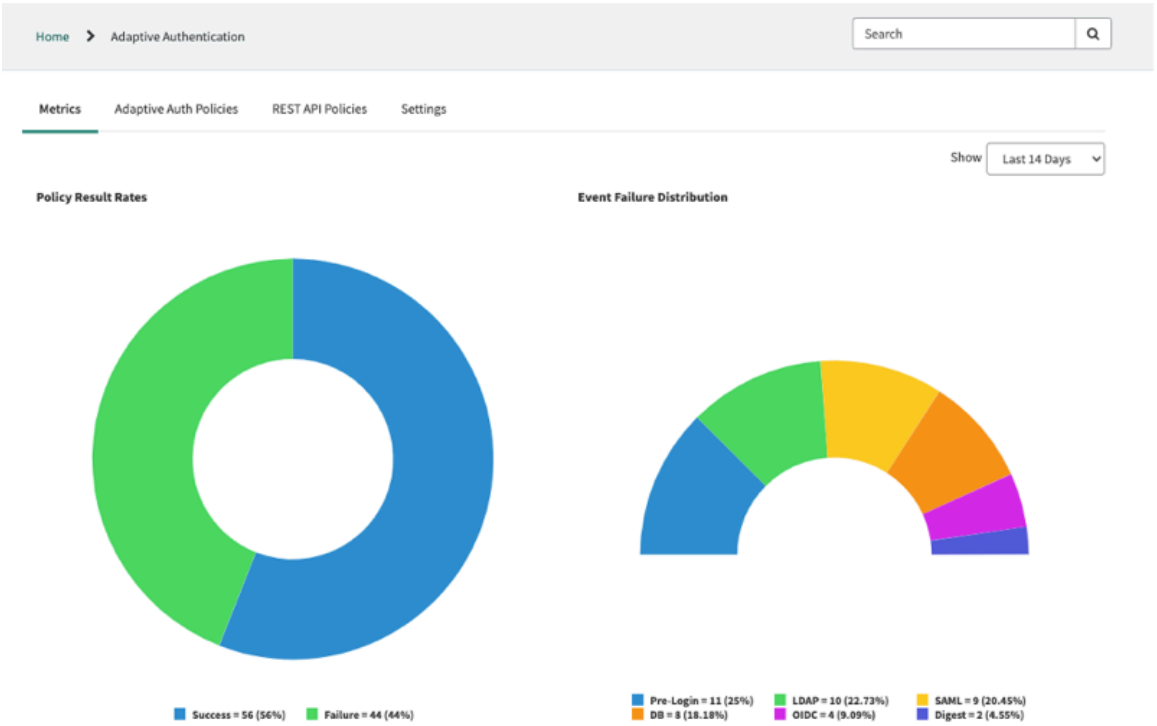
Analise as métricas de autenticação adaptável para monitorar e adicionar informações sobre como a autenticação adaptável está sendo usada em sua instância.

Exiba relatórios, configurações e políticas associadas à autenticação adaptável no local usando a página de métricas de autenticação adaptável. Os administradores de segurança podem usar relatórios para monitorar os resultados de suas políticas de autenticação adaptável. Use esses dados para obter informações e adaptar suas políticas para melhorar o desempenho.

Nota: A página de métricas de autenticação adaptável requer o plug-in **Adaptive Authentication** (com.snc.adaptive_authentication). Para obter mais detalhes sobre este recurso, consulte Autenticação adaptável.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Métricas



Use a guia **Métricas** para exibir relatórios relacionados à sua configuração de autenticação adaptável. Os relatórios a seguir são exibidos nesta guia.

- Taxas de resultados da política
- Distribuição de falha do evento
- Distribuição de sucesso do evento
- Endereços IP negados
- Logins de usuários de autenticação
- Logins de usuário de API
- Tendência de autenticação

Use a lista **Exibir** para selecionar um período de tempo para os relatórios exibidos

Políticas de autenticação adaptável

Use a guia **Políticas de autenticação adaptável** para exibir as políticas de autenticação adaptável e os contextos da política em sua instância. Clique em qualquer entrada dessas listas para exibir o registro associado. Para obter mais detalhes sobre estes registros, consulte Autenticação adaptável.

Configurações

Use a guia de configurações para exibir e configurar as propriedades do sistema de autenticação adaptável. Para obter mais informações sobre essas propriedades, consulte Configurar propriedades de autenticação adaptável

Métricas de e-mail

Analise suas métricas de e-mail para procurar comportamentos anormais relacionados aos e-mails recebidos para sua instância. Por exemplo, se as métricas indicam um pico em e-

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

mails de spam de domínios específicos, você pode definir ações de entrada que impedem sua entrega para a instância.

Para cada métrica de e-mail, uma contagem aparece para cada tipo de e-mail que é entregue ou enviado para a instância durante o dia do calendário.

Preferência de notificação	Descrição
E-mails recebidos externos	Número de e-mails recebidos no dia do calendário que foram entregues à instância de domínios de e-mail externos. **Nota:** Os domínios de e-mail externos são os domínios que não estão listados na propriedade do sistema *security.list.internal.domains*, pois essa propriedade rastreia somente os domínios de e-mail internos. Para saber mais sobre essa propriedade, consulte Propriedades do sistema disponíveis.
Spam	Número de e-mails recebidos no dia do calendário que foram entregues à instância e marcados como spam. Um número que está fora de linha com as tendências históricas pode indicar que há tentativas de comprometer a Segurança da instância.
E-mails recebidos confiáveis	Número de e-mails recebidos na instância para o dia do calendário de domínios de e-mail designados como confiáveis.
E-mails Recebidos Não Confiáveis	Número de e-mails recebidos na instância para o dia do calendário de domínios de e-mail designados como não confiáveis. Você pode designar domínios de e-mail confiáveis ou não confiáveis no formulário Domínio não confiável e confiável para que possa rastrear os e-mails de entrada que são enviados por eles. Para saber como designar domínios de e-mail confiáveis ou não confiáveis, consulte Designar domínios de e-mail como não confiáveis ou confiáveis.

Depois de clicar em uma métrica de e-mail, você pode aprender sobre os possíveis problemas de segurança de e-mail em sua instância, clicando em um dos seguintes:

Comando	Descrição
Gráfico	Contagens de e-mail recebidos e tendências de contagem ao longo do tempo para o tipo de e-mail selecionado

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Comando	Descrição
	(spam, entrada externa, não confiável ou confiável).
Registros	Registros de e-mail individuais que comprometem a contagem diária do tipo de e-mail selecionado.
Mais informações	Informações adicionais para o tipo de e-mail selecionado.

Nota: As métricas de e-mail se aplicam somente aos e-mails recebidos para a instância. As métricas não se aplicam ao tráfego normal que é processado por meio de servidores de e-mail de toda a empresa. Para saber mais sobre como definir ações de entrada e como elas afetam o processamento de seus e-mails de entrada, consulte Ações de e-mails de entrada.

Designar domínios de e-mail como não confiáveis ou confiáveis

Designe domínios de e-mail específicos como não confiáveis ou confiáveis para que você possa monitorar as métricas de e-mails recebidos dessas origens em sua instância.

Antes de Iniciar

Função necessária: security_dashboard_user ou administrador

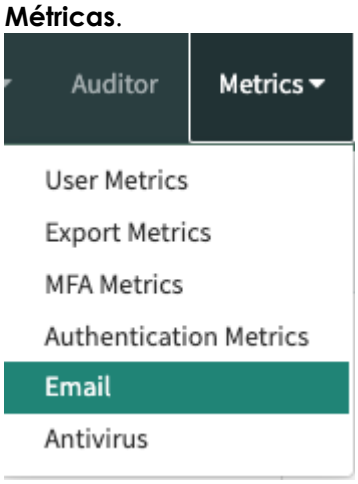
Por Que e Quando Desempenhar Esta Tarefa

Quando domínios não confiáveis ou confiáveis enviam e-mails para sua instância, suas contagens diárias aparecem nas métricas **E-mail recebido não confiável** ou **E-mail recebido confiável** na página E-mail. Você pode rastrear a atividade de e-mail desses domínios e usar logs de e-mail para exibir e-mails recebidos específicos. Você também pode especificar um usuário, geralmente um gerente ou um analista de segurança, para notificar sempre que ocorrer atividade no domínio não confiável ou confiável.

Nota: Designar um domínio de e-mail como não confiável serve somente para fins de rastreamento de segurança. Os administradores também podem configurar um filtro de endereço do sistema para ignorar e-mails de domínios não confiáveis. Para saber mais sobre como filtrar e-mails para bloquear a entrega, consulte Filtros de endereço do sistema.

Procedimento

1. Navegue até **Todos** > **Segurança do sistema** > **Central de segurança da instância**.
2. Na página inicial da Central de segurança da instância, selecione **E-mail** no menu **Métricas**.



© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Na página E-mail, na seção Domínios confiáveis e não confiáveis, clique em **Novo**.
4. No formulário, preencha os campos.

Formulário de domínio confiável e não confiável

Campo	Descrição
Domínio	Nome do domínio de e-mail que você está designando como não confiável ou confiável. Por exemplo, insira `servicenow.com/br/` para designar que os funcionários da ServiceNow podem enviar e-mails confiáveis para a instância.
Categoria	Categoria que indica se o domínio de e-mail é não confiável ou confiável: Não confiável Designa que o domínio de e-mail não é confiável. Você a usa para identificar domínios que enviam e-mails suspeitos ou que representam uma ameaça de segurança em potencial à instância. Confiável Designa que o domínio de e-mail é confiável. Você a usa para identificar domínios quando suas métricas indicam que os e-mails recebidos dele não representam ameaças à segurança. Designar o domínio como confiável permite que você rastreie sua atividade de e-mail de entrada ao longo do tempo.
Ativo	Marque a caixa para habilitar ou desabilitar o status não confiável ou confiável designado para o domínio de e-mail especificado.
Notify	Nome do usuário a ser notificado por e-mail quando ocorrer atividade no domínio confiável ou não confiável. Clique no ícone de pesquisa em destaque ( ) para pesquisar o nome do usuário. Deixe o campo **Notificar** em branco se você não quiser que as notificações sejam enviadas.

5. Selecione **Salvar**.

Resultados
As informações de domínio de e-mail confiável ou não confiável também são adicionadas à lista **Domínios não confiáveis e confiáveis** na página E-mail.

Informações relacionadas

Central de segurança da instância

Métricas de e-mail

Métricas de antivírus

Se o plug-in Varredura antivírus estiver ativado, Varredura antivírus será executado em sua instância para ajudar a protegê-la contra infecções de vírus de anexos.

As métricas a seguir aparecem para os últimos 60 dias de atividade e permitem que você avalie a eficácia das funções do Varredura antivírus.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Eventos de Antivírus

Eventos de antivírus indicam o número de eventos de antivírus em sua instância, por data. Para acessar os eventos de antivírus, navegue até **Segurança do sistema** > **Central de segurança da instância** e selecione a guia Métricas. As linhas do gráfico codificadas por cores representam os seguintes tipos de eventos de antivírus:

Cor	Descrição
Azul	Número de arquivos em quarentena por Varredura antivírus nesta instância para a data indicada.
Verde	Número de arquivos infectados baixados para a instância e colocados em quarentena na data indicada. Esses arquivos são principalmente anexos de e-mail que contêm um código de vírus ou invasor.
Amarelo	Número de arquivos em quarentena na instância que foram excluídos na data indicada.
Laranja	Número de arquivos em quarentena na instância que foram restaurados na data indicada. **Nota:** Depois que Varredura antivírus for executado e encontrar falso-positivos, você poderá restaurar um arquivo em quarentena e torná-lo acessível na instância.

- Para acessar a página Hub de análise e exibir o cartão de pontuação detalhado e as informações de análise de uma data específica, clique em uma linha colorida no gráfico de Eventos de antivírus. Por exemplo, clique na linha azul do gráfico para exibir informações de análise de arquivos em quarentena para uma data específica.
- Para exibir os seguintes detalhamentos na página Hub de análise, clique no , em seguida:

Detalhamento	Descrição
AppSec - Origem de Evento de Antivírus	Origem do evento de antivírus. ◦ **Ao carregar:** ocorreu devido ao upload de um arquivo infectado, geralmente um anexo. ◦ **Da quarentena:** ocorreu devido à quarentena de um arquivo infectado, geralmente um anexo. ◦ **Ao baixar:** ocorreu devido ao download de um arquivo infectado, geralmente um anexo. ◦ **Do registro:** ocorreu devido a um registro infectado em uma tabela.
AppSec - Tipo de Evento de Antivírus	Tipo de evento de antivírus. ◦ **Em quarentena:** ocorreu devido à quarentena de um arquivo, geralmente um anexo. ◦ **Baixado:** ocorreu devido a um download de um arquivo, geralmente um anexo.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Detalhamento	Descrição
	◦ **Restaurado:** ocorreu devido à restauração de um arquivo em quarentena. ◦ **Excluído:** ocorreu devido à exclusão de um arquivo em quarentena.
AppSec - Carregador de antivírus	Nome do usuário conectado que carregou os arquivos que eram a origem das infecções de vírus detectadas pela aplicação Varredura antivírus.

Arquivos em quarentena

Lista os arquivos infectados na instância em quarentena pelo Varredura antivírus:

Campo	Descrição
Nome de arquivo	Nome do arquivo infectado.
Tipo de conteúdo	Tipo de conteúdo que estava infectado no arquivo. Por exemplo, **application/x-dosexec** é uma aplicação infectada ou arquivo executável do DOS, enquanto **text/plain** é um arquivo .txt infectado.
Tabela	Nome da tabela que contém o arquivo infectado. Por exemplo, **incidente** aparece para um registro de arquivo de incidente.
Vírus	Nome do arquivo em quarentena pelo Varredura antivírus.
Detectado	Data e hora em que o arquivo infectado foi detectado.
Criado por	Nome do usuário que colocou o arquivo infectado em quarentena.
Criado	Data e hora em que o registro do arquivo de quarentena foi criado.
ID do sistema de tabelas	Identificador do sistema de tabela atribuído ao registro do arquivo de quarentena.

Nota: Você também pode adicionar blocos de **Arquivos em quarentena** e **Tipos de vírus** à faixa de opções de eventos. Para aprender mais, consulte Monitorar eventos de segurança e Configurar a faixa de opções de eventos de segurança.

Informações relacionadas

- Varredura antivírus
- Configuração do Varredura antivírus
- Revisar arquivos em quarentena
- Analisar a atividade do antivírus
- Hub de análise
- Detalhamentos do Performance Analytics
- Análise, Inteligência e Emissão de relatórios

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Painel de métricas de MFA

O painel de métricas de MFA mostra informações sobre a configuração da autenticação multifator de instâncias. Use o painel para garantir que sua configuração de MFA atenda aos seus padrões de segurança.

Funções necessárias de Now Platform

security_dashboard_user ou admin, necessário para exibir o painel de pontuação de conformidade de PCI.

Acessar o painel de métricas de MFA

Para abrir o painel, navegue até **Segurança do sistema** > **Central de segurança da instância**. na Central de segurança da instância, clique em **Métricas** no cabeçalho e selecione **Métricas de MFA**.

Casos de uso

Para obter exemplos de como diferentes pessoas de sua organização podem usar este painel, consulte estes casos de uso.

Usuário	Uso do painel
Usuário do painel de segurança (security_dashboard_user)	Monitore e gerencie continuamente a conformidade da Segurança da instância.
Administrador (administrador)	Monitore continuamente a conformidade da Segurança da instância para detectar e responder a ameaças à segurança.

Indicadores

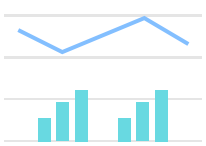
Usuários inscritos na MFA

Exibe o número total de usuários na instância inscrita na MFA. Clique para abrir o hub de análise para obter mais detalhes.

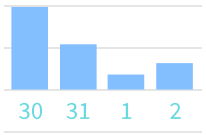
Usuários que usam o desvio de MFA

Exibe o número de usuários que usam o desvio de MFA. Clique para abrir o hub de análise para obter mais detalhes.

Visualizações de dados

Título	Tipo	Tabela de origem	Descrição
Usuários de alto privilégio da MFA	Barras 		

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Título	Tipo	Tabela de origem	Descrição
Tendência do usuário de MFA	 Tendência		

Como ativar a interface do ISC Virtual Agent

Se você tiver a função de administrador, poderá ativar o plug-in ISC Virtual Agent Conversations (com.glide.isc_virtualagent). Habilitar este plug-in instala os pacotes de conteúdo Virtual Agent e Compreensão da linguagem natural (NLU), fornecendo acesso ao Virtual Agent a partir da Central de segurança da instância.

Antes de Iniciar

Importante:

A Central de segurança da instância (ISC) atingiu o fim das vendas em setembro de 2024 e não é mais compatível ou disponível para nova ativação.

A SSC (ServiceNow Security Center, Central de segurança da ServiceNow) é a solução recomendada no futuro. Para obter mais informações, consulte Migração da Central de segurança da instância para a ServiceNow Security Center.

A interface do Virtual Agent na Central de segurança da instância está disponível somente para usuários com assinaturas ao Virtual Agent pagas e que ativaram o plug-in Glide Virtual Agent (com.glide.cs.chatbot). Para saber mais, consulte Ativar o Virtual Agent.

Função necessária: administrador.

Por Que e Quando Desempenhar Esta Tarefa

A interface do ISC Virtual Agent permite que você execute as seguintes tarefas:

- Faça perguntas relacionadas à segurança e obtenha respostas de resumo rápido e links de referência para saber mais.
- Obtenha respostas relacionadas aa Central de segurança da instância, segurança da plataforma, políticas de segurança da ServiceNow, confiança, governança, risco e outros processos.
- Pesquise recursos relacionados à segurança, como tópicos da Base de conhecimento no portal de segurança do Now Support.

Plug-ins para ISC Virtual Agent

Plug-in	Descrição
ISC Virtual Agent Conversations [com.glide.isc_virtualagent]	Habilita o pacote de conteúdo do ISC Virtual Agent Conversations para a Central de segurança da instância.
Modelo do ISC NLU para Virtual Agent Conversations	Habilita o pacote de conteúdo Compreensão da linguagem natural (NLU) para a Central de segurança da instância.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Plug-ins para ISC Virtual Agent

Plug-in	Descrição
[com.glide.isc_nlu]	

Nota: Habilitar o plug-in com.glide.isc_virtualagent ativa automaticamente com.glide.isc_nlu. No entanto, se você ativar o plug-in com.glide.isc_nlu primeiro, também deverá ativar manualmente o com.glide.isc_virtualagent.

Procedimento

1. Navegue até **Todos** > **Aplicações do sistema** > **Todas as aplicações disponíveis** > **Todas**.
2. Encontre o plug-in usando os critérios de filtro e a barra de pesquisa.

   Pesquise o plug-in pelo nome ou ID. Se não conseguir encontrar um plug-in, talvez seja necessário solicitá-lo ao pessoal ServiceNow.
3. Selecione **Instalar** para iniciar o processo de instalação.

   Nota: Quando a separação de domínio e o administrador delegado estão habilitados em uma instância, o usuário administrativo deve estar no domínio **global.** Caso contrário, será exibido o seguinte erro: `A instalação da aplicação não está disponível porque há outra operação em execução: ativação de plug-in para <plugin name>.`

   Você verá uma mensagem após a conclusão da instalação.

Configurações de proteção de segurança da instância

O conteúdo das Configurações de proteção de Segurança da instância contém descrições detalhadas e valores de conformidade para as propriedades e os plug-ins do sistema relacionados à segurança na Now Platform. Você pode definir a maioria dessas propriedades na página Configuração de conformidade de proteção na Central de segurança da instância.

Importante:

A Central de segurança da instância (ISC) atingiu o fim das vendas em setembro de 2024 e não é mais compatível ou disponível para nova ativação.

A SSC (ServiceNow Security Center, Central de segurança da ServiceNow) é a solução recomendada no futuro. Para obter mais informações, consulte Migração da Central de segurança da instância para a ServiceNow Security Center.

Visão geral e finalidade

A Central de segurança da instância calcula uma Pontuação de conformidade diária, expressa como uma porcentagem. Ele se baseia na conformidade das suas configurações de segurança de instância atuais com os valores de conformidade em Configurações de proteção de segurança de instância.

Usando a página Configuração de conformidade de proteção, você pode gerenciar as configurações de segurança específicas que podem afetar a pontuação de sua instância. Para saber mais sobre como garantir que suas instâncias atendam aos requisitos de proteção, consulte:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Central de segurança da instância
- Ajuste as configurações de segurança da instância para aumentar a conformidade

Consulte as configurações de proteção de segurança da instância sempre que você definir ou atualizar propriedades relacionadas à segurança, mesmo que alguns dos valores de conformidade possam não ser adequados para sua instância. Ao atualizar essas propriedades, certifique-se de que a instância continua a se comportar conforme o esperado. Consulte o pessoal interno apropriado que tenha experiência para determinar os impactos na segurança.

Outros recursos

Para referência do usuário, a Now Platform mantém informações abrangentes sobre os recursos de configuração na documentação do produto. Você pode acessar a maior parte do conteúdo de segurança usando os links encontrados em Proteja sua instância. Além disso, consulte o seguinte:

- Propriedades do sistema disponíveis
-
- Configurações de Alta Segurança

Tabelas de proteção de segurança de instância

Tabela Configurações de segurança

Os registros na tabela Configurações de segurança [isc_security_configurations] contêm os detalhes de uma configuração de segurança. Em um registro, você pode encontrar a descrição de uma configuração, seu estado de conformidade e outros detalhes importantes.

Use o registro de configurações de segurança para ver todas as propriedades e dependências que você precisa configurar para tornar sua configuração compatível em um só lugar.

No registro de configurações de segurança, você pode ver a dependência de segurança relacionada e os registros de grupos de dependência associados a esta configuração.

Tabela Dependências de segurança

Os registros na tabela Dependências de segurança [isc_security_dependencies] definem os critérios de entrada e de saída, bem como um tipo recomendado. Esse tipo define como a dependência é exibida na Central de segurança da instância.

Tabela Grupos de dependência

Use registros na tabela Grupos de dependência [isc_dependency_groups] para agrupar várias dependências. Todas as dependências em um grupo devem ser compatíveis para que o grupo seja considerado compatível.

Controle de acesso (proteção de segurança da instância)

Os controles de acesso determinam se o acesso a um recurso específico deve ser concedido ou negado. Eles só permitem o acesso aos recursos aos usuários com permissão para usá-los.

Autorização e autenticação não são equivalentes, embora esses termos e suas definições sejam frequentemente confundidos.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- A autenticação fornece e valida a identidade.
- A autorização inclui regras de execução que determinam quais funcionalidades e dados o usuário (ou entidade de segurança) pode acessar, garantindo a alocação apropriada de direitos de acesso após a autenticação ser bem-sucedida.

A autorização é um processo que vem após uma autenticação bem-sucedida. Você pode configurar propriedades de segurança que designam se, após determinar que um usuário possui credenciais válidas associadas a um conjunto bem definido de funções e privilégios, ocorre a autorização de recursos.

A seguir estão alguns controles de segurança que um administrador pode configurar para restringir o acesso não autorizado a entidades confidenciais dentro da Now Platform.

- Regras da lista de controle de acesso
- Configuração de uma regra de ACL
- ServiceNow controle de acesso

Acesso à API passível de script GlideSystemUserSession

A API passível de script GlideSystemUserSessionSandbox cliente chamável expõe os métodos addErrorMessageNoSanitization e addInfoMessageNoSanitization de GlideSystemUserSession para a área restrita do javascript. Isso permite que todos os usuários chamem este método por meio de script.

Quando definido como **verdadeiro**, uma sessão de usuário em área restrita tem permissão para chamar informações ou mensagens de erro sem limpeza. Um aviso será registrado quando a mensagem for chamada. Quando definido como **falso**, a chamada não é permitida.

Mais informações

Atributo	Descrição
Nome da propriedade	*glide.sandbox.usersession.allow_unsanitized_messages*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Configurável na Central de segurança da instância	Sim
Finalidade	Esta propriedade restringirá a chamada de mensagens informativas ou de erro em uma sessão de usuário em área restrita.
Tipo	booliano verdadeiro | falso
Valor recomendado	falso
Dependências de segurança	O valor dessa propriedade é uma substituição segura e não pode ser alterado depois de mudado.
Impacto funcional	(Alto) Definir a propriedade com o valor falso resultará em nenhuma criação de mensagem ou registro em log caso essas funções sejam chamadas.
Risco à segurança	(Alto) Sem a limpeza apropriada, o conteúdo potencialmente perigoso pode ser acessado e a função de erro não limpa fica disponível para o script.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Referências	Controle de Acesso Substituição de segurança

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Autorização para execução de script

Use a propriedade *glide.script_processor.authorized_script_module_role* para restringir o uso de scripts em execução da tabela *sys_app_module* para a função definida na propriedade.

Essa propriedade restringirá todos os usuários do sistema de executar qualquer script do sys_app_module, a menos que tenham a função especificada na propriedade. Use a propriedade glide.script_processor.authorized_script_module_role para especificar a função que pode executar scripts.

Mais informações

Atributo	Descrição
Nome da propriedade	*glide.script_processor.authorized_script_module_role*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Configurar na Central de segurança da instância	Sim
Finalidade	Exigir uma função designada para executar um script do *sys_app_module*.
Valor recomendado	Caixa de texto com uma lista de funções delimitada por vírgulas.
Impacto funcional	(Médio) Esta correção impõe a autenticação na forma de autorização pela função definida. • Ela executa essa autenticação ao processar solicitações de script na instância. • Ela restringe todos os usuários convidados que estão acessando esses dados. Se for o caso, você poderá criar uma nova conta para usuários que precisam acessar o conteúdo com as permissões de controle de acesso necessárias.
Risco à segurança	(Alto) Sem autorização apropriada configurada em solicitações de script, usuários não autorizados podem acessar conteúdo/dados confidenciais na instância.
Referências	Controle de Acesso

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Autenticação básica: solicitações JSONv2 (proteção de segurança da instância)

Use a propriedade *glide.basicauth.required.jsonv2* para designar se as solicitações de JSONv2 recebidas devem exigir autorização básica.

Mais informações

Atributo	Descrição
Nome da propriedade	glide.basicauth.required.jsonv2
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Configurar na Central de segurança da instância	Sim
Finalidade	Impor autorização de solicitações de JSONv2
Valor recomendado	verdadeiro
Impacto funcional	(Médio) Esta correção impõe uma combinação de métodos de autenticação na forma de autenticação básica e controle de acesso no nível do sistema. • Ela executa essa autenticação ao recuperar dados de tabelas/páginas na forma de dados JSON na instância. • Ela restringe todos os usuários convidados que estão acessando esses dados. • Crie uma conta para um usuário que precisa de acesso a este conteúdo com as permissões de controle de acesso necessárias. Para saber mais, consulte Serviço Web JSONv2 Serviço Web JSONv2.
Risco à segurança	(Alto) Sem autorização apropriada configurada nas solicitações JSON da fonte de dados, um usuário não autorizado pode acessar conteúdo/dados confidenciais na instância de destino.
Referências	Autenticação Requer autenticação básica para solicitações de JSONv2 recebidas

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Autenticação básica: solicitações SOAP (proteção de segurança da instância)

Use a propriedade *glide.basicauth.required.soap* para designar se as solicitações SOAP recebidas devem exigir autorização básica.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mais informações

Atributo	Descrição
Nome da propriedade	glide.basicauth.required.soap
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Configurar na Central de segurança da instância	Sim
Finalidade	Impor autorização de solicitações SOAP
Valor recomendado	verdadeiro
Impacto funcional	(Médio) Esta correção impõe uma combinação de métodos de autenticação na forma de autenticação básica e controle de acesso no nível do sistema. • Ela executa essa autenticação ao recuperar dados de tabelas/páginas na forma de dados SOAP na instância. • Ela restringe todos os usuários convidados que estão acessando esses dados. • Crie uma conta para um usuário que precisa de acesso a este conteúdo com as permissões de controle de acesso necessárias. Para saber mais, consulte SOAP Web Service e Credenciais de autenticação de MID Server e solicitações SOAP.
Risco à segurança	(Médio) Sem a autorização apropriada configurada nas solicitações de fonte de dados SOAP, um usuário não autorizado pode obter acesso a conteúdo/ dados confidenciais na instância de destino.
Referências	Autenticação

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Bloquear acesso para desenvolvedor delegado

Esta configuração afeta o acesso de desenvolvedores delegados que estão atualizando funções de usuário por meio de script. Quando a configuração está em conformidade, o desenvolvedor não poderá atualizar ou inserir registros na tabela `sys_user_has_role` sem também a função user_admin.

O valor desta propriedade afeta se um desenvolvedor delegado tem permissão para conceder ou receber acesso inesperado à funcionalidade na instância. Quando a propriedade contém funções, somente essas funções podem executar módulos de script.

Mais informações

Atributo	Descrição
Nome da propriedade	`com.glide.sys.security.delegateddev.block_grant_roles`

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Configurar na Central de segurança da instância	Sim
Finalidade	O valor desta propriedade afeta se um desenvolvedor delegado tem permissão para conceder ou receber acesso inesperado à funcionalidade na instância.
Tipo	comutador de alternância
Valor recomendado	verdadeiro
Dependências de segurança	nenhum
Impacto funcional	(Alto) Quando um usuário com a função delegated_developer tenta modificar um registro em `sys_user_has_role`, esta propriedade habilita verificações de segurança adicionais em relação à operação. As verificações de segurança adicionais validam que o usuário recebeu a função `user_admin` se ele tentar criar ou atualizar `sys_user_has_role`. Se ele não tiver a função `user_admin`, o acesso será negado. Quando a propriedade é falsa, essas verificações adicionais não são validadas.
Risco à segurança	(Alto) Sem a autorização apropriada, usuários não autorizados podem acessar conteúdo/dados confidenciais na instância.
Referências	Controle de Acesso

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Verifique as condições de ação de IU antes da execução (proteção de segurança da instância)

Use a propriedade *`glide.security.strict.actions`* para habilitar a verificação das condições de ações de IU em formulários e listas antes de serem executados. Quando você define esta propriedade como **verdadeira**, ela adiciona uma camada extra de validação nas ações de IU da tabela antes que elas sejam executadas.

Mais informações

Atributo	Descrição
Nome da propriedade	glide.security.strict.actions
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Configurar na Central de segurança da instância	Sim
Finalidade	Definir uma camada extra de validação nas ações de IU da tabela antes que elas sejam executadas.
Valor recomendado	verdadeiro

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Impacto funcional	(Baixo) Esta correção adiciona apenas uma camada extra de validação para verificar se há ações de IU na tabela/página de destino na instância. Contanto que os controles de acesso sejam definidos corretamente na instância do cliente, não deve haver um impacto aqui.
Risco à segurança	(Médio) A solicitação de acesso é sempre verificada quando as transações ocorrem entre duas zonas. Esta operação valida quaisquer ações de IU antes que o formulário seja renderizado para o usuário final.
Referências	Plug-in High Security

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Plug-in Contextual Security: Role Management (proteção de segurança da instância)

Ative o plug-in Contextual Security: Role Management (*com.glide.role_management*) para habilitar a segurança contextual, que protege um registro/informação usando a funcionalidade de criação, leitura, gravação e exclusão.

Depois que ele é instalado e ativado, as funções de dicionário (criadas pelo gerenciador de segurança simples) não são mais testadas. Em vez disso, o Now Platform procura regras de ACL em campos e tabelas. Ele protege os dados com a ajuda de regras de ACL em vez das regras de dicionário tradicionais baseadas em funções implementadas pelo gerenciador de segurança simples. Mesmo se você configurar o formulário de dicionário e adicionar funções a uma entrada de dicionário, não ocorrerá nenhuma mudança nos direitos.

Mais informações

Atributo	Descrição
ID do plug-in	com.glide.role_management
Tipo de configuração	Definição do sistema > Plug-ins
Configurar na Central de segurança da instância	Sim
Finalidade	Ao contrário do gerenciador de segurança simples, o gerenciador de segurança contextual está ciente da hierarquia da tabela do sistema. Você pode ter regras de segurança diferentes para um campo com base em onde ele aparece na hierarquia.
Valor recomendado	Ativo (plug-in ativado por padrão)
Impacto funcional	(Médio) Esta correção impõe o nível funcional de controles de acesso, o que permite que a aplicação determine as restrições de acesso com base somente na tabela de ACL.
Risco à segurança	(Alto) Controles de acesso de nível funcional devem ser aplicados do lado do servidor antes da execução das operações CRUD, garantindo o nível apropriado de acesso aos usuários da instância.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Referências	Contextual Security Manager

Para saber mais sobre como ativar um plug-in, consulte Ativar um plug-in.

Autorização de solicitação de CSV (proteção de segurança da instância)

Use a propriedade *glide.basicauth.required.csv* para designar se as solicitações de entrada de CSV (Comma-Separated Values, Valores separados por vírgula) devem exigir autenticação básica.

Mais informações

Atributo	Descrição
Nome da propriedade	glide.basicauth.required.csv
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Configurar na Central de segurança da instância	Sim
Finalidade	Impor autenticação básica em solicitações de CSV.
Valor recomendado	verdadeiro
Impacto funcional	(Baixo) Esta correção impõe uma combinação de métodos de autenticação na forma de autenticação básica e controle de acesso no nível do sistema. • Ela executa essa autenticação ao recuperar dados de tabelas/páginas na forma de dados CSV na instância. • Ela restringe todos os usuários convidados que estão acessando esses dados. Se for o caso, você poderá criar uma nova conta para usuários que precisam acessar o conteúdo com as permissões de controle de acesso necessárias. Para saber mais, consulte Recuperar dados de um arquivo no formato CSV.
Risco à segurança	(Médio) Sem autorização apropriada configurada nas solicitações de CSV recebidas, um usuário não autorizado pode obter acesso a conteúdo/dados confidenciais na instância de destino.
Referências	Segurança de serviços da Web

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Negação padrão (proteção de segurança da instância)

Use a propriedade *glide.sm.default_mode* para controlar o comportamento padrão do gerenciador de segurança quando ele descobrir que as regras de ACL existentes fazem parte das regras de ACL da tabela curinga.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Quando o plug-in Configurações de Alta Segurança (*com.glide.high_security*) é ativado durante a instalação da instância inicial, ele cria esta propriedade e as regras de ACL curinga passam a existir. Para fornecer acesso baseado em função a tabelas do sistema, estas regras controlam um número significativo de ACLs e operações baseadas em registro mais comuns:

- Leitura
- Gravar
- Criar
- Excluir

A menos que você use o plug-in Alta segurança com a opção de negação padrão habilitada, muitas tabelas não serão protegidas. O Now Platform usa um modelo de segurança de negação padrão que evita que usuários não administradores acessem objetos, a menos que atendam a uma regra de ACL correspondente. Usar este modelo remove muitos vetores de ataque, como scripts não seguros.

Mais informações

Atributo	Descrição
Nome da propriedade	glide.sm.default_mode
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Configurar na Central de segurança da instância	Sim
Finalidade	A prática recomendada de segurança é restringir um acesso às tabelas por um usuário não autorizado. • Se não houver regras de ACL em vigor para tabelas, esta propriedade garantirá que pelo menos ACLs curinga sejam validadas para qualquer operação CRUD realizada na tabela/campo. • Essas regras restringem as operações de leitura, gravação, criação e exclusão em todas as tabelas, a menos que o usuário tenha a função de administrador ou atenda aos requisitos de outra regra de ACL de tabela.
Valor recomendado	negar
Impacto funcional	(Alto) Se você definir esta propriedade como **Permitir**, as regras de ACL da tabela curinga permitirão operações CRUD em todas as tabelas, a menos que haja regras de ACL de tabela específicas para restringir essas operações. **Nota:** Este plug-in não é destinado a instâncias existentes, já que pode modificar o acesso de segurança a tabelas já em uso em um ambiente de produção.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Risco à segurança	(Alto) Usuários que não são administradores podem acessar objetos que correspondem às regras de ACL da tabela curinga.
Referências	Propriedade de negação padrão

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Verificar duas vezes as transações de entrada (proteção de segurança da instância)

A propriedade *glide.security.strict.updates* permite a confirmação da segurança em transações de entrada durante o envio do formulário e adiciona uma camada extra de validação de tabela antes que um formulário seja renderizado no navegador. Esta propriedade é definida como **verdadeira** por padrão.

Mais informações

Nota: Essa propriedade é definida como **true** por padrão em Vancouver e versões posteriores, e não pode ser alterada pelos administradores. Para um caso de uso em que a propriedade precise ser alterada, entre em contato com o suporte ao cliente.

Atributo	Descrição
Nome da propriedade	glide.security.strict.updates
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Configurar na Central de segurança da instância	Sim
Finalidade	Garantir uma camada adicional de verificação de permissões do usuário antes de apresentar o formulário no navegador.
Valor recomendado	verdadeiro
Impacto funcional	(Baixo) Esta correção adiciona apenas uma camada extra de validação para verificar se há permissões de usuário na tabela/página de destino na instância. Contanto que os controles de acesso sejam definidos corretamente na instância do cliente, não deve haver um impacto.
Risco à segurança	(Alto) Você sempre deve verificar a solicitação de acesso quando ocorrem transações entre duas zonas. Esta operação verifica se há permissões quando o formulário é solicitado e antes que a renderização do formulário ocorra.
Referências	

Habilitar ACLs para controlar os detalhes do perfil dinâmico (proteção de segurança da instância)

Use a propriedade *glide.live_profile.details* para designar se um usuário deve ser capaz de exibir todos os campos de detalhes, como nome da empresa e números de telefone, em um perfil dinâmico.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Dependendo da configuração da propriedade *glide.live_profile.details*, ocorre o seguinte:

- Se o valor for definido como **Mostrar**, o acesso às informações do perfil dinâmico será concedido, independentemente das ACLs criadas para o perfil de usuário.
- Se o valor for definido como **ACL**, o acesso às informações do perfil dinâmico será concedido, independentemente das ACLs criadas para o perfil de usuário.
- Se o valor for definido como **Esconder**, o acesso às informações do perfil dinâmico será restrito, independentemente das ACLs criadas para o perfil de usuário.

Mais informações

Atributo	Descrição
Nome da propriedade	glide.live_profile.details
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Configurar na Central de segurança da instância	Sim
Finalidade	O objetivo é permitir que somente usuários autorizados acessem os detalhes de um Perfil dinâmico (como Nome da empresa, Números de telefone)
Valor recomendado	ACL
Impacto funcional	(Médio) Se a propriedade não estiver habilitada, os usuários não autorizados poderão acessar os detalhes do perfil dinâmico de todos os outros usuários.
Risco à segurança	(Médio) As solicitações de API sempre devem respeitar as ACLs da tabela. A restrição deve ser aplicada para impedir que usuários não autorizados acessem detalhes de um Perfil dinâmico.

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Habilitar a verificação de ACL de AJAXGlideRecord (proteção de segurança da instância)

Use a propriedade *glide.script.secure.ajaxglideerecord* para executar a validação da regra de controle de acesso (ACL) quando registros do lado do servidor, como tabelas, forem acessados usando APIs GlideAjax em um script do cliente.

Nos scripts do cliente, é possível consultar dados arbitrários do servidor usando a API AJAXGlideRecord (GlideAjax - Cliente) API, usando uma sintaxe como um registro de glide do lado do servidor É uma ferramenta poderosa e útil em muitas implantações.

Se você optar por aplicar ACLs (Access Control Lists, listas de controle de acesso) às chamadas de API GlideAjax, só será possível consultar os dados aos quais o usuário conectado no momento tem acesso. Por exemplo, se um usuário ESS que não tem direitos para ler a tabela cmn_location estiver conectado, qualquer chamada de API GlideAjax para essa tabela falhará.

Se o Now Platform estiver sendo executado sem a verificação de chamada da ACL GlideAjax, uma API poderá retornar informações que o usuário conectado no momento não poderia acessar.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mais informações

Atributo	Descrição
Nome da propriedade	glide.script.secure.ajaxgliderecord
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Configurar na Central de segurança da instância	Sim
Finalidade	Garantir que as ACLs de segurança sejam verificadas e validadas mesmo quando os registros forem acessados por meio de APIs do lado do cliente.
Valor recomendado	verdadeiro
Impacto funcional	(Alto) Esta correção impõe o relacionamento da ACL com registros do lado do servidor quando as solicitações são feitas usando as chamadas de API AJAXGlideRecord. Se a configuração da ACL não estiver configurada corretamente, há um possível impacto. Para obter mais detalhes sobre seu impacto e como identificá-lo, consulte o artigo Auditar e revisar transações GlideRecord do lado do cliente (AJAXGlideRecord) [KB0550828] em HI Base de conhecimento .
Risco à segurança	(Alto) Por meio de scripts do cliente, é possível consultar dados arbitrários do servidor por meio da API GlideAjax. Os recursos do lado do servidor podem ser acessados sem a autorização apropriada, portanto, o uso da validação de ACL ajuda a aplicação a validar a solicitação com base na autorização configurada.
Solução alternativa	Certifique-se de que as ACLs apropriadas sejam criadas para inclusões de script, processadores e outras entidades usadas por uma API GlideAjax (AJAXGlideRecord) para que elas sejam executadas com a devida autorização. Implemente métodos como `canRead()`, `canWrite()`, `canCreate()` e `canDelete()` para executar a autorização do usuário antes de acessar registros de tabela usando GlideRecord. Outro método é usar o GlideRecordSecure. A classe é herdada do servidor GlideRecord que executa as mesmas funções do GlideRecord e também impõe ACLs.
Referências	Aplicar ACLs ao AJAXGlideRecord (registro Glide do lado do cliente) Esta propriedade pertence à mesma família de propriedades que protegem e restringem a execução de scripts originados no cliente:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
	• *glide.script.use.sandbox*: Consulte Área restrita de scripts gerados pelo cliente • *glide.script.allow.ajaxevaluate*: Consulte Habilitar AJAXEvaluate.

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Autorização de solicitação de Excel (proteção de segurança da instância)

Use a propriedade *glide.basicauth.required.excel* para designar se as solicitações de Excel recebidas devem exigir autenticação básica.

Mais informações

Atributo	Descrição
Nome da propriedade	glide.basicauth.required.excel
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Configurar na Central de segurança da instância	Sim
Finalidade	Impor autenticação básica em solicitações de Excel.
Valor recomendado	verdadeiro
Impacto funcional	(Baixo) Esta correção impõe uma combinação de métodos de autenticação na forma de autenticação básica e controle de acesso no nível do sistema. • Ela executa essa autenticação ao recuperar dados de tabelas/páginas na forma de dados de Excel na instância. • Ela restringe todos os usuários convidados que estão acessando esses dados. Se for o caso, você poderá criar uma nova conta para usuários que precisam acessar o conteúdo com as permissões de controle de acesso necessárias.
Risco à Segurança	(Médio) Sem a autorização apropriada configurada nas solicitações recebidas do Excel, um usuário não autorizado pode obter acesso a conteúdo/dados confidenciais na instância de destino.

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Plug-in Explicit Role (proteção de segurança da instância)

Ative o plug-in Explicit Role (*com.glide.explicit_roles*) para fornecer à instância as novas funções snc_internal e snc_external para aplicações B2B e B2C, impedindo que usuários externos acessem dados internos. Os usuários corporativos (funcionários) devem ter a função interna, enquanto os usuários não corporativos (não funcionários) devem ter a função externa.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Ao instalar o plug-in Explicit Role:

- Ele atribui a nova função snc_internal a todos os usuários existentes. Ele também atribui a função snc_internal a todas as tabelas sem qualquer função.
- Quando você cria um usuário ou tabela após ativar o plug-in Explicit Role, a Now Platform atribui ao usuário ou tabela a função snc_internal.
- A Now Platform impede que os usuários com a função snc_external acessem qualquer tabela que não seja explicitamente designada com a função snc_external.
- Qualquer tabela com a função pública pode ser acessada por usuários internos ou externos.
- Alguns widgets do portal de serviços exigem um login, mas não exigem nenhuma função de usuário específica. Depois de instalar o plug-in Explicit Roles, esses portais ficarão inacessíveis para usuários externos.

- ◦ Para permitir o acesso de usuários externos, edite seu widget para mudar as funções necessárias de **em branco** para **snc_internal, snc_external**.
  - ◦ Um exemplo desse problema são os clientes que usam a aplicação de gestão de casos e precisam que usuários externos possam anexar arquivos a seus registros de caso. A alteração da configuração do widget **encryption-context-picker**, conforme descrito, permite que usuários externos se conectem conforme o esperado.
  - ◦ Para obter mais informações sobre como configurar widgets, consulte Configurar opções de instância de widget.

Nota: Não mova conjuntos de atualizações do sistema entre instâncias cuja habilitação do plug-in Explicit Roles esteja diferente entre elas. Para obter mais informações, consulte Conjuntos de atualizações do sistema.

Resumo da função

snc_internal

Esta função é atribuída a todos os usuários internos (funcionários ou internos a uma organização). Qualquer novo usuário adicionado também obtém essa função durante seu primeiro login/representação, desde que o usuário não tenha a função snc_external já atribuída. Todas as regras de controle de acesso (ACLs) existentes sem uma função são corrigidas com a função 'snc_internal'. Para novas ACLs, a Now Platform adiciona automaticamente esta função se a ACL for salva sem nenhuma função.

snc_external

Esta função indica que o usuário é externo à sua organização e não deve ter acesso aos recursos, a menos que:

- Você permita explicitamente o acesso por meio de ACLs para a função snc_external, ou
- Você conceda explicitamente a eles funções adicionais.

Por padrão, os usuários com a função snc_external também não podem acessar recursos do tipo sem registro, como processadores e páginas de IU.

público

Quaisquer entidades com função pública atribuída a ela podem ser acessadas por usuários snc_internal e snc_external.

Ao usar o plug-in Explicit Role:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

1. Revise e valide se qualquer tabela com a função pública não contém nenhum registro confidencial para os usuários externos, incluindo usuários públicos não autenticados.
2. Se a tabela com a função pública contiver dados confidenciais e você quiser restringir os registros confidenciais de usuários externos:
   - Remova a função pública da tabela ou
   - Adicione uma ACL com script adicional à tabela.
3. Revise e valide se todos os endpoints, como Scripted REST APIs, usam *GlideRecordSecure* ou verificam explicitamente as funções usando `canRead()`, `canWrite()`, `canUpdate()` e `canDelete()`.

Mais informações

Atributo	Descrição
Nome do Plug-in	com.glide.explicit_roles
Tipo de configuração	Definição do sistema > Plug-in
Configurar na Central de segurança da instância	Não
Finalidade	Impedir que usuários externos acessem dados internos.
Valor recomendado	Ativo
Impacto funcional	(Baixo) Nenhum impacto significativo, pois o plug-in atribui automaticamente a função snc_internal à tabela para que os usuários internos existentes ainda tenham o acesso necessário.
Risco à segurança	(Alto) Usuários externos (não funcionários) podem acessar muitas tabelas confidenciais na Now Platform que não possuem funções atribuídas a eles. Elas devem ser acessados somente por usuários internos (funcionários).
Referências	Funções explícitas

Etapas para configurar

Ao criar um recurso ou aplicação com Explicit Roles:

1. Crie uma função que herde a função snc_external para seu novo recurso ou aplicação.
2. Ao criar um usuário externo, remova a função snc_internal e adicione a função recém-criada que herda a função snc_external.
3. Ao adicionar a nova função que herda a função snc_external à tabela existente, revise e valide se a tabela não contém nenhum registro confidencial.
4. Ao criar uma tabela, valide que a tabela só pode ser acessada por funções de usuário interno e externo autorizadas.
5. Ao criar endpoints, como Scripted REST APIs, use GlideRecordSecure ou verifique explicitamente as funções usando `canRead()`, `canWrite()`, canUpdate() e `canDelete()`.

Ao criar uma tabela com função pública, verifique se a tabela não contém nenhum registro confidencial para usuários externos, incluindo usuários públicos não autenticados.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Autorização de solicitação de importação (proteção de segurança da instância)

Use a propriedade *glide.basicauth.required.importprocessor* para designar se as solicitações de importação recebidas devem exigir autenticação básica.

Mais informações

Atributo	Descrição
Nome da propriedade	glide.basicauth.required.importprocessor
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Configurar na Central de segurança da instância	Sim
Finalidade	Impor autenticação básica em solicitações de importação.
Valor recomendado	verdadeiro
Impacto funcional	(Baixo) Esta correção impõe uma combinação de métodos de autenticação na forma de autenticação básica e controle de acesso no nível do sistema. • Ela executa essa autenticação ao importar fontes de dados para as tabelas/páginas de instância. • Ela restringe todos os usuários convidados que estão acessando esses dados. Se for o caso, você poderá criar uma nova conta para usuários que precisam acessar o conteúdo com as permissões de controle de acesso necessárias. Para saber mais, consulte Recuperar dados de um arquivo no formato CSV.
Risco à segurança	(Médio) Sem a autorização apropriada configurada nas solicitações de importação da fonte de dados, um usuário não autorizado pode obter acesso a conteúdo/dados confidenciais na instância de destino.
Referências	Segurança de serviços web SOAP Serviço web SOAP

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Autorização de solicitação de PDF (proteção de segurança da instância)

Use a propriedade *glide.basicauth.required.pdf* para designar se as solicitações de PDF recebidas devem exigir autenticação básica.

Mais informações

Atributo	Descrição
Nome da propriedade	glide.basicauth.required.pdf

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Configurar na Central de segurança da instância	Sim
Finalidade	Impor autenticação básica em solicitações de PDF.
Valor recomendado	verdadeiro
Impacto funcional	(Baixo) Esta correção impõe uma combinação de métodos de autenticação na forma de autenticação básica e controle de acesso no nível do sistema. • Ela executa essa autenticação ao recuperar dados de tabelas/páginas na forma de dados de PDF na instância. • Ela restringe todos os usuários convidados que estão acessando esses dados. Se for o caso, você poderá criar uma nova conta para usuários que precisam acessar o conteúdo com as permissões de controle de acesso necessárias. Para saber mais, consulte Conjuntos para importação de serviços web.
Risco à segurança	(Médio) Sem autorização apropriada configurada nas solicitações de PDF recebidas, um usuário não autorizado pode obter acesso a conteúdo/dados confidenciais na instância de destino.

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Monitoramento de desempenho (ACL) (proteção de segurança da instância)

Use a propriedade *glide.security.diag_txns_acl* para controlar o acesso a stats.do, threads.do e replication.do a partir de uma conexão não autenticada.

Quando você define esta propriedade como **verdadeira**, a propriedade *glide.security.diag_txns_acl* só permite o acesso ao seguinte pela conta do administrador:

- https://<instancename>.servicenow.com/stats.do
- https://<instancename>.servicenow.com/threads.do
- https://<instancename>.servicenow.com/replication.do
- https://<instancename>.servicenow.com/thread_pool_stats.do

Sem habilitar esta configuração, ainda é possível acessar esses recursos de uma conexão não autenticada.

Mais informações

Atributo	Descrição
Nome da propriedade	glide.security.diag_txns_acl

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Configurar na Central de segurança da instância	Sim
Finalidade	Restringir o acesso às páginas de configuração somente à conta do administrador
Valor recomendado	verdadeiro
Impacto funcional	(Baixo) Esta correção impõe que somente a conta do administrador obtenha acesso aos dados confidenciais da aplicação para fins de registro em log e solução de problemas.
Risco à segurança	(Baixo) Dados confidenciais, como detalhes do servidor, threads e processos executados no servidor, nunca devem estar visíveis ou acessíveis ao usuário final sem os privilégios apropriados.

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Restrição de IP de monitoramento de desempenho (proteção de segurança da instância)

Use a propriedade *glide.custom.ip.authenticate.allow* para habilitar somente uma lista separada por vírgulas especificada ou um intervalo de endereços IP para acessar as páginas stats.do, threads.do e replication.do. Se esta propriedade não estiver habilitada, será possível acessar esses tipos de páginas de qualquer endereço IP.

Nota: Com base em algumas mudanças recentes, o Controle de acesso ao endereço IP deve ser usado para todas as restrições de IP. Consulte a seção Etapas para configurar em Restringir o acesso a intervalos de IP específicos.

Mais informações

Atributo	Descrição
Nome da propriedade	glide.custom.ip.authenticate.allow
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Configurar em Central de segurança da instância	Não
Finalidade	Restringir o acesso somente às páginas de configuração dos endereços IP na lista de inclusão.
Valor recomendado	Lista separada por vírgula de endereço IP.
Impacto funcional	(Baixo) Páginas de informações confidenciais podem ser acessadas até mesmo de um endereço IP não confiável.
Risco à segurança	(Baixa) A exposição desnecessária à instância de destino na Internet deve ser restrita com a ajuda da funcionalidade de controles de acesso por IP.
Referência	Propriedades do sistema disponíveis

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Privacidade em inclusões de script de cliente chamável (proteção de segurança da instância)

Por padrão, as inclusões de script de cliente chamável que não definem explicitamente a visibilidade são públicas. Se necessário, adicione a propriedade *glide.script.ccsi.ispublic* para habilitar o controle de privacidade sobre todas as inclusões de script de cliente chamável acessadas por páginas públicas.

Ao adicionar esta propriedade, você deve definir seu valor como **falso**, o que indica que todas as inclusões de script de cliente chamável são privadas e mudam sua visibilidade nas páginas públicas.

Nota: Você não pode adicionar a propriedade com um valor **verdadeiro** ou alterar seu valor de **falso** para **verdadeiro**. Se você tentar fazer isso, será exibida uma mensagem de erro.

Se necessário, você pode alterar a configuração de privacidade de uma inclusão de script de cliente chamável adicionando a função `isPublic ()`.

- A configuração `isPublic ()` tem precedência sobre a propriedade *glide.script.ccsi.ispublic*.
- Por exemplo, se você definir `isPublic ()` como **verdadeira** em um script individual, ele será público, o que substituirá a propriedade *glide.script.ccsi.ispublic* que torna privadas todas as outras inclusões de script de cliente chamável.

Mais informações

Atributo	Descrição
Nome da propriedade	glide.script.ccsi.ispublic
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Configurar na Central de segurança da instância	Sim
Finalidade	Tornar privadas as inclusões de script de cliente chamável significa que os convidados que acessam páginas públicas não podem acessar a inclusão de script de cliente chamável. Um usuário não conectado não pode executar um script privado.
Valor recomendado	falso
Impacto funcional	(Alto) Se as inclusões de script de cliente chamável forem designadas como públicas (ou seja, esta propriedade estiver ausente), os usuários não autenticados poderão executar scripts de cliente. Adicionar a propriedade restringe a execução de scripts por um usuário não logado.
Risco à segurança	(Alto) Se você não adicionar esta propriedade, as inclusões de script do lado do cliente contornarão as ACLs, o que pode resultar em funcionalidade pública não intencional. Se o script do cliente fornecer

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
	informações confidenciais, ele poderá representar um risco potencial adverso à segurança.
Solução alternativa	Definir a propriedade *glide.script.ccsi.ispublic* como **falsa** torna privadas todas as inclusões de script de cliente chamável. Você pode alterar a configuração de privacidade de uma inclusão de script de cliente chamável adicionando a função `isPublic ()`. A função `isPublic ()` tem precedência sobre a propriedade *glide.script.ccsi.ispublic*. Adicione a seguinte sintaxe à inclusão de script: `isPublic:function(){return[true/false];},`

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Desativação do acesso público aos favoritos

Use *glide.ui.magellan.favorites.allow_public* para especificar se usuários não autenticados têm permissão para ver os **Favoritos** no navegador.

O acesso público aos favoritos será compatível se *glide.ui.magellan.favorites.allow_public* estiver definido como **falso**.

Mais informações

Atributo	Descrição
Nome da propriedade	*glide.ui.magellan.favorites.allow_public*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Configurar na Central de segurança da instância	Sim
Finalidade	Controlar se usuários não autenticados têm permissão para ver os **Favoritos** no navegador.
Tipo	verdadeiro/falso
Valor recomendado	*falso*
Dependências de segurança	Definir *glide.ui.magellan.favorites.allow_public* como **falso**
Impacto funcional	(Médio) Habilitar esta propriedade atua como uma camada de proteção contra usuários não autorizados.
Risco à segurança	(Médio) Se esta propriedade não estiver habilitada, há um risco de acesso não autorizado a dados confidenciais.
Referências	Criar ou exibir favoritos

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Restringir o acesso a intervalos de IP específicos (proteção de segurança da instância)

Use a propriedade *com.snc.ipauthenticator* para restringir o acesso a intervalos de IP específicos A menos que o acesso público seja destinado à instância, os administradores devem limitar o acesso aos blocos de rede IP atribuídos.

Pré-requisitos

Antes de definir esta propriedade, você deve ativar o plug-in Autenticação baseada no intervalo de IP *com.snc.ipauthenticator*. Para saber mais, consulte Autenticação baseada no intervalo de IP e vá à seção Etapas para configurar (abaixo).

Mais informações

Atributo	Descrição
Nome do Plug-in	com.snc.ipauthenticator
Tipo de configuração	Segurança do sistema > Controle de acesso a endereço IP
Configurar na Central de segurança da instância	Sim
Finalidade	Adicionar o intervalo de endereços IP que podem ou não acessar a instância às listas de domínios confiáveis e não confiáveis.
Valor recomendado	Ativo
Impacto funcional	(Baixo) Intervalos de IP negados pelo cliente são usados para este item de correção. Nenhum impacto conforme o cliente define a lista de destino.
Risco à segurança	(Baixa) A exposição desnecessária à instância de destino na Internet deve ser restrita com a ajuda da funcionalidade de controles de acesso por IP.
Referências	Autenticação baseada no intervalo de IP

Etapas para configurar

1. Certifique-se de que o plug-in com.snc.ipauthenticator esteja ativo.
2. Navegue até **Segurança do sistema** > **Controle de acesso de endereços IP**.
3. Clique em **Novo** para criar uma lista de exclusões (Negar) ou uma lista de inclusões (Permitir) de endereços IP.
4. Clique em **Enviar**.

Autorização de solicitação de RSS (proteção de segurança da instância)

Use a propriedade *glide.basicauth.required.rss* para designar se as solicitações de RSS recebidas devem exigir autenticação básica.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mais informações

Atributo	Descrição
Nome da propriedade	glide.basicauth.required.rss
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Configurar na Central de segurança da instância	Sim
Finalidade	Impor autenticação básica em solicitações de RSS.
Valor recomendado	verdadeiro
Impacto funcional	(Baixo) Esta correção impõe uma combinação de métodos de autenticação na forma de autenticação básica e controle de acesso no nível do sistema. • Ela executa essa autenticação ao processar solicitações de RSS na instância. • Ela restringe todos os usuários convidados que estão acessando esses dados. Se for o caso, você poderá criar uma nova conta para usuários que precisam acessar o conteúdo com as permissões de controle de acesso necessárias. Para saber mais, consulte Gerador de feed RSS.
Risco à segurança	(Médio) Sem autorização apropriada configurada nas solicitações de RSS recebidas, um usuário não autorizado pode obter acesso a conteúdo/dados confidenciais na instância de destino.
Referências	Autenticação básica RSS

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Perfil de SSO do navegador da Web SAML 2.0 (proteção de segurança da instância)

O plug-in *com.snc.integration.sso.saml20.update1* garante que o status do plug-in SAML 2.0 Single Sign-on esteja ativo.

SAML (Security Assertion Markup Language, Linguagem de marcação de segurança) é um padrão baseado em XML para a troca de dados de autenticação e autorização entre domínios de segurança. O SAML troca informações de segurança entre um provedor de identidade (um produtor de asserções) e um Provedor de serviços (um consumidor de asserções).

O plug-in *com.snc.integration.sso.saml20.update1* é um plug-in necessário, mas você não precisa ativá-lo manualmente. O *sso.multi.installer* instala todos os plug-ins relacionados ao SAML necessários e também contém scripts de implementação saml2 que fornecem opções para validação de resposta. Para saber mais, consulte os tópicos em Referências em Mais informações.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mais informações

Atributo	Descrição
Nome do Plug-in	com.snc.integration.sso.saml20.update1 (novo)
Tipo de configuração	Definição do sistema > Plug-ins
Configurar na Central de segurança da instância	Sim
Finalidade	Prevenir ataques de script entre sites.
Valor recomendado	Ativo
Função necessária	Seu administrador não pode ativar o plug-in. Solicite que essa pessoa com privilégios de segurança elevados o ative na instância.
Referências	Autenticação com integração do SAML SAML Atualizar sua integração de SAML 2.0 existente

Para saber mais sobre como ativar um plug-in, consulte Ativar um plug-in.

Autorização de solicitação de script (proteção de segurança da instância)

Use a propriedade *glide.basicauth.required.scriptedprocessor* para designar se as solicitações de script recebidas devem exigir autenticação básica.

Mais informações

Atributo	Descrição
Nome da propriedade	glide.basicauth.required.scriptedprocessor
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Configurar na Central de segurança da instância	Sim
Finalidade	Impor autenticação básica em solicitações de script.
Valor recomendado	verdadeiro
Impacto funcional	(Médio) Esta correção impõe a autenticação na forma de autorização básica. • Ela executa essa autenticação ao processar solicitações de script na instância. • Ela restringe todos os usuários convidados que estão acessando esses dados. Se for o caso, você poderá criar uma nova conta para usuários que precisam acessar o conteúdo com as permissões de controle de acesso necessárias.
Risco à segurança	(Alto) Sem a autorização apropriada configurada nas solicitações de script recebidas, um usuário não autorizado pode obter acesso a conteúdo/dados confidenciais na instância de destino.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Referências	Autenticação

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Security jump start (regras de ACL) (proteção de segurança da instância)

Ative o plug-in Security Jump Start (regras de ACL) (*com.snc.system_security*) para criar várias ACLs importantes que validam os Controles de acesso em algumas das principais tabelas do sistema na Now Platform.

Essas regras fornecem um salto na proteção de muitas tabelas do sistema, facilitando para uma organização colocar uma instância em produção. O plug-in Security Jump Start (regras de ACL) é instalado automaticamente em todas as novas instâncias.

Mais informações

Atributo	Descrição
ID do plug-in	com.snc.system_security
Tipo de configuração	Definição do sistema > Plug-ins
Configurar na Central de segurança da instância	Sim
Finalidade	Ativar o plug-in Security Jump Start (regras de ACL) para obter a conformidade de segurança apropriada. Ele fornece algumas ACLs básicas que protegem as tabelas do sistema em primeiro lugar, em vez de criar manualmente para cada tabela do sistema que vem com o provisionamento padrão de uma instância. Essas ACLs são úteis quando a instância recém-criada deve passar rapidamente para a produção.
Valor recomendado	Ativo
Impacto funcional	(Médio) Há um impacto funcional significativo se este plug-in for instalado sem auditoria das ACLs existentes na instância. A divulgação e as definições do cliente são necessárias antes que a correção ocorra.
Risco à segurança	(Alto) O controle de acesso deve ser aplicado para bloquear o acesso não intencional à instância. As regras de ACL jumpstart fornecem um ponto de partida para proteger muitas tabelas do sistema, facilitando para uma organização entrar rapidamente na produção.
Referências	Security jump start - regras de ACL

Etapas para configurar

Se este plug-in não estiver ativado em sua instância, entre em contato com o suporte da ServiceNow. Ativar o plug-in neste ponto pode modificar o acesso de segurança a tabelas já em uso em um ambiente de produção. Se um administrador estiver interessado nas novas regras de ACL fornecidas pelo plug-in, você poderá criar manualmente uma ou mais delas

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

em uma instância existente, se necessário. Esta lista de ACLs pode ser usada como diretriz nesse caso.

Para saber mais sobre como ativar um plug-in, consulte Ativar um plug-in.

Plug-in SNC Access Control (proteção de segurança da instância)

Ative o plug-in SNC Access Control (*com.snc.snc_access_control*) para controlar o acesso às suas instâncias pela equipe de Suporte e atendimento ao cliente.

A configuração padrão da Now Platform permite que o Atendimento ao cliente e suporte acesse instâncias por meio de um processo interno que cria credenciais de suporte de curto prazo. Embora todo acesso seja auditado, alguns clientes preferem controlar esse acesso.

Este plug-in permite que o Administrador do cliente proíba Suporte e atendimento ao cliente funcionários de acessar a instância. Esta decisão tem impacto nos ANSs de suporte porque você deve habilitar o acesso a Now Platform para que as atividades de suporte possam começar. Para saber mais, consulte ServiceNow controle de acesso.

Mais informações

Atributo	Descrição
Nome do Plug-in	com.snc.snc_access_control
Tipo de configuração	Definição do sistema > Plug-ins
Configurar na Central de segurança da instância	Sim
Finalidade	Proibir os funcionários de Suporte e atendimento ao cliente de acessar a instância
Valor recomendado	Ativo
Função necessária	O administrador cliente não pode ativar esse plug-in. Ele deve ser solicitado explicitamente porque ativar o plug-in requer privilégios elevados.
Impacto funcional	(Baixo) Se este plug-in estiver inativo, todos os funcionários de Suporte e atendimento ao cliente poderão acessar a instância do cliente. Habilitar o plug-in permite que o cliente restrinja o acesso apenas a funcionários autorizados de Suporte e atendimento ao cliente.
Risco à segurança	(Baixo) Exposição desnecessária de acesso à instância para um grupo maior de pessoas.
Referências	ServiceNow controle de acesso

Etapas para configurar

1. Para solicitar o plug-in, siga as etapas em Ativar o controle do acesso ao ServiceNow. Os clientes devem solicitar o plug-in SNC Access Control (com.snc.snc_access_control) do HI.
2. Para habilitar o controle de acesso SNC, siga as etapas em Configurar o controle de acesso ao ServiceNow. Configure um registro de controle de acesso para especificar um ou mais funcionários de Suporte e atendimento ao cliente que tenham permissão para fazer login em sua instância.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Verificação do tipo de conteúdo SOAP (proteção de segurança da instância)

Use a propriedade *glide.soap.require_content_type_xml* para habilitar a validação de um tipo de conteúdo como texto/xml e proteger contra solicitações SOAP inválidas.

- Quando definida como **verdadeira**, Now Platform valida o tipo de conteúdo como texto/xml e protege contra solicitações SOAP inválidas.
- Se definida como **falsa**, qualquer valor de tipo de conteúdo será permitido.

Mais informações

Atributo	Descrição
Nome da propriedade	glide.soap.require_content_type_xml
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Configurar na Central de segurança da instância	Sim
Finalidade	Proteger contra solicitações SOAP inválidas
Valor recomendado	verdadeiro
Impacto funcional	(Baixo) Esta correção permite a validação do tipo de conteúdo SOAP para todas as solicitações SOAP de entrada. • Se você estiver usando um tipo de conteúdo diferente de texto/xml para solicitações de entrada, isso poderá causar falha nas transações SOAP. • Se você não estiver usando o tipo MIME correto, isso poderá interromper as integrações de terceiros.
Risco à segurança	(Alto) Ao aceitar solicitações SOAP de entrada, a validação apropriada é realizada para garantir que o tipo de conteúdo relevante seja definido como parte da solicitação. Ela restringe as respostas SOAP inválidas que podem ser vistas como um risco à segurança.
Referência	Tipos de conteúdo

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Restrição estrita de IP (proteção de segurança da instância)

Use a propriedade *glide.ip.authenticate.strict* para permitir que um conjunto restrito de endereços IP, como DC e VPN segura, acesse esta instância.

Mais informações

Atributo	Descrição
Nome da propriedade	glide.ip.authenticate.strict

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Configurar na Central de segurança da instância	Sim
Finalidade	Permitir que os funcionários da ServiceNow acessem a instância somente por meio de um conjunto seguro de intervalos de IP
Valor recomendado	verdadeiro
Impacto funcional	(Baixo) Se esta propriedade não estiver habilitada, os funcionários da ServiceNow poderão acessar a instância do cliente por meio de todos os intervalos de IP. Habilitar a propriedade restringe o acesso a um conjunto seguro de intervalos de IP (Secure VPN, DC). **Nota:** Se você definir esta propriedade como verdadeira, o Now Platform usará uma propriedade *glide.ip.authenticate.allow.secured* mais restritiva em vez da restrição de IP de monitoramento de desempenho. Esta propriedade não pode ser substituída.*glide.ip.authenticate.allow.secured*) para um conjunto de intervalos de IP que podem acessar a instância.
Risco à segurança	(Baixo) Exposição desnecessária de acesso à instância para um grupo maior de pessoas.
Referência	Autenticação baseada no intervalo de IP

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Nota: Uma regra de negar tudo é necessária para ser adicionada ao controle de acesso IP para restringir o acesso de qualquer IP não adicionado ao controle de acesso IP. Todos os IPs permitidos necessários devem ser adicionados ao controle de acesso IP.

Autorização de solicitação de descarregamento (proteção de segurança da instância)

Use a propriedade *glide.basicauth.required.unl* (useUnloadFormat) para designar se as solicitações de descarregamento recebidas devem exigir autenticação básica.

Mais informações

Atributo	Descrição
Nome da propriedade	glide.basicauth.required.unl
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Configurar na Central de segurança da instância	Sim

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Finalidade	Impor autenticação básica em solicitações de descarregamento
Valor recomendado	verdadeiro
Impacto funcional	(Médio) Esta correção impõe uma combinação de métodos de autenticação na forma de autenticação básica e controle de acesso no nível do sistema. Ela executa essa autenticação ao recuperar dados de tabelas/páginas na forma de dados de descarregamento na instância.
Risco à segurança	(Alto) Sem a autorização apropriada configurada nas solicitações de fonte de dados de descarregamento, um usuário não autorizado pode obter acesso a conteúdo/dados confidenciais na instância de destino.
Referências	Autenticação

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Autorização de solicitação de WSDL (proteção de segurança da instância)

Use a propriedade *glide.basicauth.required.wsdl* para designar se as solicitações de WSDL (Web Services Description Language, Linguagem descritiva de Web Services) recebidas devem exigir autenticação básica.

Nota: Se optar por não exigir autenticação básica para solicitações de WSDL recebidas, você deverá modificar as regras de controle de acesso (ACL) para permitir que usuários convidados acessem o conteúdo de WSDL.

Mais informações

Atributo	Descrição
Nome da propriedade	glide.basicauth.required.wsdl
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Configurar na Central de segurança da instância	Sim
Finalidade	Impor autenticação básica em solicitações de WSDL.
Valor recomendado	verdadeiro
Impacto funcional	(Baixo) Esta correção impõe uma combinação de métodos de autenticação na forma de autenticação básica e controle de acesso no nível do sistema. • Ela executa essa autenticação ao recuperar dados de tabelas/páginas na forma de dados de WSDL na instância. • Ela restringe todos os usuários convidados que estão acessando esses dados. Se for o caso, você

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
	poderá criar uma nova conta para usuários que precisam acessar o conteúdo com as permissões de controle de acesso necessárias.
Risco à segurança	(Médio) Sem a autorização apropriada configurada nos serviços Web WSDL, um usuário não autorizado pode obter acesso a conteúdo/dados confidenciais WSDL na instância de destino.
Referências	Segurança de serviços da Web

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Autorização de solicitação de XML (proteção de segurança da instância)

Use a propriedade *glide.basicauth.required.xml* para designar se as solicitações de XML recebidas devem exigir autenticação básica.

Mais informações

Atributo	Descrição
Nome da propriedade	glide.basicauth.required.xml
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Configurar na Central de segurança da instância	Sim
Finalidade	Impor autenticação básica em solicitações de XML.
Valor recomendado	verdadeiro
Impacto funcional	(Baixo) Esta correção impõe uma combinação de métodos de autenticação na forma de autenticação básica e controle de acesso no nível do sistema. • Ela executa essa autenticação ao recuperar dados de tabelas/páginas na forma de dados de XML na instância. • Ela restringe todos os usuários convidados que estão acessando esses dados. Se for o caso, você poderá criar uma nova conta para usuários que precisam acessar o conteúdo com as permissões de controle de acesso necessárias. Para saber mais, consulte Etapa do analisador de XML.
Risco à segurança	(Médio) Sem autorização apropriada configurada nas solicitações de XML recebidas, um usuário não autorizado pode obter acesso a conteúdo/dados confidenciais na instância de destino.
Referências	Autenticação

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Autorização de solicitação de XSD (proteção de segurança da instância)

Use a propriedade *glide.basicauth.required.xsd* para designar se as solicitações de XSD (XML Schema Definition, Definição de esquema XML) recebidas devem exigir autenticação básica.

Mais informações

Atributo	Descrição
Nome da propriedade	glide.basicauth.required.xsd
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Configurar na Central de segurança da instância	Sim
Finalidade	Impor autenticação básica em solicitações de XSD.
Valor recomendado	verdadeiro
Impacto funcional	(Baixo) Esta correção impõe uma combinação de métodos de autenticação na forma de autenticação básica e controle de acesso no nível do sistema. • Ela executa essa autenticação ao recuperar dados de tabelas/páginas na forma de dados de XSD na instância. • Ela restringe todos os usuários convidados que estão acessando esses dados. Se for o caso, você poderá criar uma nova conta para usuários que precisam acessar o conteúdo com as permissões de controle de acesso necessárias. Para saber mais, consulte Sessões não interativas.
Risco à segurança	(Médio) Sem autorização apropriada configurada nas solicitações de XSD recebidas, um usuário não autorizado pode obter acesso a conteúdo/dados confidenciais na instância de destino.
Referências	Autenticação

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Anexos (proteção de segurança da instância)

Muitos processos de negócios da Now Platform permitem o upload de dados/informações. Ela verifica regularmente a validade e a segurança do texto, mas aceitar esses arquivos pode apresentar ainda mais risco.

Para reduzir o risco, você deve validar a existência de arquivos mal-intencionados para que a Now Platform possa se proteger corretamente contra invasores que enviam esses arquivos. Você lida com esses arquivos incluindo a lógica de negócios que verifica os arquivos durante o processo de upload e rejeita os arquivos considerados mal-intencionados.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Referências internas

- Administrar anexos
- Configurar propriedades do sistema de anexo

Tipos MIME para download (proteção de segurança de instância)

Use a propriedade *glide.ui.attachment.download_mime_types* para especificar uma lista de tipos MIME de anexo separados por vírgula que devem ser baixados, mas não renderizados em linha no navegador.

Para exibir uma lista de tipos MIME existentes, digite `/sys_attachment_icon_rule_list.do`. Você pode habilitar qualquer um desses tipos MIME para atender aos requisitos de conformidade de segurança em Now Platform.

Nota: Se você definir a propriedade **Forçar download de tipos MIME** como **verdadeira**, ela substituirá a propriedade **Tipos MIME para download**, que é uma lista delimitada por vírgulas de tipos MIME para download. Para saber mais, consulte Forçar download de tipos MIME.

Mais informações

Atributo	Descrição
Nome da propriedade	glide.ui.attachment.download_mime_types
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Configurar na Central de segurança da instância	Sim
Finalidade	Restringir os tipos de arquivo de serem renderizados no navegador para evitar qualquer execução de script mal-intencionado oculto.
Valor recomendado	Alguns tipos de arquivo definidos, por exemplo, texto/html, texto/csv.
Impacto funcional	(Baixo) Esta correção impõe a realização das verificações de validação antes de executar uma ação ao clicar em um anexo em uma aplicação da Now Platform. Não há nenhum impacto potencial, mas a experiência do usuário é alterada.
Risco à segurança	(Médio) Os vetores de ataque de script do lado do cliente vêm de formas diferentes e o abuso de anexo do tipo MIME não é exceção. Os invasores podem abusar dos tipos MIME e colocar conteúdo de script não intencional no anexo do lado da vítima para capturar informações confidenciais. No contexto atual, preencha a propriedade com uma lista de tipos MIME de anexo separados por vírgula que não devem ser renderizados em linha no navegador. Exemplo: texto/html

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Habilitar a lista de proibições para anexos (proteção de segurança da instância)

Use a propriedade *glide.security.attachment_type.use_blacklist* para designar se a Now Platform deve validar o anexo em relação a uma lista de exclusões especificada.

Nota: Não defina a propriedade *glide.security.attachment_type.use_blacklist* como `verdadeira` até que você tenha configurado as propriedades *glide.attachment.blacklisted.extensions* e *glide.attachment.blacklisted.types*. Para aprender mais, consulte Especificar extensões negadas e Especificar tipos de arquivo negados.

Mais informações

Atributo	Descrição
Nome da propriedade	glide.security.attachment_type.use_blacklist
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Configurar na Central de segurança da instância	Sim
Finalidade	Restringir a operação de upload (Inserir/Gravar/Atualizar) de anexos com extensões e tipos de arquivo questionáveis, como exe, dll, jar, texto/html.
Valor recomendado	verdadeiro
Impacto funcional	(Baixo) Nenhum impacto na funcionalidade, a menos que haja uma tentativa de carregar extensões de arquivo ou tipos de arquivo especificados nas propriedades da lista de exclusões (*glide.attachment.blacklisted.extensions* e *glide.attachment.blacklisted.types*)
Risco à segurança	(Médio) Um usuário mal-intencionado pode carregar anexo infectado por malware com extensões e/ou tipos de arquivos executáveis comuns.
Solução alternativa	Há propriedades disponíveis no sistema de base que tratam do mesmo problema com listas de inclusões em vez de listas de exclusões. Para saber mais, consulte: • Restringir extensões de arquivo • Carregar restrição de tipo MIME

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Habilitar restrições de download de arquivo (proteção de segurança da instância)

Use a propriedade *glide.ui.strict_customer_uploaded_static_content* para habilitar restrições nos tipos de arquivo que podem ser baixados quando forem carregados usando a funcionalidade Carregar arquivo.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você usa esta propriedade com a propriedade *glide.ui.strict_customer_uploaded_content_types*, que cria uma lista delimitada por vírgulas de tipos de arquivo restritos para download. Para saber mais, consulte Tipos de arquivo para download.

Mais informações

Atributo	Descrição
Nome da propriedade	glide.ui.strict_customer_uploaded_static_content
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Configurar em Central de segurança da instância	Não
Finalidade	Garantir que os tipos de arquivo seguros sejam baixados da aplicação.
Valor recomendado	verdadeiro
Impacto funcional	(Baixo) Esta correção impõe restrição de downloads de arquivo com base nos valores especificados na propriedade *glide.ui.strict_customer_uploaded_content_types*. Para saber mais, consulte Tipos de arquivo para download.
Risco à segurança	(Médio) As restrições de download de arquivo devem ser aplicadas a todas as fontes de entrada de usuário não confiáveis.

Impor o upload estrito da imagem do usuário (proteção de segurança da instância)

Use a propriedade *glide.security.strict.user_image_upload* para habilitar o Controle de acesso para carregar/atualizar uma imagem de perfil quando executada em um registro de usuário.

Esta configuração abre a possibilidade de um usuário não autorizado carregar uma imagem no perfil de outro usuário.

- Quando você define esta propriedade como **verdadeira**, as ACLs de tabelas são aplicadas ao carregar fotos, permitindo que somente usuários autorizados carreguem uma imagem.
- Quando você a define como **falsa**, as ACLs não são aplicadas nos carregamentos de imagem para o campo Foto.

Mais informações

Atributo	Descrição
Nome da propriedade	glide.security.strict.user_image_upload
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Configurar na Central de segurança da instância	Sim

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Finalidade	Restringir o carregamento da imagem do usuário somente a usuários autorizados.
Valor recomendado	verdadeiro
Impacto funcional	(Baixo) Nenhum impacto na funcionalidade, já que os usuários autorizados ainda podem carregar imagens em seus perfis de usuário.
Risco à segurança	(Médio) Quando você define esta propriedade como **falsa**, um usuário autenticado pode carregar uma imagem na conta de outro usuário sem autorização.

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Forçar download de tipos MIME (proteção de segurança de instância)

Use a propriedade *glide.ui.attachment.force_download_all_mime_types* para forçar o download de todos os anexos do tipo MIME.

Nota: Se você definir a propriedade **Forçar download de tipos MIME** como **verdadeira**, ela substituirá a propriedade **Tipos MIME para download**, que é uma lista delimitada por vírgulas de tipos MIME para download. Para saber mais, consulte Tipos MIME para download.

Mais informações

Atributo	Descrição
Nome da propriedade	glide.ui.attachment.force_download_all_mime_types
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Configurar em Central de segurança da instância	Não
Finalidade	Impor o download de todos os anexos, em vez de executá-los no navegador.
Valor recomendado	verdadeiro
Impacto funcional	(Médio) Esta correção impõe o download de todos os anexos. Não há nenhum impacto na funcionalidade, mas resulta em uma experiência do usuário alterada.
Risco à segurança	(Alto) Para reduzir os ataques de script do lado do cliente, os anexos de arquivo devem ser baixados à força, em vez de serem renderizados no contexto do navegador.
Referências	Propriedades do sistema disponíveis

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Restringir extensões de arquivo (proteção de segurança da instância)

Defina quais tipos de arquivo podem ser carregados em sua instância usando a propriedade do sistema *glide.attachment.extensions*. Esta propriedade usa uma lista

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

delimitada por vírgulas de tipos de extensão de arquivo permitidos. Somente os tipos de extensão de arquivo especificados podem ser carregados como anexos.

Use a propriedade *glide.attachment.extensions* em sua instância para fornecer os seguintes benefícios:

Segurança aprimorada

Use esta propriedade para melhorar a segurança, impedindo que os usuários carreguem arquivos prejudiciais como anexos, por ex., vírus. Proteja sua instância bloqueando tipos que são normalmente usados por scripts ou programas executáveis.

Evite tipos de arquivo incompatíveis

Use esta propriedade para impedir que os usuários carreguem arquivos incompatíveis. Por exemplo, alguns navegadores não são compatíveis com ícones no formato PNG. Ao não incluir a extensão do arquivo `png`, você pode impedir que os usuários carreguem arquivos PNG.

Importante: Esta propriedade não restringe arquivos com base no tipo de arquivo real (tipo MIME), mas somente com base na extensão. Para restringir uploads com base no tipo MIME, configure a propriedade *glide.security.file.mime_type.validation* depois de terminar de configurar a propriedade *glide.attachment.extensions*. Para obter detalhes sobre como configurar *glide.security.file.mime_type.validation*, consulte Carregar restrição de tipo MIME.

Etapas para configurar

1. No navegador de filtros de sua instância, insira `sys_properties.list` e pressione Enter.
2. Encontre e abra a propriedade *glide.attachment.extensions*.
3. No campo **Valor**, insira as extensões de arquivo que você deseja permitir o carregamento como anexos. Separe várias entradas no campo usando vírgulas. Um exemplo de valor para várias entradas seria *doc,docx,xls,xlxs,pdf,jpeg,jpg,png,ico*.

   Nota: Se não houver tipos de arquivo especificados no campo **Valor**, qualquer tipo de arquivo poderá ser carregado como anexo.

4. Clique em **Atualizar** para salvar suas mudanças.

Mais informações

Atributo	Descrição
Nome da propriedade	glide.attachment.extensions
Tipo de configuração	Propriedade do sistema (/sys_properties_list.do)
Configurável na Central de segurança da instância	Não
Finalidade	Habilitar somente extensões de arquivo aceitáveis a serem carregadas durante o anexo de arquivo. Isso bloqueia uma tentativa de carregar extensões potencialmente mal-intencionadas.
Valor recomendado	Algumas extensões de arquivo definidas, como doc, docx, pdf, xls, xlsx

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Impacto funcional	(Médio) Esta correção restringe todas as extensões de arquivo, exceto aquelas na lista de inclusões. Não há nenhum impacto na funcionalidade, a menos que haja uma tentativa de carregar qualquer arquivo que não seja de uma extensão aceita pela organização.
Risco à segurança	(Médio) Como a verificação do tipo MIME depende desta propriedade, é recomendável reduzir as vulnerabilidades relacionadas ao upload de arquivo mal-intencionado.

Restringir o acesso não autenticado aos anexos (proteção de segurança da instância)

Use a propriedade *glide.image_provider.security_enabled* para controlar as configurações de segurança das imagens. Se definida como **verdadeira**, as imagens serão visíveis somente para usuários autenticados e autorizados. Se definida como **falsa**, as imagens ficarão visíveis para qualquer pessoa com um URL para o anexo.

Mais informações

Atributo	Descrição
Nome da propriedade	glide.image_provider.security_enabled
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Configurar na Central de segurança da instância	Sim
Finalidade	Impedir o acesso não autenticado ao anexo quando renderizado usando o formato .iix.
Valor recomendado	verdadeiro
Impacto funcional	(Baixo) Nenhum impacto significativo na funcionalidade. A experiência do usuário pode ser um pouco afetada porque o usuário que acessava diretamente o .iix deve passar pela autenticação.
Risco à segurança	(Alto) A restrição deve ser aplicada para usuários não autenticados, pois alguns anexos podem conter informações confidenciais.
Referências	Administrar anexos Propriedades do sistema disponíveis

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Especificar extensões de anexo excluídas (proteção de segurança da instância)

Ao habilitar a validação da lista de exclusões na Now Platform, use a propriedade *glide.attachment.blacklisted.extensions* para criar uma lista delimitada por vírgulas de tipos de extensão de arquivo carregáveis restritos. O upload dos tipos de extensão de arquivo especificados é restrito.

Pré-requisitos

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Defina esta propriedade antes de definir a propriedade *glide.security.attachment_type.use_blacklist* como verdadeira. Para saber mais, consulte Habilitar lista de bloqueios de anexos.

Mais informações

Atributo	Descrição
Nome da propriedade	glide.attachment.blacklisted.extensions
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Configurar na Central de segurança da instância	Sim
Finalidade	Restringir a operação de upload (Inserir/Gravar/ Atualizar) de anexos com extensões de arquivo questionáveis.
Tipo	Cadeia de caracteres
Valor recomendado	Extensões de arquivo especificadas pelo usuário. Exemplos comuns incluem ex, dll, xslx.
Impacto funcional	(Baixo) Nenhum impacto na funcionalidade, a menos que haja uma tentativa de carregar qualquer extensão de arquivo especificada nesta propriedade.
Risco à segurança	(Médio) Um usuário mal-intencionado pode carregar anexo infectado por malware com extensões de arquivos executáveis comuns.
Solução alternativa	As propriedades estão disponíveis na funcionalidade do sistema básico que aborda o mesmo problema, com lista de inclusões em vez de lista de exclusões. Para saber mais, consulte: • Restringir extensões de arquivo • Carregar restrição de tipo MIME

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Especificar os tipos de arquivo de anexo excluídos (proteção de segurança da instância)

Quando a validação da lista de exclusões estiver habilitada na Now Platform, use a propriedade *glide.attachment.blacklisted.types* para criar uma lista delimitada por vírgulas de tipos de arquivo carregáveis restritos. O upload dos tipos de arquivo especificados é restrito.

Pré-requisitos

Defina esta propriedade antes de definir a propriedade *glide.security.attachment_type.use_blacklist* como verdadeira. Para saber mais, consulte Habilitar lista de bloqueios de anexos.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mais informações

Atributo	Descrição
Nome da propriedade	glide.attachment.blacklisted.types
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Configurar na Central de segurança da instância	Sim
Finalidade	Restringir a operação de upload (Inserir/Gravar/Atualizar) de anexos com tipos de arquivo questionáveis. Exemplo: texto/html
Valor recomendado	Alguns tipos de arquivo definidos (por exemplo: texto/html, texto/csv).
Impacto funcional	(Baixo) Nenhum impacto na funcionalidade, a menos que haja uma tentativa de carregar qualquer tipo de arquivo especificada nesta propriedade.
Risco à segurança	(Médio) Um usuário mal-intencionado pode carregar anexo infectado por malware com tipos de arquivos executáveis comuns.
Solução alternativa	As propriedades estão disponíveis na funcionalidade do sistema básico que aborda o mesmo problema com a lista de inclusões em vez da lista de exclusões. Para saber mais, consulte: • Restringir extensões de arquivo • Carregar restrição de tipo MIME

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Tipos de arquivo para download (proteção de segurança de instância)

Use a propriedade *glide.ui.strict_customer_uploaded_content_types* para criar uma lista delimitada por vírgulas de tipos de arquivo para download restritos. Os tipos de arquivos especificados são os únicos que podem ser baixados como conteúdo estático de uma instância.

Mais informações

Atributo	Descrição
Nome da propriedade	glide.ui.strict_customer_uploaded_content_types
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Configurar na Central de segurança da instância	Sim
Finalidade	Garantir que somente os tipos de arquivo nas listas de inclusões possam ser baixados.
Valor recomendado	Especificado pelo usuário (Comum: doc, docx, xls, xlsx, pdf e assim por diante)

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Impacto funcional	(Médio) Somente os arquivos que estão nas listas de inclusões podem ser baixados, o que pode afetar a política da organização. A lista de inclusões separada por vírgulas deve ser modificada para estar em conformidade com a política da organização para tipos de arquivo para download aceitáveis.
Risco à segurança	(Baixo) As restrições de download de arquivo devem ser aplicadas a todas as fontes de entrada de usuário não confiáveis.
Referências	Tipos de conteúdo

Etapas para configurar

1. Navegue até **/sys_properties_list.do** .
2. Pesquise pela propriedade *glide.ui.strict_customer_uploaded_content_types*.
3. Especifique os tipos de arquivo para download aceitáveis em uma lista separada por vírgulas conforme mostrado e clique em **Atualizar**.
   Um exemplo de um valor formatado corretamente para a lista seria *ico,gif,png,jpg,jpeg,bmp,ogg,mp3,doc,docx,xls,pdf*.

Carregar restrição de tipo MIME (proteção de segurança de instância)

Use a propriedade *glide.security.file.mime_type.validation* para ativar a verificação de tipo MIME para uploads. Você pode habilitar (definir a propriedade como **verdadeira**) ou desabilitar (defini-la como **falsa**) a validação do tipo MIME para anexos de arquivo.

Pré-requisitos

Antes de definir esta propriedade, defina a propriedade *glide.attachment.extensions*. Somente as extensões especificadas em *glide.attachment.extensions* são verificadas quanto ao tipo MIME durante o upload. Para saber mais, consulte Restringir extensões de arquivo.

Mais informações

Atributo	Descrição
Nome da propriedade	glide.security.file.mime_type.validation
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Configurar na Central de segurança da instância	Sim
Finalidade	Impor a verificação de tipo MIME/bytes mágicos durante uploads de arquivo.
Valor recomendado	verdadeiro
Impacto funcional	(Médio) Esta correção permite a verificação do tipo MIME nos anexos da aplicação. Não há nenhum impacto na funcionalidade, a menos que haja uma intenção mal-intencionada ao carregar os arquivos,

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
	já que esta validação está apenas verificando se há falhas de sincronização entre o tipo MIME e os dados.
Risco à segurança	(Médio) Para reduzir vulnerabilidades, como inclusão de arquivo e uploads de arquivo mal-intencionados, a verificação do tipo MIME deve ser habilitada.
Referências	Administrar anexos

Consulte Configurações de proteção de segurança da instância para obter detalhes sobre como configurar propriedades de proteção.

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Segurança de e-mail (proteção de segurança da instância)

Esta seção contém controles de segurança que um administrador pode configurar para garantir que as políticas de segurança apropriadas estejam em vigor para todos os e-mails de entrada.

Converter HTML de e-mail de entrada (proteção de segurança da instância)

Use a propriedade *glide.email.inbound.convert_html_inline_attachment_references* para especificar se o e-mail de entrada deve ser convertido em HTML para que as imagens do e-mail apareçam na visualização do corpo do HTML.

O seguinte acontece quando a propriedade do sistema *glide.email.inbound.convert_html_inline_attachment_reference* é definida como falsa:

- Na Now Platform, links de cid quebrados (ID de conteúdo) aparecem no lugar das imagens recebidas. O formato no qual a imagem do e-mail aparece depende da configuração da propriedade no momento em que o e-mail é recebido, e não da configuração da propriedade atual.
- O conteúdo "mal-intencionado" recebido no anexo não é mencionado no HTML do e-mail. O próprio anexo é armazenado na tabela sys_attachment.
- O processamento de e-mail de entrada não atualizará os dados HTML do e-mail para refletir o local armazenado do anexo na tabela sys_attachment. Isso resulta no seguinte:
  - Imagens em linha não aparecem na exibição de e-mail no formatador de atividades.

    Nota: Para resolver esse problema com o formatador de atividades, primeiro verifique se não há problemas de segurança. Em seguida, defina a propriedade do sistema *glide.email.inbound.convert_html_inline_attachment_reference* como **verdadeira** para permitir que os e-mails futuros recebidos contenham o URL HTML necessário para fazer referência à imagem. Alterar a propriedade não atualiza os e-mails já recebidos. O novo valor afeta somente os e-mails de entrada recebidos após a mudança da propriedade.

  - Imagens em linha não aparecem quando o e-mail é exibido na visualização HTML do e-mail.
  - Ao anexar email.body_htm em ações de entrada entre marcadores de código, as imagens estão ausentes.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Pré-requisitos

Antes de definir essa propriedade, defina a propriedade *glide.email.read.active* como verdadeira. Para saber mais, consulte Habilitar usando seu próprio servidor POP3.

Mais informações

Atributo	Descrição
Nome da propriedade	glide.email.inbound.convert_html_inline_attachment_references
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Configurar na Central de segurança da instância	Sim
Finalidade	Restringir a renderização de imagem na visualização do corpo HTML.
Valor recomendado	falso
Impacto funcional	(Médio) Depois que esta propriedade é configurada, o usuário não pode ver a visualização da imagem no corpo do e-mail.
Risco à segurança	(Médio) Se a propriedade não estiver habilitada, um invasor poderá enviar imagem mal-intencionada contendo malware.
Referências	Propriedades do e-mail Configuração de entrada de e-mails

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Pontuação e filtragem de spam de e-mail (proteção de segurança da instância)

Instale o plug-in Email Filter (*com.glide.email_filter*) para instalar a filtragem de e-mail na instância. Esta filtragem identifica cabeçalhos existentes, o que permite que você decida o que fazer com o e-mail com base no cabeçalho associado.

Cada mensagem enviada por meio de servidores de e-mail da Now Platform é avaliada quanto à probabilidade de ser spam.

Nota: Se uma instância usar um servidor de e-mail privado, este tópico não será aplicável. Para mais informações, consulte Pontuação e filtragem de spam de e-mail.

Pré-requisitos

Antes de definir esta propriedade:

- Defina a propriedade *glide.email.read.active* como verdadeira. Para saber mais, consulte Habilitar usando seu próprio servidor POP3.
- Este filtro substitui a propriedade *glide.pop3.ignore_headers*. Para saber mais, consulte Propriedades do sistema disponíveis.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mais informações

Atributo	Descrição
Nome do Plug-in	com.glide.email_filter
Tipo de configuração	Definição do sistema > Plug-ins
Configurar na Central de segurança da instância	Sim
Finalidade	Aplicar a filtragem para evitar o envio de e-mails de spam.
Valor recomendado	Ativo
Impacto funcional	(Baixo) O e-mail nunca é filtrado, bloqueado ou colocado em quarentena da instância como parte da pontuação de spam. Ele é apenas pontuado e enviado para a instância. Toda a filtragem é feita na instância com o plug-in Filtros de e-mail.
Risco à segurança	(Médio) Filtros de e-mail permite que os administradores usem um construtor de condições ou script condicional para especificar quando ignorar e-mails mal-intencionados de entrada de remetentes conhecidos/desconhecidos.
Referências	Filtros de e-mail https://support.servicenow.com/kb_view.do?sysparm_article=KB0549426

Para saber mais sobre como ativar um plug-in, consulte Ativar um plug-in.

Restringir o acesso a e-mails com tabela de destino vazia (proteção de segurança de instância)

Ative a propriedade *glide.email.email_with_no_target_visible_to_all* para restringir o acesso do usuário a e-mails, a menos que ele tenha enviado o e-mail ou tenha uma função de administrador.

Usuários não autorizados podem acessar e-mails na tabela E-mails [sys_email] que não tenham um registro de destino. Em vez de impor ACLs em entradas de e-mail, esta propriedade restringe o acesso somente ao remetente do e-mail e aos usuários com a função de administrador.

Nota: Os e-mails enviados e recebidos de/para a instância aparecem na tabela E-mails [sys_email]. No entanto, somente os e-mails recebidos que foram marcados com um estado de Erro e Ignorado devem ter uma tabela de destino vazia.

Mais informações

Atributo	Descrição
Nome da propriedade	glide.email.email_with_no_target_visible_to_all
Tipo de configuração	Propriedades do sistema [sys_properties]

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Configurar na Central de segurança da instância	Sim
Finalidade	Bloquear o cliente de e-mail de mostrar e-mails quando o usuário não autorizar o acesso.
Valor recomendado	falso
Impacto funcional	(Baixo) Os usuários não podem mais ver e-mails cuja tabela de destino esteja vazia, a menos que sejam um administrador ou o remetente do e-mail.
Risco à segurança	(Médio) Se a propriedade não estiver habilitada, os usuários não autorizados poderão acessar qualquer e-mail em que o campo target_table esteja vazio.
Referências	Propriedades avançadas de e-mail https://support.servicenow.com/kb_view.do?sysparm_article=KB0690043

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Restringir e-mails por domínio para criação de usuário (proteção de segurança da instância)

Use a propriedade *glide.user.trusted_domain* para especificar a lista separada por vírgulas de domínios confiáveis usados na criação de usuários de e-mails de entrada.

Por padrão, um asterisco (*) é usado para confiar em todos os domínios. Domínios específicos devem ser fornecidos se não for necessário permitir e-mails de todos os domínios. A instância ignora o e-mail recebido de outros domínios, a menos que seja do endereço de um usuário existente. A instância não cria usuários convidados de e-mail de domínios não confiáveis.

Pré-requisitos

Antes de definir esta propriedade:

- Defina a propriedade *glide.email.read.active* como verdadeira. Para saber mais, consulte Habilitar usando seu próprio servidor POP3.
- Defina a propriedade *glide.pop3readerjob.create_caller* como verdadeira. Para saber mais, consulte Ativar a criação automática de usuários.

> **Nota:** Ignore a propriedade *glide.user.default_password* se *glide.pop3readerjob.create_caller* estiver definida como **falsa**.

Mais informações

Atributo	Descrição
Nome da propriedade	glide.user.trusted_domain
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Configurar na Central de segurança da instância	Sim
Valor recomendado	Lista separada por vírgulas de domínios confiáveis [por exemplo, servicenow.com/br/ (um nome de domínio específico)].
Impacto funcional	(Médio) Depois que esta propriedade é configurada, a instância aceita somente e-mails de domínios confiáveis. Se você não incluir o domínio na lista confiável, haverá um impacto para os usuários convidados porque as contas serão criadas automaticamente.
Risco à segurança	(Médio) Se a propriedade não estiver habilitada, um invasor poderá usar uma campanha de falsificação/spam de e-mail para enviar vários e-mails, resultando na criação de mais usuários convidados desnecessários.
Referências	Propriedades do e-mail Configuração de entrada de e-mails

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Validação de entrada (proteção de segurança da instância)

O Now Platform executa a validação de entrada para evitar problemas resultantes da entrada de dados malformados.

Esta seção descreve os controles de segurança em Now Platform que um administrador pode configurar para minimizar a entrada de dados malformados, independentemente da origem. Essas origens incluem entrada manual do usuário ou de uma infraestrutura, entidades externas ou sistemas de banco de dados.

Permitir código HTML incorporado (proteção de segurança da instância)

Use a propriedade *glide.ui.security.allow_codetag* para desabilitar o suporte para incorporação de código HTML criado usando o marcador [code].

A Now Platform atenua muitos ataques de injeção e entre sites implementando técnicas de escape e codificação. Como resultado, os usuários não podem escrever/enviar entradas no formato HTML para campos de diário. Mas os campos de diário podem renderizar texto entre tags de código como HTML.

- No entanto, há um risco de segurança associado. Se definido como `verdadeiro`, usuários mal-intencionados podem gravar código HTML JS prejudicial que pode ser executado em um navegador do cliente diferente após a renderização de campos de diário.
- Defina esta propriedade como `falsa` para que os administradores possam impedir que os campos de diário renderizem o código HTML, desabilitando o suporte para o marcador `[code]`.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mais informações

Atributo	Descrição
Nome da propriedade	glide.ui.security.allow_codetag
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Configurar na Central de segurança da instância	Sim
Finalidade	Proteger contra scripts entre sites e execução de scripts mal-intencionados
Valor recomendado	falso
Impacto funcional	(Médio) Esta correção impõe a codificação HTML na IU e renderiza os resultados codificados para o usuário. Esta propriedade é definida como `verdadeira` por padrão. Nesse estado, sua instância exibe HTML renderizado em formulários e campos de diário. Se esta propriedade estiver definida como `falsa`, o HTML não será renderizado corretamente e as tags HTML poderão aparecer nos campos de diário em formulários. Ela pode ter um impacto adverso na funcionalidade e nas interações do usuário com os dados resultantes.
Risco à segurança	(Médio) A validação de entrada deve ocorrer na aplicação para defesa contra ataques de script entre sites. Esses ataques permitem que scripts externos sejam executados na sessão de um usuário no contexto do navegador logado. Os invasores podem usá-los para roubar informações da sessão e dados confidenciais.
Referências	Restringir o marcador CODE nos campos de diário Renderizar entradas do campo de diário como HTML Configurações de Alta Segurança

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Permitir marcadores JavaScript em HTML incorporado (proteção de segurança da instância)

A propriedade *glide.ui.security.codetag.allow_script* desabilita o suporte para incorporação de código JavaScript no HTML criado usando o marcador [code].

Nota: Por padrão, essa propriedade é definida como **falsa** na versão Vancouver e posteriores e os administradores não podem mudá-la. Para um caso de uso em que a propriedade precise ser alterada, entre em contato com o suporte ao cliente.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A Now Platform atenua muitos ataques de injeção e entre sites implementando técnicas de escape e codificação. Como resultado, os usuários não podem escrever e enviar entradas no formato HTML para campos de diário. No entanto, os campos de diário podem renderizar texto entre marcadores de código como HTML.

- No entanto, há um risco de segurança associado. Se definida como **verdadeira**, usuários mal-intencionados podem gravar código HTML JavaScript prejudicial que pode ser executado em um navegador do cliente diferente após a renderização de campos de diário.
- Defina esta propriedade como **falsa** para que os administradores possam impedir que os campos de diário renderizem o código HTML JavaScript, desabilitando o suporte para o marcador `[code]`.

Mais informações

Atributo	Descrição
Nome da propriedade	glide.ui.security.codetag.allow_script
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Configurar na Central de segurança da instância	Sim
Finalidade	Protege contra scripts entre sites e execução de scripts mal-intencionados
Valor recomendado	falso
Valor-padrão	falso
Impacto funcional	(Médio) Esta correção impõe o escape de JavaScript na IU e renderiza os resultados codificados para o usuário. Ela pode ter um impacto na funcionalidade com base na interação do usuário da instância com os dados resultantes.
Risco à segurança	(Alto) A validação de entrada deve ocorrer na aplicação para defesa contra ataques de script entre sites. Esses ataques permitem que scripts externos sejam executados na sessão do usuário no contexto do navegador logado. Os invasores podem usá-los para roubar informações da sessão e dados confidenciais.
Referências	Restringir o marcador CODE nos campos de diário Renderizar entradas do campo de diário como HTML Configurações de Alta Segurança

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Verificar Html não limpo (proteção de segurança da instância)

Use a propriedade *com.glide.security.check_unsanitized_html* para impor o comportamento de limpeza dos campos translated_html globalmente para atribuições de campo.

HTML é um dos tipos que podem ser atribuídos aos campos de dicionário. A atribuição de campos HTML a qualquer tipo de campo fornece a funcionalidade para formatar conteúdo usando marcadores HTML (por exemplo, `<p>`, `<a href>`, `<b>`, `<font>`, `<img>`). Para evitar atividades mal-intencionadas, determinados marcadores HTML podem ser desabilitados usando uma lista de bloqueios. Esta propriedade impedirá que marcadores não permitidos sejam usados em campos translated_html em sua instância.

- Defina esta propriedade para **impor** o comportamento de limpeza dos campos translated_html.
- Defina a propriedade como **desabilitada** para desativar a limpeza de HTML para permitir marcadores de HTML bloqueados em campos translated_html.

Mais informações

Atributo	Descrição
Nome da propriedade	com.glide.security.check_unsanitized_html
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Configurar na Central de segurança da instância	Sim
Finalidade	Impedir o uso de marcadores HTML não seguros para proteger contra ataques, como script entre sites.
Tipo	Cadeia de caracteres
Valor recomendado	*impor*
Impacto funcional	(Médio) Esta correção impõe que a limpeza de HTML ocorra na IU e renderiza os campos html traduzidos para o usuário. Isso pode afetar a legibilidade e a formatação.
Risco à segurança	(Alto) A validação de entrada deve ocorrer na aplicação para defesa contra ataques de script entre sites. Esses ataques permitem que scripts externos sejam executados nas sessões do usuário no contexto do navegador conectado. Os invasores podem usá-los para roubar informações da sessão e dados confidenciais.
Referências	Limpador de HTML

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Área restrita para scripts gerados pelo cliente (proteção de segurança da instância)

Use a propriedade *glide.script.use.sandbox* para habilitar a área restrita de script.

Há dois casos na Now Platform que permitem ao cliente enviar scripts ao servidor para avaliação:

Filtros ou consultas

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

É válido enviar um filtro para o servidor, como `assigned_to=JavaScript:getMyGroups ()`.

API do sistema

A chamada de API permite que o cliente execute scripts arbitrários no servidor e receba uma resposta.

Se você habilitar a área restrita de script, o script que está sendo avaliado em qualquer um desses dois pontos de entrada será executado em uma área restrita com direitos reduzidos, com as seguintes características:

- Somente as regras de negócios marcadas como cliente chamável estão disponíveis na área restrita.
- Somente as inclusões de script marcadas como cliente chamável estão disponíveis na área restrita.
- Certas chamadas de API (em grande parte, mas não inteiramente, limitadas àquelas que lidam com acesso direto ao banco de dados não são permitidas.
- Você não pode inserir, atualizar ou excluir dados de dentro da área restrita. Por exemplo, todas as chamadas para `current.update ()` serão ignoradas. Se você executar a Now Platform sem habilitar a área restrita de script, nenhuma dessas restrições se aplicará.

Mais informações

Atributo	Descrição
Nome da propriedade	glide.script.use.sandbox
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Configurar na Central de segurança da instância	Sim
Finalidade	Impor a validação das consultas JavaScript do lado do cliente que são iniciadas na plataforma
Valor recomendado	verdadeiro
Impacto funcional	(Alto) Essa correção impõe a validação das consultas JavaScript do lado do cliente que são iniciadas na contra a Now Platform Há um possível impacto se o cliente tiver personalizações que incluem consultas JavaScript codificadas para executar operações CRUD.
Risco à segurança	(Alto) A Now Platform fornece uma ampla variedade de recursos e funcionalidades por meio de consultas JavaScript. No entanto, sem a autorização e a validação apropriadas, é possível que um invasor execute operações não autorizadas na plataforma.
Referências	Configurar propriedade da área restrita de script *glide.script.use.sandbox* pertence à mesma família de propriedades que protegem e restringem a execução de scripts originados no cliente:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
	• *glide.script.allow.ajaxevaluate*: Consulte Habilitar AJAXEvaluate. • *glide.script.secure.ajaxgliderecord*: Consulte Habilitar a verificação de ACL de AJAXGlideRecord.

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Habilitar AJAXEvaluate (proteção de segurança da instância)

Use a propriedade *glide.script.allow.ajaxevaluate* para restringir a execução arbitrária do client script usando a API do sistema no lado do servidor.

Há dois casos em Now Platform que permitem ao cliente enviar scripts ao servidor para avaliação:

Filtros e/ou consultas

É válido enviar um filtro para o servidor, como `assigned_to=javascript:getMyGroups()`.

API do sistema

A chamada de API AJAXEvaluate permite que o cliente execute scripts arbitrários no servidor e receba uma resposta.

Quando você define esta propriedade como **falsa**, o Now Platform não habilita o uso da chamada de API AJAXEvaluate do client script.

Mais informações

Atributo	Descrição
Nome da propriedade	glide.script.allow.ajaxevaluate
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Configurar na Central de segurança da instância	Sim
Finalidade	Restringir a execução arbitrária do client script usando a API do sistema no lado do servidor.
Valor recomendado	falso
Impacto funcional	(Médio) Esta correção força o processador AJAEvaluate a ser desligado. Isso pode afetar a funcionalidade se você estiver usando explicitamente o processador de avaliação AJAX como parte de qualquer script personalizado. Para obter mais informações, consulte GlideAjax.
Risco à segurança	(Alto) AJAXEvaluate pode permitir que código JavaScript arbitrário seja executado no navegador do cliente aplicando os objetos do lado do servidor.
Referências	Configurar propriedade da área restrita de script

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
	GlideAjax *glide.script.allow.ajaxevaluate* pertence à mesma família de propriedades que protegem e restringem a execução de scripts originados no cliente: • *glide.script.use.sandbox*: Consulte Área restrita de scripts gerados pelo cliente • *glide.script.secure.ajaxglideerecord*: Consulte Habilitar a verificação de ACL de AJAXGlideRecord.

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Escape da fórmula do Excel (proteção de segurança da instância)

Use a propriedade *glide.export.escape_formulas* para impedir a injeção do Excel, também conhecida como injeção de fórmula.

A injeção do Excel ocorre quando os sites incorporam entradas não confiáveis em arquivos do Excel. Quando você usa um aplicativo de planilha, como o Microsoft Excel ou o LibreOffice Call, para abrir um arquivo, todas as células que começam com +, -, = ou @ são interpretadas como uma fórmula. Quando você define a propriedade *glide.export.escape_formulas* como **verdadeira**, os valores de cadeia de caracteres que começam com +, -, = ou @ são anexados com um único apóstrofo ao exportar para arquivos CSV, XLS ou XLSX.

Mais informações

Atributo	Descrição
Nome da propriedade	glide.export.escape_formulas
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Configurar na Central de segurança da instância	Sim
Finalidade	Evitar a aplicação no Excel ou na injeção de fórmula.
Valor recomendado	verdadeiro
Impacto funcional	(Baixo) Fórmulas mal-intencionadas podem ser usadas para sequestrar o computador do usuário, explorando vulnerabilidades no software de planilha.
Risco à segurança	(Médio) As fórmulas maliciosas representam um risco mesmo quando a planilha de incorporação não contém informações confidenciais, pois elas podem ser usadas para comprometer o computador do visualizador.
Solução alternativa	Como alternativa, considere remover todos os espaços em branco à direita onde for possível e limitar todos os dados fornecidos pelo cliente a caracteres alfanuméricos.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Referências	Propriedades do sistema disponíveis

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Escape de HTML (proteção de segurança da instância)

Use a propriedade *glide.ui.escape_html_list_field* para forçar escapes de HTML para campos HTML em uma exibição de lista.

HTML é um dos tipos que podem ser atribuídos aos campos de dicionário. A atribuição de campos HTML a qualquer tipo de campo fornece a funcionalidade para formatar conteúdo usando códigos HTML (por exemplo, `<p>`, `<a href>`, `<b>`, `<font>`, `<img>`). Um usuário mal-intencionado pode injetar código HTML no campo de formulário para executar scripts indesejados em diferentes sessões de cliente/usuário.

- Defina esta propriedade como **verdadeira** para executar um escape de HTML antes que os registros/campos sejam renderizados no navegador quando a tabela aparecer como uma exibição de lista.
- Se estiver definida como **falsa** e você selecionar essa coluna em uma exibição de lista ao exibir uma tabela ou lista de registros, esses campos em formato HTML poderão ser exibidos.

Mais informações

Atributo	Descrição
Nome da propriedade	glide.ui.escape_html_list_field
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Configurar na Central de segurança da instância	Sim
Finalidade	Prevenir ataques de script entre sites à aplicação.
Valor recomendado	verdadeiro
Impacto funcional	(Médio) Esta correção impõe a codificação de HTML na IU no nível de analisador HTML e, então, renderiza os resultados codificados para o usuário. Ela pode ter um impacto na funcionalidade com base na interação do usuário da instância com os dados resultantes.
Risco à segurança	(Alto) A validação de entrada deve ocorrer na aplicação para defesa contra ataques de script entre sites. Esses ataques permitem que scripts externos sejam executados nas sessões do usuário no contexto do navegador conectado. Os invasores podem usá-los para roubar informações da sessão e dados confidenciais.
Referências	Configurações de Alta Segurança

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Escape do JavaScript (proteção de segurança da instância)

Use a propriedade *glide.html.escape_script* para forçar o escape de marcadores JavaScript (`<script></script>`) em campos HTML nas exibições de lista.

HTML é um dos tipos que podem ser atribuídos aos campos de dicionário. A atribuição de campos HTML a qualquer tipo de campo fornece a funcionalidade para formatar conteúdo usando códigos HTML (por exemplo, `<p>`, `<a href>`, `<b>`, `<font>`, `<img>`). Se você definir *glide.html.escape_script* como **falsa**, os marcadores (`<script></script>`) podem surgir quando você selecionar essa coluna em uma exibição de lista ao exibir uma tabela ou lista de registros.

Um invasor mal-intencionado pode inserir código JavaScript incorporando-o nos marcadores (`<script></script>`). O invasor pode se aproveitar ao injetar um vetor JS sofisticado que pode ser executado quando qualquer usuário abrir o registro da tabela.

Mais informações

Atributo	Descrição
Nome da propriedade	glide.html.escape_script
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Configurar na Central de segurança da instância	Sim
Finalidade	Prevenir ataques de script entre sites contra uma aplicação.
Valor recomendado	verdadeiro
Impacto funcional	(Médio) Esta correção impõe o escape de JavaScript na IU e renderiza os resultados codificados para o usuário. Ela pode ter um impacto na funcionalidade com base na interação do usuário da instância com os dados resultantes.
Risco à segurança	(Alto) A validação de entrada deve ocorrer na aplicação para defesa contra ataques de script entre sites. Esses ataques permitem que scripts externos sejam executados na sessão do usuário no contexto do navegador logado. Os invasores podem usá-los para roubar informações da sessão e dados confidenciais.
Referências	Propriedades do sistema disponíveis Configurações de Alta Segurança

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Escapar do Jelly (proteção de segurança da instância)

Use a propriedade *glide.ui.escape_all_script* para forçar o escape de todos os scripts injetados no Jelly.

Ela escapa de todas as cadeias de caracteres JS e HTML incluídas em<j:jelly> `...` </j:jelly> antes de serem gravadas no fluxo de saída, evitando que vários problemas de XSS ocorram.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mais informações

Atributo	Descrição
Nome da propriedade	glide.ui.escape_all_script
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Configurar na Central de segurança da instância	Sim

Finalidade	Se a propriedade não estiver definida como **verdadeira**, os desenvolvedores precisarão executar várias etapas em cada script Jelly personalizado para evitar problemas de XSS. Essas etapas incluem localizar as variáveis Jelly enviadas para o fluxo de saída para renderizar em páginas da Web e executar o escape em cada um dos seguintes marcadores:
	`$â {JS:expression}`
	`$â {HTML:expression}`
	OU
	`$â {JS,HTML:expression}`

Valor recomendado	verdadeiro
Impacto funcional	(Médio) Esta correção impõe o escape do Jelly no nível do analisador. Ela pode ter um impacto na funcionalidade na interação do usuário da instância com os dados resultantes.
Risco à segurança	(Alto) A validação de entrada deve ocorrer em todas as entradas do usuário inseridas na aplicação. Ao fazer isso, os ataques de injeção contra a plataforma podem ser defendidos e protegidos.
Solução alternativa	A IU pode ser afetada porque alguns dos scripts e marcadores HTML projetados para renderização em uma página da Web podem aparecer quebrados. Esta correção envia a página codificada de saída para o navegador renderizar. Por exemplo, em vez de `'minha cadeia de caracteres aqui'`, ela pode exibir `'<u>minha cadeia de caracteres aqui</u>`, já que o marcador `<u>` teve o escape correto. Nesse caso, para impedir o escape, adicione o prefixo NOESC à expressão do Jelly para impedir o escape de JS. Por exemplo: • Antes: ($[jvar_context_menus]); • Depois: `($[NOESC: jvar_context_menus]);` • Antes: $[jvar_ui_policy_scripts] • Depois: `$[NOESC: jvar_ui_policy_scripts]`

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Referências	Configurações de Alta Segurança Marcadores Jelly

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Escape do XML (proteção de segurança da instância)

A propriedade *glide.ui.escape_text* força o escape de valores XML no nível do analisador antes de transmiti-los ao navegador do cliente.

Nota: Essa propriedade é definida como **true** por padrão em Vancouver e versões posteriores, e não pode ser alterada pelos administradores. Para um caso de uso em que a propriedade precise ser alterada, entre em contato com o suporte ao cliente.

O script entre sites ocorre quando um invasor injeta JavaScript mal-intencionado em um ponto de entrada. A plataforma/aplicação não consegue escapar do JavaScript malicioso antes de transmiti-lo ao navegador da vítima para execução. O escape neste contexto significa o seguinte:

- **&** --> `&`
- **<** --> `<`
- **>** --> `>`
- **"** --> `"`
- **'** --> `'`
- **/** --> `/`

Exemplo: `<script>alert('XSS Attack');</script>`

Escape: `<script>alert('XSS Attack');</script>`

Mais informações

Atributo	Descrição
Nome da propriedade	glide.ui.escape_text
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Configurar na Central de segurança da instância	Sim
Finalidade	O escape de XML garante que os navegadores não analisem o JavaScript mal-intencionado incorporado em dados não confiáveis e o executem como JavaScript.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
	• Um usuário mal-intencionado pode tentar um ataque XSS para sequestrar a sessão de outros usuários ou redirecionar o usuário para um site mal-intencionado. • A Now Platform contém código para proteger os cookies, mas o escape depende desta propriedade ser definida como **verdadeira**.
Valor recomendado	verdadeiro
Impacto funcional	(Médio) Essa correção impõe a codificação XML no nível do analisador XML na interface do usuário. Ele renderiza os resultados codificados para o usuário, o que pode ter um impacto na funcionalidade com base na interação do usuário da instância com os dados resultantes.
Risco à segurança	(Alto) A validação de entrada deve ocorrer na aplicação para defesa contra ataques de script entre sites. Esses ataques permitem que scripts externos sejam executados na sessão do usuário no contexto do navegador logado. Os invasores podem usá-los para roubar informações da sessão e dados confidenciais.

Solução alternativa	Depois de definir esta propriedade como **verdadeira**, a renderização é interrompida nos marcadores HTML na descrição do item do catálogo ou no texto de ajuda da variável do item do catálogo. Você pode não conseguir usar a formatação HTML em alguns campos.
	
	No entanto, se a propriedade *glide.ui.escape_text* for desativada, todas as expressões JEXL serão prefixadas com um codificador de saída:
	
	`${JS:expression}`
	
	`${HTML:expression}`
	
	ou
	
	`${JS,HTML:expression}`

Referências	Configurações de Alta Segurança

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Limpador de Html (proteção de segurança da instância)

Use a propriedade *glide.html.sanitize_all_fields* para habilitar a inclusão de script HTMLSanitizer, que limpa a entrada de HTML, de acordo com os atributos das listas de exclusões e de inclusões configuradas em um script.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Os tipos de campo disponíveis com dicionário/campos incluem HTML e HTML traduzido. Esses campos de entrada HTML permitem que os usuários gravem entrada no formato HTML, por exemplo:

`<h1>Teste</h1>`), usando os marcadores HTML mais básicos, como `<img>`, `<a href …>`e `<iframe>`.

Isso pode abrir uma porta para que um invasor injete um vetor mal-intencionado com marcadores HTML, como:

```
[<IMG SRC=" &#14; JavaScript:alert('XSS');">] [<IMG
onmouseover="alert('xss')">], [a href="" onclick=alert (/xss/)].
```

Mais informações

Atributo	Descrição
Nome da propriedade	glide.html.sanitize_all_fields
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Configurar na Central de segurança da instância	Sim
Finalidade	Prevenir ataques de script entre sites e injeção de HTML à aplicação
Valor recomendado	verdadeiro
Impacto funcional	(Alto) Esta correção impõe o mecanismo de codificação de saída HTML antes que os dados do usuário sejam renderizados de volta para o usuário. Se o cliente tiver alguma personalização que envolva a renderização do atributo HTML ou dos dados de conteúdo, haverá um impacto na funcionalidade.
Risco à segurança	(Alto) A entrada do usuário deve ser tratada com segurança quando os dados são armazenados e processados na aplicação. Isso reduz os ataques de script entre sites do lado do cliente ao codificar os dados de saída.
Solução alternativa	Esta propriedade limpa todos os campos HTML no sistema. Se você precisar habilitar a limpeza de HTML em campos individuais, consulte Habilitar a limpeza em campos individuais. Você também pode configurar a lista de inclusões ou de exclusões para limpar marcadores HTML e atributos de acordo com a política da sua organização.
Referências	Habilitar o limpador de HTML Limpador de HTML

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Interpolação Jelly/JS (proteção de segurança da instância)

Use a propriedade *glide.ui.jelly.js_interpolation.protect* para garantir que qualquer JavaScript prestes a ser executado em uma página do Jelly esteja protegido contra injeção com a ajuda da interpolação do Jelly.

Quando você define a propriedade como **verdadeira**, uma aplicação passa por uma árvore de scripts Jelly (aninhada). Ela envolve expressões Jelly potencialmente perigosas com um filtro que:

- Escapa dos resultados por segurança, ou
- Se a segurança não puder ser garantida, gera uma SecurityException porque a expressão que seria avaliada representa um possível problema de segurança.

Mais informações

Atributo	Descrição
Nome da propriedade	glide.ui.jelly.js_interpolation.protect
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Configurar na Central de segurança da instância	Sim
Finalidade	Atenuar os ataques de execução de código mal-intencionado que podem ocorrer usando o Jelly Injection.
Valor recomendado	Verdadeiro
Impacto funcional	(Alto) Esta propriedade faz uma melhor estimativa se uma expressão está entre aspas. Ela pode citar incorretamente uma expressão legítima. Nesse caso, pode ser necessário marcar manualmente uma expressão como segura.
Risco à segurança	(Médio) A injeção de JEXL é uma forma de injeção de entrada exclusiva da Now Platform que pode levar à falsificação de solicitação entre sites e à execução de código. Desativar completamente a proteção pode abrir muitas vulnerabilidades de segurança P1.
Solução alternativa	Para marcar manualmente uma expressão como segura, adicione o prefixo SAFE à expressão do Jelly: `${SAFE:sysparm_input};` Adicionar SAFE às cegas a cada expressão é a maneira incorreta de abordar o problema, pois pode abrir uma vulnerabilidade de segurança. • Somente adicione SAFE a uma expressão se você puder garantir que a expressão não contém a entrada do cliente. • Caso contiver, um cliente mal-intencionado pode causar avaliação de JavaScript privilegiado.
Referências	Marcadores Jelly

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
	Configurações de Alta Segurança

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Segurança estrita de solicitação SOAP (proteção de segurança da instância)

Use a propriedade *glide.soap.strict_security* para impor a segurança do serviço da Web.

Esta propriedade usa uma combinação de:

- Desafio/resposta da autenticação básica sobre o protocolo HTTP e
- Controles de acesso no nível do sistema no plug-in Segurança contextual: Role Management.

Se você definir esta propriedade como **verdadeira**, ela executará as seguintes ações:

- Se o usuário tiver a função apropriada para executar a operação, ela verificará a solicitação de entrada do SOAP para validação da autorização da função. Isso ocorre durante chamadas/solicitações do SOAP Web Services feitas em relação a tabelas da Now Platform ao executar operações CRIAR, LER, ATUALIZAR ou EXCLUIR.
- Verifica as ACLs no nível do sistema ao recuperar dados na forma de dados SOAP na tabela.
- Verifica as ACLs no nível de campo para qualquer operação CRUD executada em um campo de tabela.

Mais informações

Atributo	Descrição
Nome da propriedade	glide.soap.strict_security
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Configurar na Central de segurança da instância	Sim
Finalidade	Garantir que as ACLs de segurança sejam verificadas e validadas mesmo quando os registros forem acessados por meio de chamadas SOAP.
Valor recomendado	verdadeiro
Impacto funcional	(Alto) Esta correção impõe o controle de acesso no nível do sistema ao recuperar dados de tabelas/ páginas na forma de dados SOAP na instância. Se houver usuários acessando esses dados, eles serão restritos/terão permissão para acessar os dados com base nas regras de ACL. Para obter as funções padrão que têm acesso aos dados SOAP, consulte Funções SOAP.
Risco à segurança	(Alto) Sem a autorização apropriada configurada nas solicitações SOAP recebidas, um usuário não

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
	autorizado pode obter acesso a conteúdo/dados confidenciais na instância de destino.
Referências	Impor segurança estrita para SOAP de entrada SOAP Web Services

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Comunicações seguras (proteção de segurança da instância)

As propriedades de comunicação segura estão relacionadas à segurança do transporte de tráfego HTTP.

Confiança de certificado (proteção de segurança da instância)

Por padrão, a propriedade *com.glide.communications.trustmanager_trust_all* está definida como **falsa**. A Now Platform confia somente em certificados que ela pode verificar na loja de certificados JVM. Certificados autoassinados e assinados pela empresa não são confiáveis.

Nota: Os valores dessas propriedades são e não podem ser alterados depois de mudados (eles não são reversíveis) Por motivos de segurança, não altere o valor desta propriedade. Se tiver alguma dúvida, entre em contato com Suporte e atendimento ao cliente.

Mais informações

Atributo	Descrição
Nome da propriedade	com.glide.communications.trustmanager_trust_all
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Configurar na Central de segurança da instância	Sim
Finalidade	Impor a validação de certificado para solicitações de saída.
Valor recomendado	falso
Impacto funcional	(Médio) Esta correção impõe validação estrita no campo de CA (autoridade de certificação). Se uma entidade confiável (CA) emitir o certificado, a instância o aceitará para uso posterior.
Risco à segurança	(Médio) Por motivos de confidencialidade e integridade, a aplicação deve validar a CA do certificado antes de usar o certificado para qualquer operação transacional.
Referências	Certificados Verificação de nome de host do cliente HTTP

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Desabilitação de SSLv2/SSLv3 (proteção de segurança da instância)

Use a propriedade *glide.outbound.sslv3.disabled* para forçar o MID Server a usar TLS ao fazer conexões de saída, como solicitações REST e SOAP. Normalmente, as conexões de saída de uma instância são forçadas a usar TLS em vez de SSL.

Mais informações

Atributo	Descrição
Nome da propriedade	glide.outbound.sslv3.disabled
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Configurar na Central de segurança da instância	Sim
Finalidade	Para impor o uso de TLS durante todas as conexões de saída da instância do ServiceNow.
Valor recomendado	verdadeiro
Impacto funcional	(Médio) Esta correção impõe o uso da versão do protocolo TLS na comunicação em HTTPS. Se houver dispositivos que os clientes/usuários da instância estão usando e que não são compatíveis com a comunicação TLS, pode haver uma possível indisponibilidade.
Risco à segurança	(Médio) Versões legadas de SSL foram comprovadas como inseguras quando utilizadas para implementação de shell seguro de HTTP, devido a ataques do lado do cliente, incluindo BEAST e heartbleed de SSL.

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Verificação de nome de host do cliente HTTP

Use *com.glide.communications.httpclient.verify_hostname* para verificar o nome do host e a cadeia de certificados apresentados por hosts SSL remotos.

Defina *com.glide.communications.httpclient.verify_hostname* como **verdadeiro** para proteger contra ataques MitM (man-in-the-middle) nos quais as comunicações entre duas partes são interceptadas. Definir esta propriedade substitui a propriedade *com.glide.communications.trustmanager_trust_all*.

Mais informações

Atributo	Descrição
Nome da propriedade	*com.glide.communications.httpclient.verify_hostname*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Configurar na Central de segurança da instância	Sim
Finalidade	Desabilitar o processo de verificação de certificação, que avalia todas as certificações na cadeia de certificação ao verificar o status de revogação.
Tipo	verdadeiro | falso
Valor recomendado	verdadeiro
Impacto funcional	(Médio) Permite que um certificado não validado se conecte como um host inseguro.
Risco à segurança	(Médio) Permite ou impede que o cliente http se conecte a um nome de host potencialmente perigoso, sem exceção.
Referências	Certificados Confiança de certificado

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Verificação de certificado revogada

Use esta propriedade para desativar o processo de verificação de certificação que avalia todas as certificações na cadeia de certificação verificando o status de revogação.

As chamadas de API que usam o plug-in High Security podem configurar esta propriedade. Se a cadeia de certificação completa não estiver definida no repositório confiável da instância ou os certificados usados talvez não sejam compatíveis com uma verificação de revogação OCSP (Online Certificate Status Protocol, Protocolo de status de certificado on-line), erros podem ser retornados para as chamadas de API.

A verificação de revogação do certificado pode ser desativada definindo a propriedade *com.glide.communications.httpclient.verify_revoked_certificate* como **falsa**.

Os erros associados a uma incapacidade de fazer a verificação são NPE, SSLPeerUnverifiedException, CertPathValidatorException. Esses erros podem ser encapsulados em um HttpException. Vários fatores podem afetar a capacidade de fazer uma verificação bem-sucedida:

- O URI deve estar acessível para a instância. Observe que a implementação do OCSP original pode não ter acesso a uma conexão por proxy.
- O serviço OCSP referenciador deve estar on-line quando a verificação é feita.

Nota: Os valores dessas propriedades são e não podem ser alterados depois de mudados (eles não são reversíveis) Se tiver alguma dúvida, entre em contato com Suporte e atendimento ao cliente.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mais informações

Atributo	Descrição
Nome da propriedade	*com.glide.communications.httpclient.verify_revoked_certi*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Configurar na Central de segurança da instância	Sim
Finalidade	Desabilitar o processo de verificação de certificado que avalia todos os certificados na cadeia de certificados verificando o status de revogação. Somente um certificado de servidor autoassinado precisaria ser carregado no repositório confiável da instância.
Tipo	verdadeiro | falso
Valor padrão	verdadeiro
Valor recomendado	verdadeiro
Impacto funcional	(Médio)
Risco à segurança	(Médio) Chamadas de API usando o plug-in High Security não serão verificadas usando uma verificação de revogação OCSP no repositório confiável da instância.
Referências	Certificados

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Práticas recomendadas de segurança (proteção de segurança da instância)

Além das configurações de segurança, algum esforço manual extra é necessário para proteger ainda mais as aplicações da Now Platform no dia a dia. Esta seção contém tarefas de segurança que um administrador deve executar periodicamente dentro de um determinado intervalo de tempo.

Definição automática de opções de tipo de conteúdo [Removido na Central de segurança 1.3.3]

O cabeçalho HTTP de resposta X-Content-Type-Options é usado pelo servidor para indicar que os tipos MIME (Multipurpose Internet Mail Extensions) anunciados nos cabeçalhos de tipo de conteúdo devem ser seguidos.

Definir este cabeçalho impedirá que o navegador interprete arquivos como algo diferente do declarado pelo tipo de conteúdo nos cabeçalhos HTTP. Este cabeçalho pode ajudar a mitigar ataques de confusão MIME.

As opções de tipo de conteúdo definidas automaticamente serão compatíveis se *glide.security.header.auto_set_x_content_type_options* estiver definido como **verdadeiro**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mais informações

Atributo	Descrição
Nome da propriedade	*glide.security.header.auto_set_x_content_type_options*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Configurar na Central de segurança da instância	Sim
Finalidade	Evitar que o navegador interprete os arquivos como algo diferente do declarado pelo tipo de conteúdo nos cabeçalhos HTTP.
Tipo	booliano
Valor recomendado	verdadeiro
Impacto funcional	(Alto) Este cabeçalho pode ajudar a mitigar ataques de confusão MIME.
Risco à segurança	(Alto) Se esta propriedade não estiver habilitada, o navegador poderá interpretar incorretamente o tipo de conteúdo nos cabeçalhos HTTP.
Referências	Tipos MIME para download

Valor do cabeçalho HTTP Cache-Control (proteção de segurança da instância)

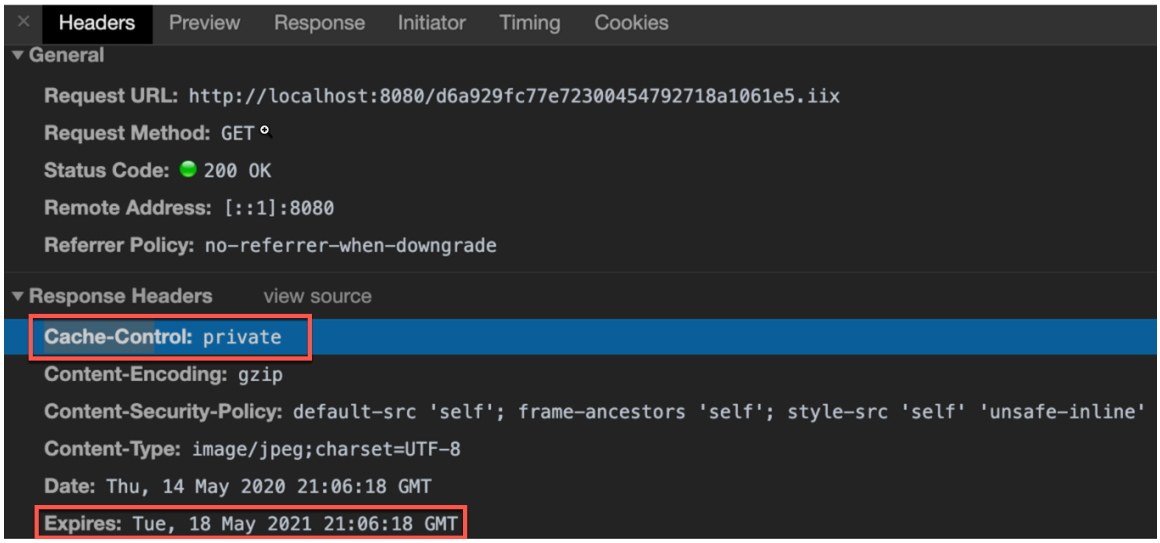
Use a propriedade *glide.http.cache_control* para definir o valor padrão de cache-control nos cabeçalhos de resposta HTTP que Now Platform envia ao solicitar dados de conteúdo estático para uma página. Exemplos de conteúdo estático incluem imagens, CSS e JavaScript renderizados de dentro para uma página.

A propriedade *glide.http.cache_control* define o valor de controle de cache padrão nos cabeçalhos de resposta HTTP como **privado** ou **público**. O padrão é **público**.

Valor	Descrição
privado	O conteúdo estático pode ser armazenado em cache no nível do navegador (cliente), mas não no nível do servidor proxy.
público	O conteúdo estático pode ser armazenado em cache no nível do navegador (cliente) e também no nível do servidor proxy.

O valor de Expires nos cabeçalhos de resposta HTTP controla quando o conteúdo estático expira e tem um valor padrão de 369 dias. Para substituir manualmente o valor padrão, use a propriedade *glide.http.expire.days*.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Nota: Você pode usar a propriedade *glide.http.cache* para habilitar ou desabilitar a configuração dos valores Cache-Control e Expires nos cabeçalhos de resposta HTTP. O padrão é **verdadeiro**, o que permite que você defina:

- Valor padrão de Cache-Control usando a propriedade *glide.http.cache_control*.
- Valor padrão de Expires usando a propriedade *glide.http.expire.days*.

Mais informações

Atributo	Descrição
Nome da propriedade	glide.http.cache_control
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Configurar na Central de segurança da instância	Sim
Finalidade	Configurar o valor do cabeçalho de resposta HTTP do Cache-Control para conteúdo estático.
Valor padrão	público
Valor recomendado	privado
Impacto funcional	(Médio) Define o valor de Cache-Control padrão em um cabeçalho de resposta HTTP.
Risco à segurança	(Alto) Se você definir esta propriedade como **pública**, as instâncias com CDN/proxies poderão armazenar em cache o conteúdo estático e renderizar sem autenticação. • **privado** é uma configuração mais apropriada para instâncias com configuração de CDN/proxy. • Se uma instância não tiver uma configuração de CDN/proxy, qualquer um dos valores deve servir.

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Impor segurança em relatórios

Desative esta propriedade para impedir que o usuário publique ou acesse relatórios. Esta propriedade desabilita o recurso de emissão de relatórios publicados em relatórios.

Habilite a publicação de relatórios definindo *glide.report.published_reports.enabled* como **verdadeiro**.

Impor segurança em relatórios é compatível se *glide.report.published_reports.enabled* estiver definido como **falso**.

Mais informações

Atributo	Descrição
Nome da propriedade	*glide.report.published_reports.enabled*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Configurar na Central de segurança da instância	Sim
Finalidade	Desabilitar o recurso de emissão de relatórios publicados em relatórios.
Tipo	verdadeiro | falso
Valor recomendado	**falso**
Impacto funcional	(Médio) O usuário não pode publicar relatórios.
Risco à segurança	(Médio) Se esta propriedade não estiver habilitada, os usuários poderão acessar ou publicar relatórios expondo dados confidenciais. Publicar um relatório cria um URL que qualquer pessoa pode usar para acessar o relatório, incluindo pessoas que não são usuários. Quando alguém navega até o URL, o relatório é gerado com os dados atuais da instância.
Referências	Publicar um relatório

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Plug-in High Security (proteção de segurança da instância)

Quando você ativa o plug-in High security, ele cria ou atualiza centenas de configurações diferentes para controlar o nível de segurança em sua instância. Essas configurações atenuam muitos dos principais ataques OWASP, permitindo controle de acesso estrito, validação de entrada e codificação de saída.

Essas configurações incluem:

- Controle de Acesso
- Regras de negócios
- Propriedades do sistema
- Ação de Política de IU
- ações de script
- Inclusões de script

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exemplo

Consulte os exemplos para as seguintes propriedades:

Propriedade	Tópico
glide.ui.escape_all_script	Escapar do Jelly
glide.security.strict.actions	Verifique a ação de IU antes da execução
glide.security.csrf_previous.allow	Token anti-CSRF
glide.security.csrf.strict.validation.mode	Validação estrita de CSRF

Mais informações

Atributo	Descrição
Nome do Plug-in	com.glide.high_security
Tipo de configuração	Definição do sistema > Plug-ins - Desenvolvimento
Finalidade	É obrigatório ativar este plug-in. Ele aumenta o nível de segurança de uma instância, o que reduz a superfície de ataque ao atenuar os 10 principais ataques do owasp, incluindo CSRF, XSS, protegendo cookies de sessão e uploads de arquivo.
Valor recomendado	Ativo
Impacto funcional	(Alto) Este plug-in permite várias configurações de segurança do sistema, o que pode afetar a IU e a funcionalidade.
Risco à segurança	(Alto) Muitas configurações de segurança são acidentalmente deixadas em aberto, o que pode abrir a porta para algumas das vulnerabilidades críticas.
Referências	Ativar configurações de alta segurança Configurações de Alta Segurança

Para saber mais sobre como ativar um plug-in, consulte Ativar um plug-in.

IDs de login individuais (proteção de segurança da instância)

Certifique-se de que todos os usuários tenham IDs de usuário individuais, o que permite a auditoria de todas as atividades do usuário.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: As contas de usuário local que não estão sendo usadas devem ter o sinalizador **Ativo** definido como falso.

- Definir o sinalizador **Ativo** como **falso** define automaticamente o sinalizador **Bloqueado** como **verdadeiro**. Se o sinalizador **Bloqueado** estiver definido como **verdadeiro**, ele não permitirá que a conta do usuário seja autenticada na instância.
- Definir o sinalizador **Ativo** como **falso** não remove um usuário da Now Platform, mas remove a visibilidade de contas que não são de administrador.
- Se o sinalizador **Ativo** estiver definido como **falso**e o sinalizador **Bloqueado** também estiver definido como **falso**, um usuário ainda poderá fazer login nesta conta.

Para saber mais sobre contas de usuário, consulte Administração de usuário.

Ofuscação da IU para celular (proteção de segurança da instância)

Use a propriedade *glide.ui.m.blur_ui_when_backgrounded*para ofuscar todos os campos do snapshot enquanto a imagem é salva durante o processo em segundo plano para ofuscar.

Em dispositivos Android, o sistema operacional Android faz uma captura de tela para uso no menu de tarefas recentes quando a aplicação é enviada para segundo plano. Os usuários também podem fazer capturas de tela manuais da aplicação, que são armazenadas publicamente no dispositivo.

Em dispositivos iOS, o sistema operacional iOS também permite que as aplicações salvem um arquivo de imagem. Este arquivo representa a última tela vista pelo usuário quando a aplicação é enviada para segundo plano. Embora a intenção seja fornecer uma melhor experiência do usuário, isso também cria um risco à segurança porque as imagens são salvas como arquivos de imagem PNG.

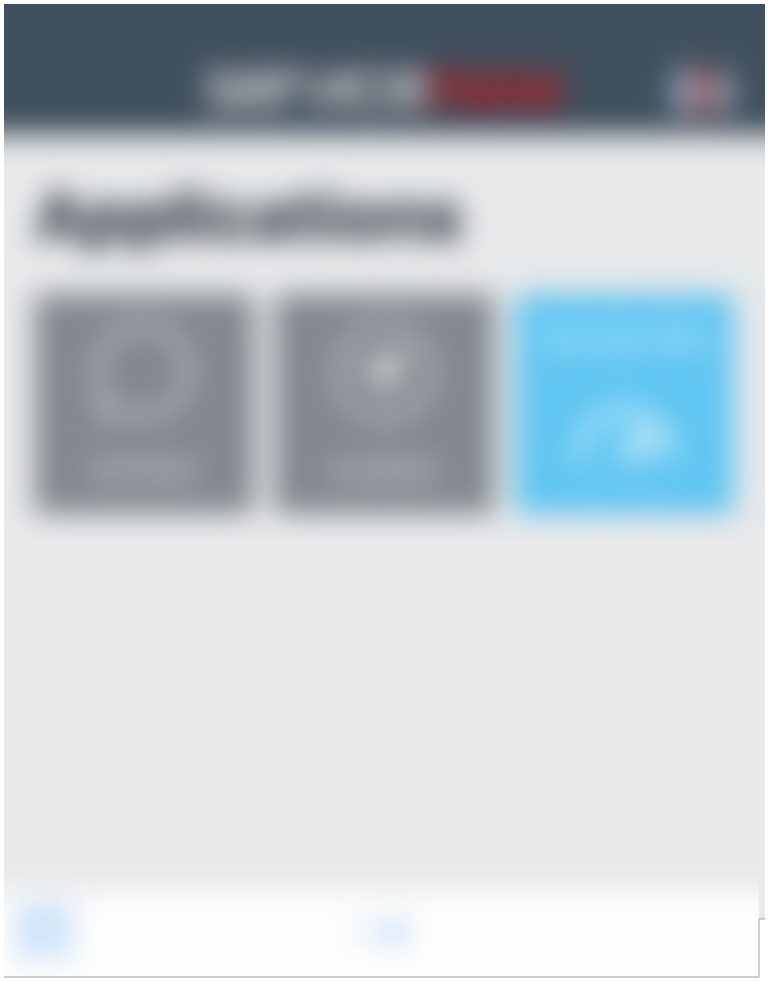
Nota: Esta definição ou configuração é por instância, portanto, o usuário deve se conectar à instância com a propriedade configurada.

Para ofuscar todos os campos do snapshot no app ServiceNow Classic, consulte Configurar a opção do app de desfoque para melhorar a segurança.

Exemplo

Quando você define esta propriedade como **verdadeira**. A aplicação em segundo plano é ofuscada para dispositivos iOS e finalizada para dispositivos Android iOS.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Mais informações

Atributo	Descrição
Nome da propriedade/plug-in	glide.ui.m.blur_ui_when_backgrounded
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Configurável na Central de segurança da instância	Não
Finalidade	Ofuscar todos os campos do snapshot enquanto a imagem é salva durante o processo em segundo plano.
Valor recomendado	verdadeiro
Impacto funcional	(Baixo) Se a propriedade *glide.ui.m.blur_ui_when_backgrounded* estiver definida como **verdadeira**, os aplicativos nativos usarão o parâmetro definido no servidor para desfocar a tela quando o aplicativo entrar em segundo plano.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
	• As capturas de tela tiradas pelo iOS e pelo Android são desfocadas quando o aplicativo entra em segundo plano. • A experiência do usuário pode ser afetada negativamente porque ele não poderá ver o conteúdo quando o app for enviado para segundo plano.
Risco à segurança	(Médio) Um dispositivo comprometido (desbloqueado) permite que um invasor tenha acesso total ao sistema de arquivos, com acesso a esses arquivos/snapshots com informações confidenciais incorporadas a eles.

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Patches e atualizações (proteção de segurança da instância)

Certifique-se de que a instância esteja executando o nível de patch mais atual. As correções de segurança são lançadas rotineiramente para a Now Platform em muitos dos patches e hotfixes que acompanham as atualizações de recursos do produto. Atualizar quando novos patches e correções estão disponíveis reduz o risco de vulnerabilidades potenciais.

A Now Platform passa por dois testes de invasão por semana, em média.

- Embora a maioria desses testes não resulte em vulnerabilidades significativas, há vulnerabilidades encontradas e corrigidas regularmente.
- Informações sobre versões, patches e correções da Now Platform podem ser encontradas na seção Notas de versão da documentação do produto. Consulte Notas de versão para upgrades para obter mais informações.

Remover dados de demonstração (proteção de segurança da instância)

Dados de demonstração, especialmente contas de demonstração, são normalmente incluídos quando uma instância é criada. Quando isso acontece, todos os dados de demonstração devem ser removidos antes de usar a instância em não produção ou em produção.

Abra uma solicitação no HI. Certifique-se de criar uma conta administrativa antes de enviar a solicitação.

É altamente recomendável que a remoção de dados de demonstração na produção seja verificada com sucesso em uma instância de produto em fase de desenvolvimento que seja um clone recente da instância de produção.

Recursos internos

https://support.servicenow.com/kb_view.do?sysparm_article=KB0550107

https://community.servicenow.com/community?id=community_blog&sys_id=786eaeaddbd0dbc01dcaf3231f961959

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Remover dados de demonstração usando o Catálogo de serviços

Em vez de enviar a solicitação como um incidente, determinados usuários podem solicitar a remoção de dados de demonstração em uma instância usando o Catálogo de serviços. Esses usuários incluem usuários internos e os usuários que tenham as funções customer_admin ou partner_admin.

1. Navegue até https://support.servicenow.com/now .
2. Especifique a instância da qual os dados de demonstração serão removidos.

   Se você estiver tendo problemas para encontrar sua instância, inicie o nome da instância com * para executar uma consulta de conteúdo.

3. Clique em **Autoatendimento** > **Remover dados de demonstração** > **.**
4. Especifique a data e a hora para remover os dados de demonstração da instância selecionada.

   A data e a hora devem ser pelo menos quatro horas posteriores à hora atual.

5. Clique em **Enviar**.

Uma nova solicitação de mudança é criada e aparece automaticamente. A **Data de término planejada** é calculada automaticamente com base na **Data de início planejada** mais cinco horas, que é o tempo que o processo leva. Na solicitação de mudança. Use a Lista de observação para adicionar outros membros da sua equipe que devem estar cientes do status da solicitação de mudança.

Lista de inclusões de segurança (proteção da segurança da instância)

Um modelo de segurança "positivo" (também conhecido como "lista de inclusões") é aquele que define o que é permitido e rejeita todo o resto. Esta seção contém controles de segurança que um administrador pode configurar para restringir o comportamento a listas de inclusões conhecidas.

Nota: As propriedades da lista de inclusões de segurança devem ser configuradas manualmente em cada instância, pois os Conjuntos de atualizações não promoverão a configuração e retornarão um erro.

Verificar as chamadas de membros da lista de permissões (proteção de segurança da instância)

Revise e remova entradas de chamada de membro da lista de inclusões conforme necessário da tabela sys_whitelist_member.

As entradas de chamada de membro podem acessar os recursos Java no lado do servidor para executar operações baseadas em aplicações sem validação apropriada. Como isso pode causar divulgações não autorizadas ou alteração de dados do cliente, é uma grave preocupação de segurança.

Mais informações

Atributo	Descrição
Nome da tabela	sys_whitelist_member

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
	Nota: Em versões recentes, somente funcionários da ServiceNow podem acessar esta tabela; nem mesmo os administradores podem fazer isso.
Tipo de configuração	Tabela
Configurar na Central de segurança da instância	Sim
Finalidade	Revisar e remover entradas desta tabela.
Valor recomendado	Nenhum registro deve existir na tabela (a lista deve estar vazia).
Impacto funcional	(Baixo) Não deve haver nenhum impacto, desde que você revise e aprove os resultados gerados ao executar o Packages call removal tool. Para garantir o funcionamento adequado da instância, teste as mudanças em um ambiente de não produção antes de implantar no ambiente de produção. Para saber mais, consulte Packages call removal tool.
Risco à segurança	(Alto) As chamadas de API do lado do cliente que resultam na recuperação de dados ou no acesso a objetos no servidor são consideradas perigosas do ponto de vista da segurança. Valide esses itens para autorização e restrição de acesso a objetos confidenciais.

Etapas para configurar

Nota: As etapas a seguir são semelhantes às etapas descritas nas seções Etapas para configurar em:

- Packages call removal tool
- Verificar chamadas de pacotes da lista de permissões

Se você já as concluiu, pode ignorar essas etapas.

1. Habilite o plug-in Packages call removal tool. Para saber mais, consulte Packages call removal tool.
2. Usando o navegador de filtros, navegue até o **Utilitário de remoção de chamada de pacotes**.
3. Clique em cada script começando de (1) a (4). Aguarde a saída e prossiga para a próxima.
4. Depois de executar o script (4), uma lista de campos afetados aparece na página de Itens de chamada de pacotes.
5. Resolva todos os itens nas seções Proposto e Erro.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Esta ferramenta pode relatar algumas chamadas de pacote usadas em `sa_mapping_ext_commands` e `sa_custom_operation`. Essas chamadas de pacote pertencem ao MID Server. Como não há classes, o código é executado no MID Server. Se você encontrar as seguintes chamadas de membros na seção Erros, marque-as como **Rejeitadas** (Ignoradas). A ferramenta não relata essa chamada de membro novamente.

- `Packages.com.snc.sw.util.JSONUtil.toJSONPlain(file_content);`
- `Packages.com.snc.sw.util.JSONUtil.toJSONPlain(file_name);`
- `Packages.com.snc.sw.commands.HttpCallHandler;`
- `Packages.com.snc.sw.dto.ProviderType.SSH`

6. Entre em contato com o suporte ServiceNow para obter mais correções.

Verificar as chamadas de pacotes da lista de permissões (proteção de segurança da instância)

Revise e remova entradas de chamada de pacote de lista de inclusões conforme necessário da tabela sys_whitelist_package.

As entradas de chamada de pacote podem acessar recursos Java no lado do servidor para executar operações baseadas em aplicações sem validação apropriada. Como isso pode causar divulgações não autorizadas ou alteração de dados do cliente, é uma grave preocupação de segurança.

Mais informações

Atributo	Descrição
Nome da tabela	sys_whitelist_package **Nota:** Em versões recentes, somente Suporte e atendimento ao cliente podem acessar esta tabela; nem mesmo os administradores podem fazer isso.
Tipo de configuração	Tabela
Configurar na Central de segurança da instância	Sim
Finalidade	Revisar e remover entradas desta tabela.
Valor recomendado	Nenhum registro deve existir na tabela (a lista deve estar vazia).
Impacto funcional	(Baixo) Não deve haver impacto, desde que os resultados da execução do Packages call removal tool sejam revisados e aprovados. Para garantir o funcionamento adequado da instância, teste as mudanças em um ambiente de não produção antes de implantar no ambiente de produção. Para saber mais, consulte Packages call removal tool.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Risco à segurança	(Alto) As chamadas de API do lado do cliente que resultam na recuperação de dados ou no acesso a objetos no servidor são consideradas perigosas do ponto de vista da segurança. Valide esses itens para autorização e restrição de acesso a objetos confidenciais.
Solução alternativa	Entre em contato com o suporte da ServiceNow para obter assistência.

Etapas para configurar

1. Habilite o plug-in Packages Call Removal Tool. Para saber mais, consulte Packages call removal tool.
2. Usando o navegador de filtros, navegue até o **Utilitário de remoção de chamada de pacotes**.
3. Clique em cada script começando de (1) a (4). Aguarde a saída e prossiga para a próxima.
4. Depois de executar o script (4), uma lista de campos afetados aparece na página de Itens de chamada de pacotes.
5. Resolva todos os itens nas seções Proposto e Erro.

   Nota: Esta ferramenta pode relatar algumas chamadas de pacote usadas em `sa_mapping_ext_commands` e `sa_custom_operation`. Essas chamadas de pacote pertencem ao MID Server. Como não há classes, o código é executado no MID Server. Se você encontrar as seguintes chamadas de pacotes na seção Erros, marque-as como **Rejeitadas** (Ignoradas). A ferramenta não relata essa chamada de pacote novamente.

   - `Packages.com.snc.sw.util.JSONUtil.toJSONPlain(file_content);`
   - `Packages.com.snc.sw.util.JSONUtil.toJSONPlain(file_name);`
   - `Packages.com.snc.sw.commands.HttpCallHandler;`
   - `Packages.com.snc.sw.dto.ProviderType.SSH`

6. Entre em contato com o suporte ServiceNow para obter mais correções.

Habilitar lista de permissões de URL para comunicação de iframe de origem cruzada (proteção de segurança da instância)

Use a propriedade *`glide.ui.concourse.onmessage_enforce_same_origin`* para habilitar a comunicação de origem cruzada entre `iframes`.

O `OpenFrame` só pode processar mensagens de domínios confiáveis especificados na propriedade *`glide.ui.concourse.onmessage_enforce_same_origin_whitelist`*. Para obter mais informações, consulte Especificar a lista de permissões de UTL para comunicação de iframe de origem cruzada.

Mais informações

Atributo	Descrição
Nome da propriedade	glide.ui.concourse.onmessage_enforce_same_origin

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Configurar na Central de segurança da instância	Sim
Finalidade	Habilitar a lista de inclusão de domínios confiáveis para que eles possam se comunicar entre iframes para openframe.
Valor recomendado	verdadeiro
Impacto funcional	(Médio) Se você não colocar os domínios pretendidos na lista de inclusões, a capacidade de incorporar outras páginas em instâncias da Now Platform poderá ser limitada.
Risco à segurança	(Alto) Se uma página da Web contiver manipuladores de eventos que não executam a validação de origem apropriada, uma página da Web ou script de qualquer origem poderá se comunicar com ela. Ela também pode iniciar qualquer funcionalidade executada pelo manipulador de eventos.
Referências	Visão geral do OpenFrame

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Impor links relativos (proteção de segurança da instância)

Use a propriedade *glide.cms.catalog_uri_relative* para impor links relativos do parâmetro URI em `em/ess/catalog.do`.

- Quando definida como **verdadeira**, somente URLs relativas são permitidas por meio da página `/ess/catalog.do` usando o parâmetro *uri*.
- Quando definida como **falsa**, todas as URLs são permitidas, o que pode permitir vinculação a conteúdo externo não autorizado.

Mais informações

Atributo	Descrição
Nome da propriedade	glide.cms.catalog_uri_relative
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Configurar na Central de segurança da instância	Sim
Finalidade	Restringir as tentativas de vincular conteúdo externo não autorizado.
Valor recomendado	verdadeiro
Impacto funcional	(Baixo) Esta correção impõe a validação na página do Catálogo de forma que somente URLs relativas sejam permitidas. Links existentes para aplicações da Web externos são quebrados.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Risco à segurança	(Alto) URLs absolutos podem representar um risco à segurança quando usados como parte de um parâmetro ou um valor de campo, redirecionando a página de origem para um site controlado por um adversário.

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Packages Call Removal Tool (proteção de segurança da instância)

Habilite e execute o plug-in Packages Call Removal Tool (*com.glide.script.packages_call_removal*) e analise se cada uma das mudanças propostas deve ser concluída ou rejeitada.

O Packages Call Removal Tool é um plug-in que:

- Verifica scripts em busca de chamadas de pacote para classes Java da Now Platform.
- Propõe mudanças para substituí-las por nomes GlideScript preferenciais.
- Facilita as mudanças de script.

Nota: Se este registro for um registro do sistema de base, o uso da recomendação da ferramenta fará com que o item seja marcado como customer_update. Esse script pode não aceitar mais atualizações no futuro. Em versões posteriores, as tabelas sys_whtelist_xxx devem estar vazias. No entanto, ainda pode ser útil usar essa ferramenta porque ela sinaliza Pacotes, chamadas xxx.

O Packages Call Removal Tool pode relatar algumas chamadas de pacote usadas em `sa_mapping_ext_commands` e `sa_custom_operation`. Essas chamadas de pacote pertencem ao MID Server. Como não há classes, o código é executado no MID Server. Se você encontrar qualquer uma das chamadas de pacote listadas a seguir na seção Erros, marque-as como Rejeitadas (Ignoradas). A ferramenta não relata essa chamada de pacote novamente.

- `Packages.com.snc.sw.util.JSONUtil.toJSONPlain(file_content);`
- `Packages.com.snc.sw.util.JSONUtil.toJSONPlain(file_name);`
- `Packages.com.snc.sw.commands.HttpCallHandler;`
- `Packages.com.snc.sw.dto.ProviderType.SSH`

Mais informações

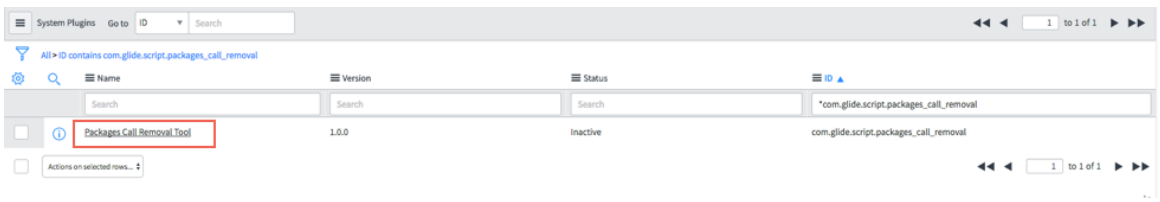
Atributo	Descrição
Nome do Plug-in	com.glide.script.packages_call_removal
Tipo de configuração	Definição do sistema > Plug-ins
Configurar na Central de segurança da instância	Sim
Finalidade	Remover/substituir chamadas de pacote/membro não autorizadas por nomes Glide aceitáveis (GlideScriptable) que só permitem o acesso autorizado aos dados.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

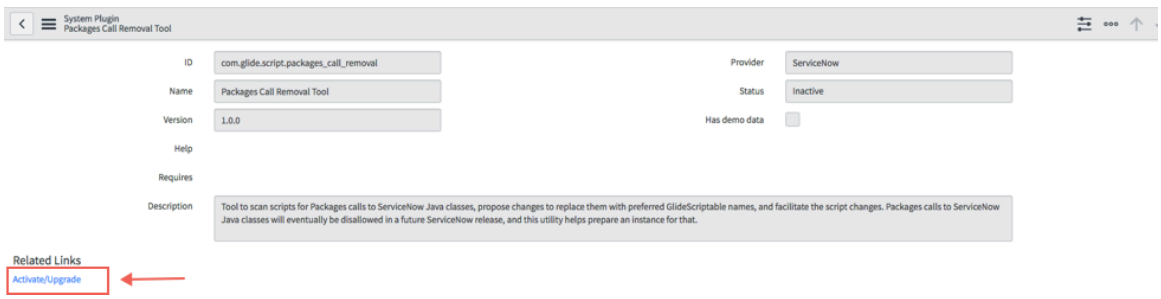
Atributo	Descrição
Valor recomendado	Ativo
Impacto funcional	(Baixo) Esta correção substitui as chamadas de pacote por APIs *GlideScriptable* e pode afetar as personalizações que incluem chamadas de pacote. A ferramenta não substitui as chamadas de pacote automaticamente. Em vez disso, ela fornece sugestões que são armazenadas na tabela packages_call_item. Seu administrador pode decidir se aceita ou rejeita a mudança proposta.
Risco à segurança	(Médio) As chamadas de API do lado do cliente que resultam na recuperação de dados ou no acesso a objetos no servidor são consideradas perigosas do ponto de vista da segurança. Elas devem ser validadas para autorização e restrição de acesso a objetos confidenciais.

Etapas para configurar

1. Navegue até **Definição do sistema** > **Plug-ins**.

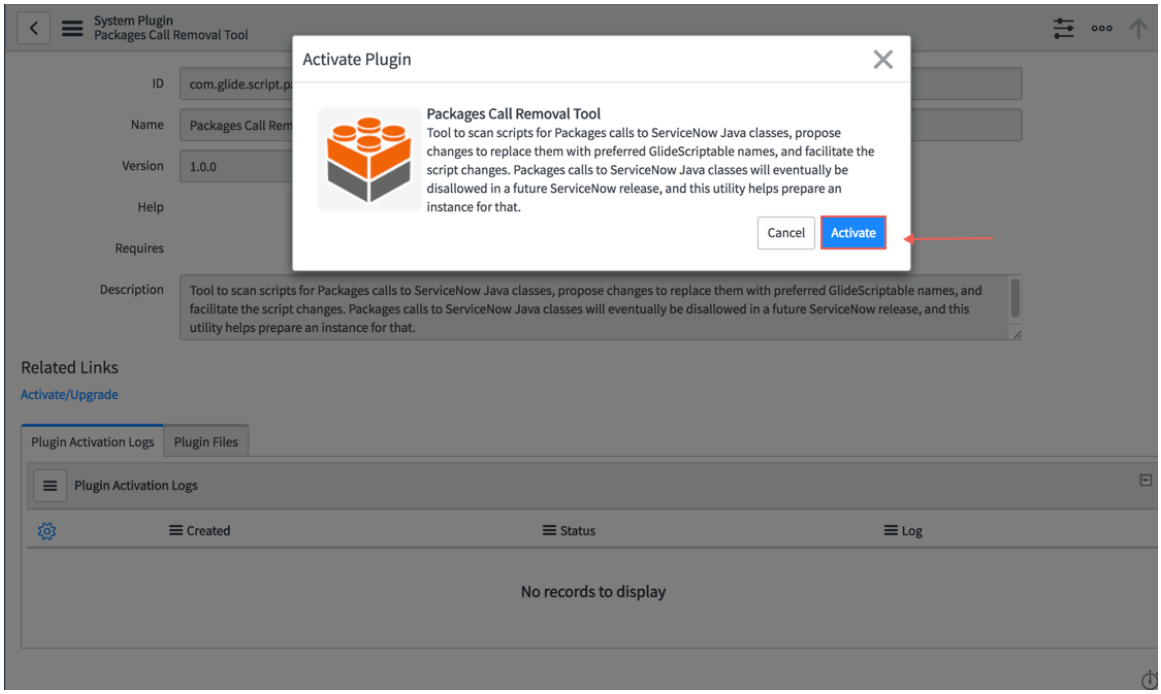


2. Pesquise o plug-in ID = *com.glide.script.packages_call_removal*.



3. Clique em **Ativar/Fazer upgrade** para ativar o plug-in.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Para verificar chamadas de pacote de lista de inclusões e chamadas de membro da lista de inclusões, conclua as ações descritas nas seções Etapas para configurar nos seguintes tópicos:
   - Verificar chamadas de membros da lista de permissões
   - Verificar chamadas de pacotes da lista de permissões

Especificar lista de permissões de URL para comunicação de iframe de origem cruzada (proteção de segurança da instância)

Use a propriedade *glide.ui.concourse.onmessage_enforce_same_origin_whitelist* para ativar a comunicação de origens cruzadas entre `iframes` de domínios confiáveis especificados em uma lista de inclusão.

Mais informações

Atributo	Descrição
Nome da propriedade	glide.ui.concourse.onmessage_enforce_same_origin_whitelist
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Configurar em Central de segurança da instância	Não
Finalidade	Habilitar a lista de inclusões de domínios confiáveis para que eles possam se comunicar entre iframes para openframe.
Requisito	Obrigatório
Impacto funcional	(Médio) Se você não incluir os domínios pretendidos, a capacidade de incorporar outras páginas nas instâncias da Now Platform poderá ser limitada.
Risco à segurança	(Alto) Se uma página da Web contiver manipuladores de eventos que não executam a validação de

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
	origem apropriada, uma página da Web ou script de qualquer origem poderá se comunicar com ela. Ela também pode iniciar qualquer funcionalidade executada pelo manipulador de eventos. A comunicação com iframes de outros domínios é um risco à segurança.

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Lista de permissões de URL para redirecionamentos de logout (proteção de segurança da instância)

Use a propriedade *glide.security.url.whitelist* para adicionar uma camada extra de validação para garantir que qualquer URL externo introduzido faça parte dos URLs da lista de inclusões.

O redirecionamento aberto ocorre quando uma página da Web vulnerável é redirecionada para uma página não confiável e mal-intencionada que pode comprometer o usuário. Os ataques de redirecionamento aberto vêm com um ataque de phishing porque o link vulnerável modificado é idêntico ao site original, aumentando a probabilidade de sucesso do ataque de phishing.

Esta propriedade é aplicável nos seguintes casos:

- `/logout.do?sysparm_goto_url={External URL}`
- `/cms_login_redirect.do?sysparm_goto_url={External URL}`

Os usuários são direcionados para um site externo confiável após fazerem logout da instância:

- `/logout_redirect.do?sysparm_url={External URL}`
- `/saml_redirector.do?sysparm_uri={External URL}`

Quando o SAML está habilitado, ele invoca um URL de logout do IDP (identity provider, provedor de identidade).

Mais informações

Atributo	Descrição
Nome da propriedade	glide.security.url.whitelist
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Configurar na Central de segurança da instância	Sim
Finalidade	Implementar o redirecionamento de URL seguro durante o login, logout ou outros redirecionamentos. Esta propriedade atenua um dos 10 principais ataques da OWASP, chamados de redirecionamentos e encaminhamentos inválidos.
Tipo	Cadeia de caracteres separada por vírgula e espaço. Exemplo: `https://exemplo.com, https://wiki.exemplo.com`.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Valor	Os URLs aprovados da sua organização [Alguns FQDN (Fully Qualified Domain Name, Nome de domínio completo) definidos, por exemplo, http://www.servicenow.com.br]
Impacto funcional	(Médio) Esta correção impõe validação na página de logout. Isso pode ter um impacto funcional em um usuário de uma instância com uma configuração SSO/SAML.
Risco à segurança	(Alto) O redirecionamento aberto do lado do cliente pode permitir que o invasor redirecione as vítimas/usuários para o site controlado pelo invasor e é visto como um risco à segurança.
Referências	Correções e erros de Multi-SSO (SAML 2.0)

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Política de segurança de conteúdo do cliente incorporado do Virtual Agent (proteção de segurança da instância)

Use a propriedade *com.glide.cs.embed.csp_frame_ancestors* para habilitar a configuração da política frame-ancestors somente para a página `https://<your-instance>.service-now.com/sn_va_web_client_app_embed.do`.

O plug-in do Virtual Agent permite a incorporação de um cliente em uma página da Web externa. Para habilitar a página do cliente a ser incorporada na página da Web, a Política de segurança de conteúdo deve permitir a página externa como um quadro primário.

Nota: Evite usar somente `'*'` como Política de segurança de conteúdo, pois isso habilitaria todos os domínios e deixaria a aplicação potencialmente vulnerável a clickjacking.

Mais informações

Atributo	Descrição
Nome da propriedade	com.glide.cs.embed.csp_frame_ancestors
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Configurar em Central de segurança da instância	Não
Finalidade	Habilitar a criação de Política de segurança de conteúdo personalizada para a página do Virtual Agent incorporável.
Valor recomendado	Definir como domínios confiáveis
Impacto funcional	(Alto) O cliente incorporável do Virtual Agent não permite a incorporação em sites externos, a menos que a Política de segurança de conteúdo esteja configurada corretamente.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Risco à segurança	(Médio) Se configurada incorretamente (permitindo todos os quadros primários), pode deixar a página do cliente incorporável vulnerável a clickjacking.
Referências	Incorporar o cliente web do Virtual Agent em uma página web externa Para saber mais sobre como criar uma Política de segurança de conteúdo de ancestrais de quadros, consulte aqui.

Etapas para configurar

1. Navegue até **/sys_properties_list.do** .
2. Pesquise pela propriedade *com.glide.cs.embed.csp_frame_ancestors*.
3. Atribua uma política de segurança de conteúdo aceitável (permitir somente a empresa ou outros domínios aceitos) e clique em **Atualizar**.

X-Frame-Options do cliente incorporado do Virtual Agent (proteção de segurança da instância)

Use a propriedade *com.glide.cs.embed.xframe_options* para habilitar a configuração do cabeçalho X-Frame apenas para a página `https://<your-instance>.service-now.com/sn_va_web_client_app_embed.do`.

O plug-in do Virtual Agent permite a incorporação de um cliente em uma página da Web externa. Para habilitar a página do cliente a ser incorporada na página da Web, o cabeçalho X-Frame-Options deve habilitar o `iframe` a ser incluído no quadro primário.

Nota: Evite usar `allow-from *` como o valor do cabeçalho X-Frame-Options porque isso habilitaria todos os domínios e deixaria a aplicação potencialmente vulnerável a clickjacking.

Mais informações

Atributo	Descrição
Nome da propriedade	com.glide.cs.embed.xframe_options
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Configurar em Central de segurança da instância	Não
Finalidade	Habilitar a especificação da diretiva para o cabeçalho X-Frame-Options para a página incorporável do Virtual Agent.
Valor recomendado	sameorigin
Impacto funcional	(Alto) O cliente incorporável do Virtual Agent não se habilita a ser incorporado em sites externos, a menos que o cabeçalho X-Frame-Options esteja configurado corretamente.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Risco à segurança	(Médio) Se configurada incorretamente (permitindo todos os quadros primários), pode deixar a página do cliente incorporável vulnerável a clickjacking.
Referências	Incorporar o cliente web do Virtual Agent em uma página web externa

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

X-Frame-Options: SAMEORIGIN (proteção de segurança da instância)

Use a propriedade *glide.set_x_frame_options* para definir o cabeçalho de resposta X-Frame-Options como SAMEORIGIN para todas as páginas de IU.

Use o cabeçalho de resposta HTTP X-Frame-Options para indicar se o navegador deve ter permissão para renderizar uma página em um `<frame>` ou `<iframe>`. Os sites podem usar esta função para evitar ataques de clickjacking, garantindo que seu conteúdo não seja incorporado a outros sites. Um invasor poderia incorporar sua página na página dele e tornar os elementos da sua página maliciosos. O usuário final pode achar que a página é real já que se parece com a sua página. O usuário final pode clicar nos elementos normalmente e acabar executando o scripts ou elementos maliciosos.

Mais informações

Atributo	Descrição
Nome da propriedade	glide.set_x_frame_options
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Configurar na Central de segurança da instância	Sim
Finalidade	Atenuar os ataques de ClickJacking.
Valor recomendado	verdadeiro
Impacto funcional	(Baixo) Esta correção impõe a restrição para renderizar uma aplicação da Now Platform em um aplicativo de terceiros na forma de um iFrame. Se você tiver essa integração, o aplicativo não será renderizado no aplicativo personalizado de terceiros.
Risco à segurança	(Médio) A política Same Origin permite que você restrinja um domínio de recuperar um script ou um recurso de outros domínios. Todos os navegadores modernos oferecem suporte a esta funcionalidade. A política valida a conexão com base no protocolo, na porta e no host. CORS (Cross Origin Request, Solicitação de origem cruzada) é uma modificação da política Same Origin que permite o acesso a recursos/scripts de outro domínio quando declarado explicitamente como uma parte do valor do cabeçalho.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
	• Nesse caso, o cabeçalho **X-Frame-Options** controla se a aplicação da Now Platform pode ser renderizada no site de terceiros. • Ele reduz a exposição confidencial, pois o valor da propriedade, quando definido como **SAMEORIGIN**, não permite que a renderização aconteça.
Referências	Propriedades do sistema disponíveis Configurar iFrames

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Validação de processamento de entidade externa de XML

Essas propriedades permitem a expansão da entidade e restringem qualquer entidade externa (por exemplo, URL) quando incluídas como parte da referência XML DOCTYPE. O DTD é basicamente um esquema XML. Se você está procurando uma solução para declarações de entidade que podem ter potencial para XXE (entidade externa), habilite uma defesa com lista de inclusões contra XXE usando propriedades do sistema.

Para análise de XMLDocument e XMLUtil

Se suas personalizações usarem `XMLDocument` ou `XMLUtil`, defina as seguintes propriedades do sistema. Elas controlam a expansão da entidade e permitem a validação de entidades externas, o que permite o processamento apenas de algumas nas listas de inclusões.

Configuração do limite de expansão da entidade (proteção de segurança da instância)

Use a propriedade *`glide.xmlutil.max_entity_expansion`* para alterar o limite máximo de expansão da entidade para um número menor.

A Now Platform não processa outras expansões de entidade que sejam maiores do que o limite permitido especificado nesta propriedade.

Nota: 3000 é o mínimo padrão imposto pela Now Platform, que é considerado um limite seguro. Portanto, a plataforma considera este mínimo padrão se o valor inteiro inserido estiver abaixo de 3000.

Mais informações

Atributo	Descrição
Nome da propriedade	glide.xmlutil.max_entity_expansion
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Configurar na Central de segurança da instância	Sim
Finalidade	Este controle de correção deve ser habilitado para defesa contra ataques de expansão de entidade XML/Billion laughs.
Valor recomendado	3000

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Impacto funcional	(Baixo) Se a personalização estiver usando a expansão de entidade grande, a Now Platform poderá bloquear o processamento posterior.
Risco à segurança	(Alto) Um invasor pode usar esta vulnerabilidade para expandir os dados de forma exponencial, consumindo rapidamente todos os recursos do sistema.

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Validação de entidade XMLdoc/XMLUtil com lista de permissões (proteção de segurança da instância)

Use a propriedade *glide.xml.entity.whitelist.enabled* para habilitar a validação de entidade externa e só permitir o processamento de entidades listadas de inclusão.

- Se você definir esta propriedade como **verdadeira**, ela permitirá o processamento somente de entidades com lista de inclusões (configuração recomendada).
- Se você definir esta propriedade como **falsa**, ela permitirá o processamento de todas as entidades externas.

Pré-requisitos

Antes de definir essa propriedade, defina uma listagem de FQDN delimitada por vírgula na propriedade *glide.xml.entity.whitelist*, que são os únicos URLs que podem ser acessados usando a propriedade de processamento de entidade de XML. Para saber mais, consulte Processamento de entidade externa XML - lista de permissões.

Mais informações

Atributo	Descrição
Nome da propriedade	*glide.xml.entity.whitelist.enabled*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Configurar na Central de segurança da instância	Sim
Finalidade	Esse controle de correção deve ser ativado para se defender contra ataques XXE.
Valor recomendado	verdadeiro
Impacto funcional	(Baixo) Se a personalização estiver usando uma entidade externa, não a inclusão listada na propriedade *glide.xml.entity.whitelist*, a Now Platform poderá bloquear o processamento adicional. Para saber mais, consulte Processamento de entidade externa XML - lista de permissões.
Risco à segurança	(Alto) Um invasor pode usar o DTD para incluir solicitações HTTP arbitrárias que o servidor pode executar. Isso pode levar a outros ataques usando o

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
	relacionamento de confiança do servidor com outras entidades.
Solução alternativa	Se você não estiver usando a expansão de entidade externa, desabilite-a. Para saber mais, consulte Desabilitar expansão de entidade.

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Para analisadores de XMLDocument2

Se suas personalizações usarem um analisador de XMLDocument2, use as seguintes propriedades do sistema para habilitar a validação de entidade externa.

Desabilitar a expansão da entidade (proteção de segurança da instância)

Se as personalizações não exigirem expansão de entidade, use a propriedade *glide.stax.allow_entity_resolution* para desabilitar completamente a expansão de entidade externa. O XML conclui a análise, mas não inclui entidades internas ou externas.

- Se você definir esta propriedade como **verdadeira**, todas as entidades externas tentarão resolver ou expandir as entidades de assunto, sujeitas à configuração da propriedade *glide.stax.whitelist_enabled*.
- Se você definir essa propriedade como **falsa**, todas as resoluções e expansões da entidade serão bloqueadas. Para saber mais, consulte Validação de entidade XMLdoc2 com lista de permissões.

Pré-requisitos

Antes de definir esta propriedade:

- Defina as propriedades *glide.xml.entity.whitelist.enabled* e *glide.stax.whitelist_enabled* como verdadeiras. Para aprender mais, consulte Validação de entidade XMLdoc/XMLUtil com lista de permissões e Validação de entidade XMLdoc2 com lista de permissões.
- Defina uma lista de FQDN delimitada por vírgulas na propriedade *glide.xml.entity.whitelist*, que são os únicos URLs que podem ser acessados usando o a propriedade de processamento de entidade de XML. Para saber mais, consulte Processamento de entidade externa XML - lista de permissões.

Mais informações

Atributo	Descrição
Nome da propriedade	glide.stax.allow_entity_resolution
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Configurar na Central de segurança da instância	Sim
Finalidade	Este controle de correção deve ser habilitado para defesa contra um ataque de expansão de entidade XML/Billion laughs.
Valor recomendado	falso

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Impacto funcional	(Baixo) Se a personalização estiver usando expansão de entidade, então, a Now Platform pode bloquear o processamento adicional.
Risco à segurança	(Alto) Um invasor pode usar esta vulnerabilidade para expandir os dados de forma exponencial, consumindo rapidamente todos os recursos do sistema.
Solução alternativa	Se a personalização exigir expansão da entidade, defina esta propriedade como verdadeira e siga as etapas documentadas na Validação de entidade XMLdoc2 com lista de permissões.

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Para obter mais informações sobre os recursos OWASp, consulte OWASp.

Validação de entidade XMLdoc2 com lista de permissões (proteção de segurança da instância)

Use uma propriedade para habilitar o processamento, usando XMLDocument2, de entidades externas com lista de inclusões.

Pré-requisitos

Antes de definir esta propriedade:

- Defina a propriedade *glide.xml.entity.whitelist.enabled* como verdadeira. Para saber mais, consulte Validação de entidade XMLdoc/XMLUtil com lista de permissões.
- Defina uma lista de FQDN delimitada por vírgulas na propriedade *glide.xml.entity.whitelist*, que são os únicos URLs que podem ser acessados usando o a propriedade de processamento de entidade de XML. Para saber mais, consulte Processamento de entidade externa XML - lista de permissões.

Mais informações

Atributo	Descrição
Nome da propriedade	glide.stax.whitelist_enabled
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Configurar na Central de segurança da instância	Sim
Finalidade	Esse controle de correção deve ser habilitado para se defender contra ataques de entidade externa de XML.
Valor recomendado	verdadeiro
Impacto funcional	(Baixo) Se a personalização estiver usando uma entidade externa que não esteja incluída na lista, a Now Platform poderá bloquear o processamento adicional. Para saber mais, consulte Processamento de entidade externa de XML - lista de permissões.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Risco à segurança	(Alto) Um invasor pode usar o DTD pode incluir solicitações HTTP arbitrárias que o servidor pode executar. Usar a relação de confiança do servidor com outras entidades pode levar a outros ataques.

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Processamento de entidade externa de XML - lista de permissões (proteção de segurança da instância)

Use a propriedade *glide.xml.entity.whitelist* para habilitar o acesso a uma listagem de FQDN delimitada por vírgulas, se necessário. Esses URLs são os únicos que podem ser acessados usando o processamento de entidade de XML.

Pré-requisitos

Antes de definir esta propriedade, defina a propriedade *glide.xml.entity.whitelist.enabled*, que permite a validação de uma entidade externa e só permite o processamento da lista de inclusões especificada na propriedade *glide.xml.entity.whitelist*. Para saber mais, consulte Validação de entidade XMLdoc/XMLUtil com lista de permissões.

Mais informações

Atributo	Descrição
Nome da propriedade	glide.xml.entity.whitelist
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Configurar na Central de segurança da instância	Sim
Finalidade	Criar uma lista de inclusões de URLs que o processamento da entidade de XML pode acessar.
Valor recomendado	Usuário especificado (por exemplo, https://google.com)
Impacto funcional	(Baixo) O processamento da entidade externa pode ser bloqueado se não for mencionado na lista de inclusões. Quando a lista de inclusões está habilitada, ela requer o formulário PÚBLICO de uma definição de entidade externa.
Risco à segurança	(Alto) Um invasor pode usar o DTD pode incluir solicitações HTTP arbitrárias que o servidor pode executar. Isso pode levar a outros ataques usando o relacionamento de confiança do servidor com outras entidades

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Gestão de sessões (proteção de segurança da instância)

O Gestão de sessões ajuda a identificar corretamente o tráfego que pertence a um usuário específico. Tome precauções para garantir que não haja abuso do relacionamento de confiança.

As aplicações s da Web podem criar sessões para rastrear usuários anônimos após a primeira solicitação do usuário. Um exemplo seria manter a preferência de idioma do usuário, garantindo:

- Identificação do usuário em todas as solicitações subsequentes.
- Aplicação de controles de acesso de segurança.
- Autorização de acesso aos dados privados do usuário.
- Aumento da usabilidade da aplicação.

Portanto, as aplicações da Web atuais podem fornecer recursos de sessão de pré e pós-autenticação.

Autenticação e Gestão de sessões

Autenticação é o processo de verificar se um indivíduo, entidade ou site é quem afirma ser.

A autenticação tenta verificar a identidade digital do remetente de uma comunicação. Testar o esquema de autenticação significa entender como o processo de autenticação funciona e usar essas informações para contornar o mecanismo de autenticação. Um exemplo comum é o processo de login. A autenticação ocorre após o envio de um nome de usuário, ID de usuário e um ou mais itens de informações privadas que somente o usuário conheceria.

O Gestão de sessões inclui propriedades relacionadas à segurança que um administrador pode configurar para garantir que os mecanismos de gerenciamento de sessão seguro sejam estabelecidos na Now Platform.

Tempo limite absoluto da sessão (proteção de segurança da instância)

Use a propriedade *glide.ui.user_cookie.max_life_span_in_days* para definir uma duração máxima para os cookies de usuários criados quando os usuários fazem login com a caixa de seleção **Lembrar-me** selecionada. Quando o cookie expirear, os usuários que tiverem selecionado a caixa de seleção **Lembrar-me** serão forçados a se reautenticar na instância.

Ela habilita a validade do cookie de usuário durante dias específicos a partir de quando o cookie foi publicado pela primeira vez. O valor padrão é 30 dias e o limite máximo é de 365 dias.

Nota: Para impor um tempo máximo de sesssão para sessões de usuário ativas, consulte Configurar um tempo ativo máximo para sessões de usuário.

Mais informações

Atributo	Descrição
Nome da propriedade	*glide.ui.user_cookie.max_life_span_in_days*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Configurar na Central de segurança da instância	Sim

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Finalidade	Para forçar os usuários que selecionaram a caixa de seleção **Lembrar-me** a se reautenticar após dias específicos.
Impacto funcional	(Médio) Esta propriedade impõe um novo login obrigatório, evitando qualquer tipo de rotação de cookie após um determinado intervalo de tempo.
Risco à segurança	(Médio) Os cookies do usuário ativos por um período indefinido de tempo são um risco à segurança e devem expirar em uma configuração baseada em tempo.
Referências	Propriedades do sistema disponíveis Lembrar minhas informações

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Token anti-CSRF (proteção de segurança da instância)

Use a propriedade *glide.security.use_csrf_token* para garantir o uso de um token seguro para identificar e validar solicitações de entrada, que por sua vez são usadas para impedir esses ataques.

A CSRF (Cross-Site Request Forgery, falsificação de solicitação de site cruzado) é um ataque que força um usuário final a executar ações indesejadas em uma aplicação da Web na qual ele está autenticado no momento. Os ataques de CSRF visam especificamente solicitações de mudança de estado, e não o roubo de dados, já que o invasor não tem como ver a resposta à solicitação forjada.

As propriedades a seguir podem ser habilitadas para controles adicionais pelo token CSRF:

- *glide.security.csrf_previous.time_limit*
- *glide.security.csrf_previous.allow*
- *glide.security.csrf.strict.validation.mode*

Mais informações

Atributo	Descrição
Nome da propriedade	glide.security.use_csrf_token
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Configurar na Central de segurança da instância	Sim
Finalidade	Proteger a aplicação de um possível ataque de CSRF.
Valor recomendado	verdadeiro
Impacto funcional	(Baixo) Esta correção permite uma etapa de validação extra antes que o usuário da instância envie uma solicitação de gravação para a instância. Cada solicitação de gravação contém um token CSRF (ou seja, um ID de validação/CSRF vinculado

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
	à sessão do usuário). Quando a sessão do usuário expira, o token de segurança expira também.
Risco à segurança	(Alto) A falsificação de solicitação de site cruzado é um risco de segurança significativo que viola a integridade dos dados da instância. Um invasor pode iniciar o ataque de CSRF abusando da confiança de um usuário da instância. Com a ajuda de ataques de engenharia social, um usuário pode enviar uma solicitação malformada em nome do invasor na instância.

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Alterar credenciais padrão (proteção de segurança da instância)

Use a caixa de seleção **A senha precisa ser redefinida** em Usuários e grupos para garantir que um usuário ilegítimo não possa tirar proveito dos dados padrão.

A Now Platform inclui alguns dados padrão quando a instância é zbootada ou quando você provisiona uma nova instância. Ela pode conter as contas de usuário de demonstração, como administrador padrão, ITIL e funcionário. Definir a propriedade torna necessário mudar o administrador padrão, a ITIL e as credenciais do funcionário ao fazer login na aplicação.

Etapas para configurar

1. Faça login com o nome de usuário **admin** e a senha **admin**.
2. Navegue até **Segurança do sistema** > **Usuários** > **Usuários e grupos.**
3. Pesquise o usuário em ID do usuário **admin** e Nome **administrador**. Clique na ID do usuário do **administrador** para modificar as configurações do usuário.
4. Modifique o campo **E-mail** para refletir um endereço de e-mail válido para esse usuário.
5. Marque a caixa de seleção a **A senha precisa ser redefinida**.
6. Clique em **Atualizar**.
7. Logout.
8. Faça login novamente para ser solicitado a definir uma nova senha.
9. Repita as etapas 3 a 7 para ITIL e contas de funcionário.

Cookies somente HTTP (proteção de segurança da instância)

Use a propriedade *glide.cookies.http_only* para habilitar o atributo HTTPOnly para cookies confidenciais.

Use o atributo HTTPOnly para impedir ataques, como script entre sites, porque ele não permite o acesso ao cookie usando um script do lado do cliente, como JavaScript. Ele não elimina os riscos de script entre sites, mas elimina alguns vetores de exploração.

Mais informações

Atributo	Descrição
Nome da propriedade	glide.cookies.http_only

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Configurar na Central de segurança da instância	Sim
Finalidade	Reduzir o risco de um script do lado do cliente acessar o cookie protegido.
Valor recomendado	verdadeiro
Impacto funcional	(Baixo) Esta correção adiciona um sinalizador HTTPOnly extra nos cookies da sessão, protegendo-os contra roubos. • Se você tiver uma funcionalidade personalizada que requer JavaScript para acessar o cookie do usuário, essa funcionalidade será interrompida. Não será o caso em circunstâncias normais. • A Now Platform lida com a gestão de sessão e não deve haver um motivo para um script personalizado acessar os cookies do usuário.
Risco à segurança	(Médio) Os cookies de sessão na aplicação autenticam um usuário final e fornecem permissões de acesso implícitas na aplicação. Isso significa que há uma necessidade de protegê-los contra roubos ou exportação. Sinalizadores HTTP somente protegem os cookies de sessão de injeções de JavaScript ou vulnerabilidades de script entre sites que os roubam.
Referências	Propriedades do sistema disponíveis

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Validação estrita de CSRF (proteção de segurança da instância)

Use a propriedade *glide.security.csrf.strict.validation.mode* para habilitar a validação estrita do token CSRF. Se o token CSRF não corresponder, impedirá o reenvio da solicitação.

Mais informações

Atributo	Descrição
Nome da propriedade	glide.security.csrf.strict.validation.mode
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Configurar na Central de segurança da instância	Sim
Finalidade	Impor a validação estrita do token CSRF e impedir sua reutilização.
Valor recomendado	verdadeiro
Impacto funcional	(Médio) Esta correção permite uma etapa de validação extra antes que o usuário da instância

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
	envie uma solicitação de gravação para a instância. Ela verifica se o token CSRF atual foi usado anteriormente. Se sim, impede o envio de outras solicitações de gravação.
Risco à segurança	(Médio) A falsificação de solicitação de site cruzado é um risco de segurança significativo que viola a integridade dos dados da instância. Um invasor pode iniciar o ataque de CSRF em qualquer usuário da instância abusando da confiança do usuário da instância. Com a ajuda de ataques de engenharia social, um usuário pode enviar uma solicitação malformada à instância em nome do invasor.

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Desabilitar autenticação sem senha (proteção de segurança da instância)

Use a propriedade *glide.login.no_blank_password* para impedir que os usuários efetuem login na Now Platform com senhas em branco ou deixando o campo **Senha** vazio.

Mesmo que o administrador atribua intencionalmente um valor nulo ou uma senha em branco nos registros do usuário, um usuário não poderá fazer login sem fornecer um valor no campo **Senha**.

Mais informações

Atributo	Descrição
Nome da propriedade	glide.login.no_blank_password
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Configurar na Central de segurança da instância	Sim
Finalidade	Garantir uma autenticação forte, já que às vezes o nome de usuário é fácil de adivinhar em uma organização.
Valor recomendado	verdadeiro
Impacto funcional	(Baixo) Operações não devem usar senhas em branco porque isso é visto como um risco de segurança crítico. No entanto, se houver um caso válido para esse uso, há a possibilidade de uma indisponibilidade. Usuários com senhas em branco não poderão fazer login na instância.
Risco à segurança	(Alto) Um invasor pode fazer login na instância com os nomes de usuário padrão ou por indivíduo/grupo específico (geralmente nome.sobrenome) sem qualquer senha. Isso é visto como um risco de segurança crítico, pois permitiria que um usuário público violasse a confidencialidade e a integridade dos dados da instância.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Habilitar autenticação multifator (MFA) (proteção de segurança da instância)

Use a propriedade *glide.authenticate.multifactor* para habilitar a autenticação multifator (MFA) na instância. A MFA é um requisito de segurança que requer que um usuário insira mais de um conjunto de credenciais para autenticar em uma instância.

Mais informações

Atributo	Descrição
Nome da propriedade	glide.authenticate.multifactor
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Configurar na Central de segurança da instância	Sim
Finalidade	Reforçar a segurança da instância com a introdução da autenticação multifator para logins de usuário interativos.
Valor recomendado	verdadeiro
Impacto funcional	(Médio) Habilitar esta propriedade melhora a experiência do usuário. Ela atua como uma camada extra de proteção e segurança contra credenciais comprometidas.
Risco à segurança	(Médio) Se esta propriedade não estiver habilitada, há um risco de acesso não autorizado a dados confidenciais.
Referências	Propriedades do sistema de autenticação multifator

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Definir critérios de autenticação multifator baseados em função

Use a propriedade *glide.authenticate.multifactor* para impor a MFA (multi-factor authentication, autenticação multifator) baseada em função para todos os usuários atribuídos a funções específicas.

Imponha autenticação multifator com base nas funções atribuídas ao usuário. Se um usuário tiver sido atribuído à função "admin", "security_admin" ou "user_admin" na lista de funções multifator, a MFA será aplicada

- Defina essa propriedade como **verdadeira** para impor a autenticação multifator baseada em função a todos os usuários atribuídos a funções específicas.
- Defina essa propriedade como **falsa** para impor a autenticação multifator baseada em função a todos os usuários atribuídos a funções específicas.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mais informações

Atributo	Descrição
Nome da propriedade	*glide.authenticate.multifactor*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Configurar na Central de segurança da instância	Sim
Finalidade	Impor a autenticação multifator baseada em função a todos os usuários atribuídos a funções específicas.
Tipo	verdadeiro/falso
Valor recomendado	*verdadeiro*
Dependências de segurança	Ativar **Autenticação multifator baseada em função** junto à tabela **Critérios de multifator**.
Impacto funcional	(Médio) Habilitar esta propriedade melhora a experiência do usuário. Ela atua como uma camada extra de proteção e segurança contra credenciais comprometidas.
Risco à segurança	(Médio) Se esta propriedade não estiver habilitada, há um risco de acesso não autorizado a dados confidenciais.
Referências	Configuração dos critérios multifatores baseados em função

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Habilitar verificações da política de Redefinição de senha (proteção de segurança da instância)

Use a propriedade **glide.enable.password_policy** para habilitar verificações de política de senha sempre que um usuário mudar a senha usando a interface do usuário.

Para definir qual política de senha usar quando esta propriedade estiver habilitada, consulte Habilitação das políticas de senha na sua instância.

Nota: A **glide.enable.password_policy** não se aplica quando um administrador muda uma senha ou adiciona um usuário por meio de script.

Mais informações

Atributo	Descrição
Nome da propriedade	glide.enable.password_policy
Configurar na Central de segurança da instância	Sim
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Finalidade	Aplicar a política de senha no momento da mudança de senha.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Valor recomendado	verdadeiro (para senhas de maior força)
Impacto funcional	(Médio) Definir a propriedade como verdadeira ativa as verificações de política de senha quando um usuário redefine a senha.
Risco à segurança	(Médio) Sem uma política de senha, um usuário pode criar uma senha fraca, o que aumenta a probabilidade de um adversário obter acesso à instância.

Etapas para configurar

Se você definir esta configuração na página de Configuração de conformidade de proteção na Central de segurança da instância:

1. Em **Médio**, selecione **Gestão de sessões**.
2. Na configuração **Habilitar verificações da política de Redefinição de senha**, selecione **Média** para senhas de força média ou **Alta** para senhas mais robustas e de maior força. Selecionar uma dessas opções define a propriedade **glide.enable.password_policy** como verdadeira e inicia um fluxo de trabalho que atualiza automaticamente sua política de senha.

Além disso, você pode definir a propriedade do sistema *glide.apply.password_policy.on_login* para habilitar verificações de política de senha no momento do login.

Gerenciamento de tentativas de login com falha (proteção de segurança da instância)

Há duas ações de script disponíveis que permitem a um administrador de site gerenciar o número de vezes que um usuário pode fornecer uma senha incorreta antes de ser bloqueado na Now Platform. Você pode habilitar qualquer uma dessas ações de script para gerenciar tentativas de login sem êxito.

Mais informações

Atributo	Descrição
Nome da propriedade/plug-in	N/D
Tipo de configuração	Política do Sistema > Ações de Script
Configurar na Central de segurança da instância	Sim
Finalidade	Impor uma política rígida para tentativas de login com falha para evitar ataques de força bruta de credenciais.
Valor recomendado	Ativo
Impacto funcional	(Baixo) Esta correção permite ao administrador da instância monitorar e relatar qualquer acesso de usuário mal-intencionado. Nenhum impacto na funcionalidade, somente mudança na experiência do usuário.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Risco à segurança	(Médio) Aplique uma estratégia de registro em log e auditoria definida para que você possa identificar e agir em atividades suspeitas em tempo hábil.
Referências	

Etapas para configurar

1. Navegue até **Política do sistema** > **Ações de Script.**
2. Pesquise o nome *`*SNC User`*.
3. Para habilitar o gerenciamento de tentativas de login sem êxito, altere o estado Ativo das ações de script *`SNC User Lockout Check with Auto Unlock`* ou *`SNC User Lockout Check`* de **falso** para **verdadeiro**.
4. Para redefinir o contador de login sem êxito após um login bem-sucedido, você pode ativar a ação de script *`SNC User Clear`*.

Preenchimento automático do campo de senha (proteção de segurança da instância)

Use a propriedade *`glide.login.autocomplete`* para permitir que navegadores usem o preenchimento automático em campos de senha de formulários de login.

Mais informações

Atributo	Descrição
Nome da propriedade	glide.login.autocomplete
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Configurar na Central de segurança da instância	Sim
Finalidade	Desabilitar o navegador para tentar preencher automaticamente um campo de senha.
Valor recomendado	falso
Impacto funcional	(Baixo) Esta correção faz com que o sinalizador de **Preenchimento automático do campo de senha** seja desativado de forma que o cache de histórico de senha por navegador não seja mostrado no campo. Não deve haver nenhum impacto na funcionalidade.
Risco à segurança	(Baixo) Os campos de autenticação de usuário devem ser validados e nunca devem permitir o cache do lado do cliente.
Referências	https://support.servicenow.com/kb_view.do?sysparm_article=KB0563953

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Remover credenciais da página de boas-vindas (proteção de segurança da instância)

Modifique o conteúdo padrão na página de boas-vindas para remover as credenciais padrão.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Dois registros de Como fazer login fazem parte dos dados de demonstração do plug-in CMS. Se você não instalar os dados de demonstração para uma instância, esses registros não existirão. Nesse caso, a configuração é considerada em conformidade com as práticas de segurança recomendadas. Para saber mais, consulte Práticas recomendadas de segurança.

Etapas para configurar

1. Navegue até **IU do sistema** > **Conteúdo da página de boas-vindas** > .
2. Encontre as duas seções com uma descrição resumida de **Como fazer login**.
3. Altere o estado Ativo de cada uma de **verdadeiro** para **falso**.

Remover a opção Lembrar-me (proteção de segurança da instância)

Use a propriedade *glide.ui.forgetme* para remover a caixa de seleção **Lembrar-me** da página de login para impedir que as informações de login sejam armazenadas em cache.

Mais informações

Atributo	Descrição
Nome da propriedade	glide.ui.forgetme
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Configurar na Central de segurança da instância	Sim
Finalidade	Garantir que nenhuma informação de autenticação seja armazenada em cache.
Valor recomendado	verdadeiro
Impacto funcional	(Baixo) Esta correção mudaria a experiência do usuário, desconectando-o automaticamente da instância quando a sessão expirar. A expiração da sessão dependeria exclusivamente do valor definido na propriedade do sistema, conforme detalhado em Gerenciar sessões de usuário.
Risco à segurança	(Médio) Quando você marca a caixa de seleção **Lembrar-me** no login, um cookie extra é armazenado no computador do usuário. • Sua finalidade é restabelecer automaticamente a sessão para as visitas subsequentes do usuário conectado. • Isso representa um risco de segurança, pois permite que a sessão do usuário esteja ativa até que ele faça logout intencionalmente. A probabilidade de um ataque para este cenário aumenta quando o usuário final deixa o navegador sem supervisão ou se ele for comprometido por um ataque diferente.
Referências	Remover a caixa de seleção Lembrar-me

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Rotação de identificadores de sessão HTTP (proteção de segurança da instância)

Use a propriedade *glide.ui.rotate_sessions* para habilitar a rotação dos identificadores de sessão HTTP para reduzir vulnerabilidades de segurança.

Se o ID de sessão de um usuário não autenticado não mudar após a autenticação, uma aplicação da Web estará vulnerável a um ataque de fixação de sessão. Um usuário mal-intencionado pode iniciar uma sessão não autenticada e fornecer o ID de sessão associado à vítima. Depois que a vítima é autenticada, o usuário mal-intencionado agora compartilha essa sessão autenticada.

Mais informações

Atributo	Descrição
Nome da propriedade	glide.ui.rotate_sessions
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Configurar na Central de segurança da instância	Sim
Finalidade	Obter uma autenticação de sessão mais segura.
Valor recomendado	verdadeiro
Impacto funcional	(Médio) Esta correção modifica o SessionID quando o usuário navega de uma página não autenticada para páginas autenticadas. • Se você estiver usando um proxy ou codificando o SessionID quando um usuário fizer login pela primeira vez, ou para qualquer finalidade, poderá haver um possível impacto na funcionalidade. • Se você estiver usando o plug-in SAML 2.0 para autenticação de Single Sign-on, ele poderá interferir no compartilhamento de informações da sessão entre a instância e o Provedor de identidade. Nesse caso, você pode definir esta propriedade como falsa.
Risco à segurança	(Tardio) SessionID é usado para processar e autenticar o usuário da instância, mantendo o estado da sessão no navegador. Portanto, SessionID é considerado como dados confidenciais e deve ser seguro por padrão. A Rotação de sessão é um controle de segurança que impõe a alteração de sessionID sempre que o usuário navega de páginas não autenticadas para autenticar páginas.
Referências	Autenticação com SAML

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Cookies de sessão segura (proteção de segurança da instância)

Use a propriedade *glide.ui.secure_cookies* para exigir cookies formatados corretamente

Quando você define a propriedade como verdadeira, sua instância rejeita uma sessão se o cookie associado não estiver no formato esperado.

Mais informações

Atributo	Descrição
Nome da propriedade	glide.ui.secure_cookies
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Configurar na Central de segurança da instância	Sim
Finalidade	Obter uma autenticação de sessão mais segura.
Valor recomendado	verdadeiro
Impacto funcional	(Baixo) Quando a propriedade é definida como verdadeira, os cookies formatados incorretamente são rejeitados. Quando esse tipo de cookie é rejeitado, o usuário deve fazer login novamente.

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Política de referência de segurança (proteção de segurança da instância)

Use a propriedade *com.glide.security.referrerpolicy* para controlar quais dados de referenciador devem ser enviados em cabeçalhos de resposta HTTP quando as páginas Now Platform enviam solicitações de dados. O valor de Política de referência em um cabeçalho HTTP controla quais informações de referência devem ser incluídas nas solicitações de dados.

Valores da política de referência de segurança

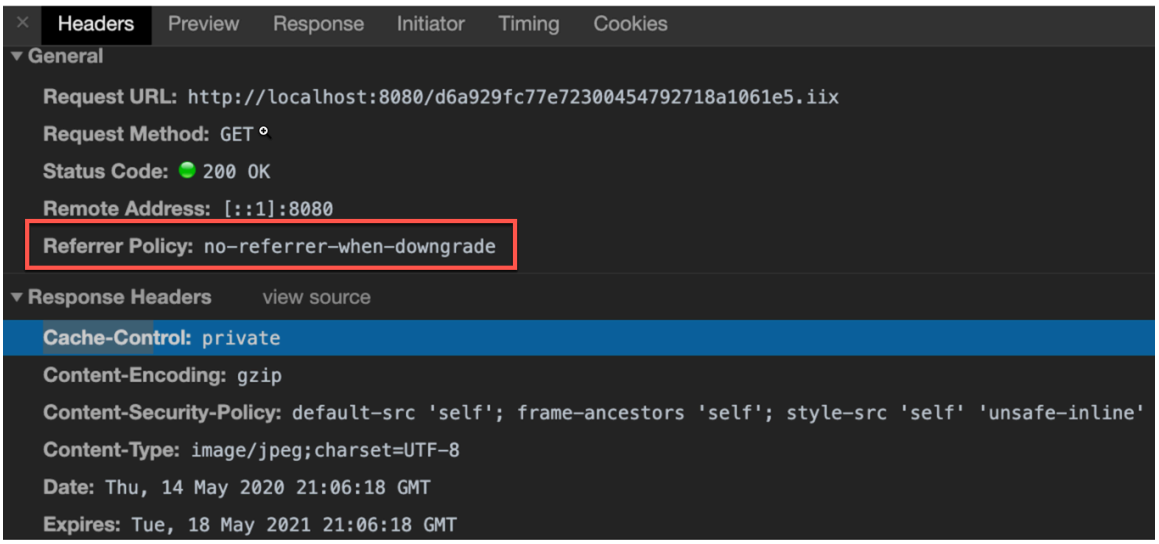
Defina a propriedade *com.glide.security.referrerpolicy* como um dos seguintes valores.

valor	Descrição
padrão	A instância da Now Platform gerencia o nível de informações enviadas nos cabeçalhos de referência apropriados para a solicitação de página da Now Platform específica.
mesma origem	As páginas da Now Platform enviam um URL de referenciador completo na instância e no mesmo domínio, e nenhum cabeçalho de referenciador para a origem externa. Esta configuração garante um bom nível de segurança da instância.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

valor	Descrição
origem	As páginas da Now Platform enviam o URL base no cabeçalho do referenciador na instância e no mesmo domínio, e também externamente. Esta configuração garante um bom nível de segurança da instância.
origin-when-cross-origin	As páginas da Now Platform enviam todo o URL no cabeçalho do referenciador dentro da instância e do mesmo domínio e envia apenas o URL base externamente. Esta configuração garante um bom nível de segurança da instância.
no-referrer-when-downgrade	As páginas da Now Platform enviam a origem, o caminho e a cadeia de caracteres de consulta no URL, desde que não haja downgrade em um protocolo de segurança. **Nota:** Esta configuração não garante um bom nível de segurança de instância na Now Platform e não deve ser usada.

Exemplo de política de referenciador e resumo de valores



© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mais informações

Atributo	Descrição
Nome da propriedade	com.glide.security.referrerpolicy
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Configurar em Central de segurança da instância	Não
Finalidade	Controla a quantidade de dados de entrada enviada por meio do cabeçalho "referenciador" quando uma página da Now Platform envia uma solicitação de dados.
Valor recomendado	padrão
Impacto funcional	(Baixo) Se definida como "padrão", a instância da Now Platform gerenciará o nível de informações enviadas nos cabeçalhos de referência.
Risco à segurança	(Alto) Definir este valor de propriedade como "no-referrer-when-downgrade" não garante um bom nível de segurança para sua instância.
Referência	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy https://developer.mozilla.org/en-US/docs/Glossary/origin

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Tempo limite da atividade da sessão (proteção de segurança da instância)

Use a propriedade *glide.ui.session_timeout* para designar, em minutos, o valor do tempo limite da atividade.

Existem vários impactos funcionais na definição desta propriedade:

- Quanto mais longo for o tempo limite da sessão especificada, maior será a quantidade de memória utilizada durante uma sessão de processamento. O sistema de base usa uma duração de tempo limite padrão do Apache Tomcat de 30 minutos.
- A Now Platform ainda desconecta os usuários com Lembrar-me. Após 30 minutos de inatividade na aplicação, a plataforma desconecta o usuário automaticamente, a menos que a caixa de seleção **Lembrar-me** na página de login esteja marcada. A diferença é que eles não fazem login novamente para continuar.
- Se houver medidores ou conteúdo nas páginas iniciais dos usuários que sejam atualizados automaticamente, esse tempo limite poderá nunca ser atingido.

Mais informações

Atributo	Descrição
Nome da propriedade	glide.ui.session_timeout
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Configurar na Central de segurança da instância	Sim
Finalidade	Impor o tempo limite da sessão.
Valor recomendado	Tempo limite especificado pelo usuário em minutos. 30 minutos é o valor recomendado, mas esse valor pode variar dependendo da funcionalidade e do requisito de segurança. Não defina este valor como mais de um dia.
Impacto funcional	(Médio) Esta correção impõe a expiração oportuna da conta do usuário. Nenhum impacto na funcionalidade, no entanto, a experiência do usuário é alterada.
Risco à segurança	(Médio) As sessões do usuário ativas por um período indefinido de tempo são um risco de segurança e devem expirar em uma configuração baseada em tempo.
Referências	Gerenciar sessões do usuário

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Tempo limite da janela da sessão (proteção de segurança da instância)

Use a propriedade *glide.ui.user_cookie.life_span_in_days* para definir o período de expiração do cookie Lembrar-me. O valor padrão é 15 dias e o limite máximo é de 30 dias.

Mais informações

Atributo	Descrição
Nome da propriedade	glide.ui.user_cookie.life_span_in_days
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Configurar na Central de segurança da instância	Sim
Finalidade	Habilitar a expiração padrão do cookie "lembrar-me".
Valor recomendado	Valor inteiro definido pelo usuário (nº de dias) [Exemplo: 15]
Impacto funcional	(Médio) Esta propriedade é habilitada pelo usuário final quando o usuário final marca a caixa de seleção **Lembrar-me** na página de login e faz login na Now Platform.
Risco à segurança	(Médio) Os cookies do usuário ativos por um período indefinido de tempo são um risco à segurança e devem expirar em uma configuração baseada em tempo.
Referências	Propriedades do sistema disponíveis Lembrar minhas informações

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Configurar senhas para contas de usuário criadas automaticamente

Use as propriedades do sistema *glide.email.inbound.use_default_password* e *glide.user.default_password* para definir como criar senhas para novos usuários criados a partir de e-mails de entrada.

As propriedades do sistema descritas neste documento definem como a instância lida com senhas para contas de usuário geradas de e-mails de entrada. Sua instância precisa ser configurada com a capacidade de receber e-mails e habilitar a criação automática de usuários. Consulte a seção abaixo para obter detalhes sobre essas configurações.

Depois que sua instância for configurada para criar contas automaticamente, você pode usar as propriedades para determinar se deve usar uma senha padrão e definir essa senha, se necessário.

Pré-requisitos

Para usar essas propriedades, sua instância deve ser configurada para criar automaticamente novas contas de usuário.

- Você deve configurar seu próprio servidor POP3 para armazenar e receber e-mails para sua instância. Em seguida, você deve definir a propriedade do sistema *glide.email.read.active* como verdadeira. Para saber mais sobre como configurar um servidor POP3 em sua instância, consulte Habilitar usando seu próprio servidor POP3.
- Defina a propriedade *glide.pop3readerjob.create_caller* como verdadeira. Com esta mudança de propriedade, sua instância pode criar usuários automaticamente a partir do e-mail recebido. Para saber mais, consulte Ativar a criação automática de usuários.

  Nota: Ignore a propriedade *glide.user.default_password* se *glide.pop3readerjob.create_caller* estiver definida como **falsa**.

Como sua instância define senhas

Em Quebec e nas versões anteriores de ServiceNow, sua instância cria novas contas de usuário a partir de e-mails recebidos usando uma senha complexa definida na propriedade do sistema *glide.user.default_password*. Os usuários usam essa senha na primeira vez em que fazem login e, em seguida, a instância solicita uma nova senha ao usuário. Se você fez upgrade da sua instância para Rome ou versões posteriores, este processo permanecerá inalterado. Como administrador, você pode atualizar sua instância para usar o novo método descrito abaixo.

Em novas instâncias que começam com a versão Rome, as contas de usuário criadas a partir de e-mails de entrada não têm uma senha. Quando um usuário acessa a instância pela primeira vez com sua nova conta, ele deve inserir o nome de usuário e clicar no botão **Esqueceu a senha?** para criar uma senha inicial.

Em Rome e versões posteriores, você pode escolher qual processo sua instância segue, definindo um valor na propriedade do sistema *glide.email.inbound.use_default_password*. Para mudar o comportamento padrão descrito acima, crie esta propriedade do sistema usando as seguintes informações:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo Propriedade do sistema	valor
Nome	glide.email.inbound.use_default_password
Tipo	verdadeiro | falso
valor	Selecione um valor com base no comportamento desejado: verdadeiro Novas contas usam uma senha padrão definida na propriedade do sistema *glide.user.default_password*. falso Novas contas não têm uma senha padrão. Os usuários devem definir uma senha, conforme descrito anteriormente nesta seção.

Para obter mais detalhes sobre como criar propriedades do sistema, consulte Adicionar uma propriedade do sistema.

Defina uma senha padrão

Se sua instância estiver configurada para usar uma senha padrão, você deverá definir essa senha usando a propriedade do sistema *glide.user.default_password*. Crie esta propriedade usando as seguintes informações:

Campo Propriedade do sistema	valor
Nome	glide.user.default_password
Tipo	senha2
valor	Insira uma senha exclusiva para usar como padrão. Use a complexidade de senha forte para ajudar a garantir a segurança da sua instância.

Configurações de proteção

O conteúdo de configurações de proteção da Central de Segurança ServiceNow, Inc. contém descrições detalhadas e valores de conformidade para as propriedades do sistema relacionadas à segurança e aos plug-ins em Now Platform. Você pode definir essas propriedades usando o app de configurações de proteção na Central de segurança.

Visão geral e finalidade

A Central de segurança calcula uma pontuação de conformidade diária, expressa como uma porcentagem que é baseada na conformidade das configurações de segurança da instância atuais com os valores de conformidade nas configurações de proteção da Central de segurança.

Você pode gerenciar as definições de configuração de segurança específicas que podem afetar a pontuação da sua instância diretamente da Central de segurança.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

As configurações de proteção são explicadas com vários atributos descritos na tabela.

Detalhes da configuração das configurações de proteção

Atributo da configuração	Descrição
Visão geral	Fornece uma visão geral de alto nível da recomendação.
Nome da configuração	A propriedade ou o nome do plug-in.
Tipo de configuração	Descreve onde a propriedade pode ser configurada fora da Central de Segurança, como nas propriedades do sistema (*sys_properties_list.do*).
Tipo de dados	Descreve o tipo de valor necessário para a configuração. Os exemplos são booliano verdadeiro/falso, instalação, plug-in, cadeia de caracteres etc.
Valor recomendado	O valor recomendado pela Central de Segurança para aprimorar a conformidade de segurança em sua instância.
Valor-padrão	O valor para o qual a configuração está definida no sistema de base.
Categoria	O nome e o link para a categoria da configuração de proteção.
Risco à segurança	**Pontuação de gravidade**: a pontuação indica o possível risco de segurança para sua instância de acordo com a probabilidade de a vulnerabilidade ser explorada. A vulnerabilidade de segurança é considerada e pontuada individualmente usando a pontuação do CVSS (Sistema de Pontuação de Vulnerabilidade Comum) em uma escala que varia de **0,0** a **10,0**. Consulte https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator para obter informações adicionais.
	Classificação de gravidade por pontuação do CVSS: • Crítico: 9,0-10,0 • Alta: 7,0-8,9 • Médio: 4,0-6,9 • Baixo: 0,01-3,9 • Nenhum: 0,0
	Detalhes do risco de segurança: descreve a importância da configuração de definição e o risco de não utilizar a configuração recomendada.
Dependências e pré-requisitos	Configurações relacionadas ou configurações que são necessárias antes ou em conjunto com a configuração de proteção.
Impacto funcional	O impacto desta configuração de proteção sobre a operação da sua instância.
Referências	Links para a documentação de configuração ou outras informações úteis.

Nota: Algumas das configurações só podem ser concluídas por Suporte e atendimento ao cliente e serão indicadas como tal.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para saber mais sobre como garantir que suas instâncias atendam aos requisitos de proteção, consulte Proteção de segurança.

Outros recursos

Para referência do usuário, a Now Platform mantém informações abrangentes sobre os recursos de configuração na documentação do produto. Você pode acessar a maior parte do conteúdo de segurança usando os links encontrados em Proteja sua instância. Além disso, consulte o seguinte:

- Propriedades do sistema disponíveis
- Propriedades de configurações de segurança gerais
- Configurações de alta segurança

Linha de base das configurações de proteção

Explore como versões de linha de base distintas para configurações de proteção se alinham a diferentes versões da família e da Store.

Security Center funciona ingerindo um subconjunto de propriedades do sistema de uma instância e exibindo seus detalhes de configuração, junto com o impacto da não conformidade na segurança do app. A linha de base serve como ponto de referência para as propriedades do sistema que são ingeridas com cada versão do app Security Center.

Visão geral da linha de base das configurações de proteção

Versão do Centro de Segurança	Versão da linha de base das configurações de proteção	Famílias compatíveis	Data de lançamento da Store	Instalado por padrão com
SSC v1.1	Linha de base v1.0	Utah, Vancouver	Maio de 2023	Família Vancouver
SSC v1.2	Linha de base v1.0	Utah, Vancouver	Ago de 2023	Apenas Store
SSC v1.3	Linha de base v2.0	Vancouver, Washington	Nov de 2023	Família Washington
SSC v1.5	Linha de base v4.0	Washington, Xanadu	Maio de 2024	Xanadu
SSC v1.6	Linha de base v4.0	Washington DC, Xanadu	Agosto de 2024	

Novas configurações de proteção para a linha de base versão 4.0

Esta é uma lista de todas as novas configurações de proteção lançadas com a linha de base versão 4.0 da Central de segurança.

- Revisão das condições desnecessárias de controle de acesso a funções explícitas [Removido na Central de segurança 1.5]
- Habilitar regras de consulta de gestão de pedidos de serviço para organizações de serviço [Novo na Central de segurança 1.5]
- Desabilitar a raiz de confiança da ServiceNow
- Restringir o acesso de leitura ao contexto de fluxo [Novo na Central de segurança 1.5]

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Limitar o intervalo do token de atualização móvel de acesso à sessão baseada em política [Novo na Central de Segurança 1.5]
- Habilitar acesso à sessão baseado em política para dispositivos móveis [Novo na Central de segurança 1.5]
- Impedir que usuários inativos façam login [Novo na Central de segurança 1.5]
- Configurar funções de administrador de grupo de atribuição de gestão de eventos [Novo na Central de segurança 1.5]
- Impor escopo de segurança para o Espaço do agente para Gestão de casos de RH [Novo na Central de segurança 1.5]
- Impor o Playbook para licenças e permissões ao escopo de segurança [Novo na Central de segurança 1.5]

Novas configurações de proteção da linha de base versão 2.0

Confira uma lista de todas as novas configurações de proteção lançadas com a linha de base Security Center versão 2.0.

- Como impor o uso de alias de credencial [Novo na Central de segurança 1.3 e atualizado na 1.5]
- Impor verificação do OCSP em caso de erro de rede [Novo na Central de segurança 1.3]
- Verificar a cadeia de certificados e o nome do host [Novo na Central de segurança 1.3]
- Verificar revogação de certificado [Novo na Central de segurança 1.3]
- Definir uma política de segurança de conteúdo para arquivos SVG [Novo na Central de segurança 1.3]
- Uso da operação segura de inserção múltipla na API de conjuntos para importação [Novo na Central de segurança 1.3]
- Habilitar o plug-in de tabelas protegidas [Novo na Central de segurança 1.3]
- Impor política de referenciador seguro [Novo na Central de segurança 1.3]
- Definir funções de exceção de tempo limite de sessão ativa [Novo na Central de segurança 1.3]
- Invalidação proativa de sessões inativas [Novo na Central de segurança 1.3]
- Validar tipo de arquivo MIME no SOAP Web Service AttachmentCreator [Novo na Central de segurança 1.3]
- Autenticação baseada em certificado não imposta [Novo na Central de segurança 1.3]
- Registrar eventos de auditoria de sessão [Novo na Central de segurança 1.3]
- Exigir autenticação no processador HTTP da Gestão de eventos [Novo na Central de segurança 1.3]
- Como impor regras de segurança para compartilhar painéis [Novo na Central de segurança 1.3]
- Proibir clonagem de destino [Novo na Central de segurança 1.3]
- Impor a segurança de escopo para serviços digitais para setor público [Novo na Central de segurança 1.3]
- Impor o acesso por ACL com escopo definido para os Information Request Playbooks [Novo na Central de segurança 1.3]
- Limitar a duração da sessão ativa do convidado [Novo na Central de segurança 1.3]
- Limitar a duração da sessão ativa de integrações [Novo na Central de segurança 1.3]

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Restringir o acesso às bases de conhecimento [Novo na Central de segurança 1.3]
- Ocultar comentários de usuários em artigos [Novo na Central de segurança 1.3]
- Restringir parâmetros OAuth no corpo de POST [Novo na Central de segurança 1.3]
- Como limitar o tamanho de anexos em fluxos de treinamento e previsão [Novo na Central de segurança 1.3 e atualizado na 1.5]
- Garantir que a criação e a exclusão de painéis exijam verificação de acesso [Novo na Central de segurança 1.3]
- Como desativar o comportamento legado de limitação do escopo do GlideRecord [Novo na Central de segurança 1.3]
- Como impor restrições de escopo da aplicação [Novo na Central de segurança 1.3]
- Exigir acesso de gravação à página Adicionar item do Catálogo de serviços [Novo na Central de segurança 1.3]
- Tempo de validação do token anti-CSRF [Novo na Central de segurança 1.3]
- Garantir a verificação das ACLs da tabela de arquivamento [Novo na Central de segurança 1.3]
- Habilitar o gerenciador de segurança Java protegido [Novo na Central de segurança 1.3]
- Impor privilégio de elevação estrita [Novo na Central de segurança 1.3]
- Exigir limpeza da área de transferência ao colocar a aplicação para celular em segundo plano [Novo na Central de segurança 1.3]
- Impor requisitos de criptografia e senha do dispositivo [Novo na Central de segurança 1.3]
- Limitar a duração da sessão ativa da IU [Novo na Central de segurança 1.3]
- Habilitar o log de auditoria de MID [Novo na Central de segurança 1.3 e atualizado na 1.5]
- Fábricas exigidas de conexão JMS [Novo na Central de segurança 1.3 e atualizado na 1.5]
- Exigência de captcha para walk-up experience de convidados na aplicação Atendimento ao cliente [Novo na Central de segurança 1.3 e atualizado na 1.5]
- Verificação da representação na avaliação de ACL no app de RH [Novo na Central de segurança 1.3 e atualizado na 1.5]
- Como restringir atualizações de casos de RH nos e-mails pessoais [Novo na Central de segurança 1.3 e atualizado na 1.5]

Configurações atualizadas de proteção da versão de linha de base 4.0

A lista de configurações de proteção que passaram por atualização na versão de linha de base 4.0 da Security Center.

A versão de linha de base 4.0 inclui várias atualizações nas descrições resumidas de estilo e consistência entre registros. Além disso, muitos scripts relacionados às propriedades também foram atualizados para melhorar a precisão do valor padrão para os casos em que a propriedade foi removida da tabela sys_property.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Documentação	Atualizações
Exigência de autorização para solicitações SOAP [Atualizado na Central de segurança 1.3 e 1.5]	• Novo nome da configuração técnica: *glide.basicauth.required.soap, glide.soap.require_ws_security* • Nome antigo da configuração técnica: *glide.basicauth.required.soap*
Como habilitar o Sanitizer de HTML no Virtual Agent [Atualizado na Central de segurança 1.3]	• Nova descrição resumida: Como habilitar a limpeza de HTML no Virtual Agent • Descrição resumida antiga: Como habilitar a limpeza de HTML
Negação de acesso interno a funções externas explícitas [Atualizado na Central de segurança 1.5]	• Novo nome da configuração técnica: *glide.security.explicit_roles.enable_internal_u* • Nome antigo da configuração técnica: *glide.security.explicit_roles.enable_internal_u*
Como definir tipos MIME para download restritos [Atualizado na Central de segurança 1.3]	• Nova descrição resumida: Como definir tipos MIME restritos para download • Descrição resumida antiga: Como restringir tipos MIME para download
Restrição de domínios de e-mail para registro de usuários externos [Atualizado na Central de segurança 1.5]	• Nova descrição resumida: Como definir tipos MIME restritos para download • Descrição resumida antiga: Como restringir tipos MIME para download
Como minimizar a duração da expiração do link de registro de usuário externo [Atualizado na Central de segurança 1.3 e 1.5]	• Nova descrição resumida: Como minimizar a duração de expiração do link de registro de usuário externo • Descrição resumida antiga: Como minimizar a duração de expiração do link de registro de usuário externo (aplicabilidade do plug-in: registro de usuário externo)
Proibir o download de arquivos infectados	• Nova descrição resumida: Como proibir o download de arquivo infectado • Descrição resumida antiga: Como proibir o download de arquivos infectados

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Documentação	Atualizações
Desabilitar depuração do Multi-SSO	• Nova descrição resumida: Como desabilitar depuração do Multi-SSO • Descrição resumida antiga: Como desabilitar depuração Multi-SSO (aplicabilidade do plug-in: Single Sign-On de vários provedores)
Como definir endereços IP internos permitidos da ServiceNow [Atualizado na Central de segurança 1.3 e 1.5]	• Novo nome da configuração técnica: *glide.ip.authenticate.strict* • Nome antigo da configuração técnica: *glide.ip.authenticate.strict,glide.ip.authentic*
Como aplicar a separação de domínios em campos de referência com pontos [Atualizado na Central de segurança 1.3 e 1.5]	• Nova descrição resumida: Como aplicar separação de domínio em campos de referência com pontos • Descrição resumida antiga: Como aplicar separação de domínios em campos de referência com pontos (aplicabilidade do plug-in: separação de domínios)
Como habilitar a recuperação de conta [Atualizado na Central de segurança 1.3 e 1.5]	• Nova descrição resumida: Como habilitar recuperação de conta • Descrição resumida antiga: Como habilitar recuperação de conta (aplicabilidade do plug-in: Single Sign-On de vários provedores)
Como minimizar o limite de expansão da entidade [Atualizado na Central de segurança 1.3]	• Nova descrição resumida: Como minimizar o limite de expansão da entidade para GlideXMLUtil com script • Descrição resumida antiga: Como minimizar o limite de expansão da entidade
Como ativar a versão atualizada do plug-in Multi-SSO [Atualizado na Central de segurança 1.3 e 1.5]	• Nova descrição resumida: Como habilitar a versão atualizada do plug-in Multi-SSO • Descrição resumida antiga: Como habilitar a versão atualizada do plug-in Multi-SSO (aplicabilidade do plug-in: Single Sign-On de vários provedores)

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Documentação	Atualizações
Não usar certificados de demonstração para configurações SAML ativas [Atualizado na Central de segurança 1.5]	• Nova descrição resumida: Não use certificados de demonstração para configurações SAML ativas • Descrição resumida antiga: Não use certificados de demonstração para configurações SAML ativas (aplicabilidade do plug-in: Single Sign-On de vários provedores)
Como minimizar a duração da restrição "notBefore" ou "notOnOrAfter" de SAML [Atualizado na Central de segurança 1.3 e 1.5]	• Nova descrição resumida: Como minimizar a duração da restrição SAML "notBefore" ou "notOnOrAfter" • Descrição resumida antiga: Como minimizar a duração da restrição SAML "notBefore" ou "notOnOrAfter" (aplicabilidade do plug-in: Single Sign-On de vários provedores)
Bloqueio de tokens anti-CSRF expirados [Atualizado na Central de segurança 1.5]	• Nova descrição resumida: Como bloquear tokens anti-CSRF expirados • Descrição resumida antiga: Como bloquear tokens CSRF expirados
Exigência de captcha para walk-up experience de convidados na aplicação Atendimento ao cliente [Novo na Central de segurança 1.3 e atualizado na 1.5]	• Nova descrição resumida: Como exigir captcha para Walk-up Experience de convidado na aplicação de atendimento ao cliente • Descrição resumida antiga: Como exigir captcha para Walk-up Experience de convidado na aplicação de atendimento ao cliente (aplicabilidade do plug-in: Walk-up Experience de convidado para atendimento ao cliente)
Verificação da representação na avaliação de ACL no app de RH [Novo na Central de segurança 1.3 e atualizado na 1.5]	• Nova descrição resumida: Como verificar representação na avaliação da ACL no app de RH • Descrição resumida antiga: Como verificar representação na avaliação da ACL no app de RH (aplicabilidade do plug-in: app com escopo de Recursos Humanos)

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Documentação	Atualizações
Como restringir atualizações de casos de RH nos e-mails pessoais [Novo na Central de segurança 1.3 e atualizado na 1.5]	• Nova descrição resumida: Como restringir atualizações de caso de RH de e-mails pessoais • Descrição resumida antiga: Como restringir atualizações de caso de RH de e-mails pessoais (aplicabilidade do plug-in: app com escopo de Recursos Humanos)
Habilitar o log de auditoria de MID [Novo na Central de segurança 1.3 e atualizado na 1.5]	• Nova descrição resumida: Como habilitar log de auditoria do MID • Descrição resumida antiga: Como habilitar log de auditoria do MID (aplicabilidade do plug-in: MID Server)
Como impor o uso de alias de credencial [Novo na Central de segurança 1.3 e atualizado na 1.5]	• Nova descrição resumida: Como impor uso de alias de credencial • Descrição resumida antiga: Como impor uso de alias de credencial (aplicabilidade do plug-in: MID Server)
Aplicar a validação estrita do token CSRF	• Nova descrição resumida: Como aplicar validação estrita do token CSRF • Descrição resumida antiga: Validação estrita de CSRF
Fábricas exigidas de conexão JMS [Novo na Central de segurança 1.3 e atualizado na 1.5]	• Nova descrição resumida: Fábricas de conexão JMS necessárias • Descrição resumida antiga: Fábricas de conexão JMS necessárias (aplicabilidade do plug-in: MID Server)
Como limitar o tamanho de anexos em fluxos de treinamento e previsão [Novo na Central de segurança 1.3 e atualizado na 1.5]	• Nova descrição resumida: Como limitar o tamanho do anexo em fluxos de treinamento e previsão • Descrição resumida antiga: Como limitar o tamanho do anexo em fluxos de treinamento e previsão (aplicabilidade do plug-in: Inteligência para documentos da plataforma)

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Documentação	Atualizações
Como limitar o tamanho do corpo da resposta HTTP [Novo na Central de segurança 1.3 e atualizado na 1.5]	• Nova descrição resumida: Como limitar o tamanho do corpo da resposta HTTP • Descrição resumida antiga: Como garantir que as respostas HTTP não acionem uma exceção de falta de memória devido ao tamanho do corpo da resposta

Configurações de proteção atualizadas da linha de base versão 2.0

Esta lista contém as configurações de proteção que foram atualizadas na linha de base Security Center versão 2.0.

Documentação	Atualizações
Como restringir solicitações JSONP a URLs confiáveis [Atualizado na Central de segurança 1.3]	• Nova descrição resumida: Restringir solicitações JSONP a URLs confiáveis • Descrição resumida antiga: Lista de inclusões de solicitação JSONP
Como minimizar o tamanho permitido do anexo [Atualizado na Central de segurança 1.3]	• Nova descrição resumida: tamanho mínimo permitido de anexo • Descrição resumida antiga: tamanho máximo permitido de anexo
Como impor a confiança de certificado [Atualizado na Central de segurança 1.3 e removido na 1.5]	• Nova descrição resumida: Aplicar confiança de certificado • Descrição resumida antiga: Confiança de certificado
Definir opções do Xframe para impedir a incorporação de sites de terceiros [Atualizado na Central de segurança 1.3]	• Nova descrição resumida: Definir opções do Xframe para impedir a incorporação de sites de terceiros • Descrição resumida antiga: Opções do Xframe
Como habilitar o Sanitizer de HTML no Virtual Agent [Atualizado na Central de segurança 1.3]	• Nova descrição resumida: Habilitar o limpador de HTML no Virtual Agent • Descrição resumida antiga: Habilitar limpador de HTML

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Documentação	Atualizações
Restringir o acesso de leitura de desenvolvedores delegados [Atualizado na Central de segurança 1.3]	• Nova descrição resumida: Restringir o acesso de leitura de desenvolvedores delegados • Descrição resumida antiga: Lista de permissões de acesso de leitura para desenvolvedores delegados
Ativar pontuação e filtragem de spam de e-mail [Atualizado na Central de segurança 1.3]	• Nova descrição resumida: Habilitar pontuação e filtragem de spam de e-mail • Descrição resumida antiga: Pontuação e filtragem de spam de e-mail
Plug-in Alta segurança [Atualizado na Central de segurança 1.3]	• Nova descrição resumida: Habilitar plug-in de alta segurança • Descrição resumida antiga: Plug-in de alta segurança
Ativar o plug-in de segurança contextual [Atualizado na Central de segurança 1.3]de	• Nova descrição resumida: Habilitar plug-in de segurança contextual • Descrição resumida antiga: Plug-in de segurança contextual
Impor a limpeza de HTML [Atualizado na Central de segurança 1.3]	• Nova descrição resumida: Aplicar limpeza de HTML • Descrição resumida antiga: Verificar HTML não limpo
Definição de usuário convidado para solicitações SOAP [Atualizado na Central de segurança 1.3]	• Nova descrição resumida: Definir usuário convidado para solicitações SOAP • Descrição resumida antiga: Usuário convidado para solicitações SOAP
Como ativar o plug-in Controle de acesso de SNC [Atualizado na Central de segurança 1.3]	• Nova descrição resumida: Habilitar plug-in de controle de acesso do SNC • Descrição resumida antiga: Plug-in de controle de acesso do SNC
Habilitar o plug-in Security Jump Start (regras de ACL) [Atualizado na Central de segurança 1.3]	• Nova descrição resumida: Habilitar plug-in de início rápido de segurança • Descrição resumida antiga: Habilitar plug-in de início rápido de segurança (Regras ACL)

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Documentação	Atualizações
Desabilitar o comportamento do AngularJS legado [Atualizado na Central de segurança 1.3]	• Nova descrição resumida: Desativar comportamento do AngularJS legado • Descrição resumida antiga: Comportamento do AngularJS legado
Como limitar as sessões interativas simultâneas [Atualizado na Central de segurança 1.3]	• Nova descrição resumida: Limitar sessões interativas simultâneas • Descrição resumida antiga: Limite de sessões interativas simultâneas para autenticação do Glide
Limitar sessões simultâneas em todos os nós [Atualizado na Central de segurança 1.3]	• Nova descrição resumida: Limitar sessões simultâneas em todos os nós • Descrição resumida antiga: Limite de sessões simultâneas para autenticação do Glide em todos os nós
Minimizar a quantidade de sessões interativas simultâneas [Atualizado na Central de segurança 1.3]	• Nova descrição resumida: Minimizar a quantidade de sessões interativas simultâneas • Descrição resumida antiga: Sessões interativas simultâneas máximas para autenticação do Glide
Ativar a autenticação multifator baseada em função [Atualizado na Central de segurança 1.3]	• Nova descrição resumida: Ativar autenticação multifator com base na função • Descrição resumida antiga: Autenticação multifator com base na função
Como ativar a versão atualizada do plug-in Multi-SSO [Atualizado na Central de segurança 1.3 e 1.5]	• Nova descrição resumida: Ativar a versão atualizada do plug-in MultiSSO • Descrição resumida antiga: Versão atualizada do plug-in MultiSSO está ativada
Como minimizar a duração da restrição "notBefore" ou "notOnOrAfter" de SAML [Atualizado na Central de segurança 1.3 e 1.5]	• Nova descrição resumida: Minimizar a duração da restrição "notBefore" ou "notOnOrAfter" de SAML • Descrição resumida antiga: Restrição SAML "notBefore" ou "notOnOrAfter"

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Documentação	Atualizações
Exigir autorização para solicitações de API [Atualizado na Central de segurança 1.3]	• Nova descrição resumida: Exigir autorização para solicitações de API • Descrição resumida antiga: Autorização de solicitação de API
Exigir autorização para solicitações de CSV [Atualizado na Central de segurança 1.3]	• Nova descrição resumida: Exigir autorização para solicitações CSV • Descrição resumida antiga: Autorização de solicitação de CSV
Exigir autorização da REST API do agente de dados [Atualizado na Central de segurança 1.3]	• Nova descrição resumida: Exigir autorização para REST API do Data Broker • Descrição resumida antiga: Autorização da REST API do Data Broker
Exigir autorização para solicitações do Excel [Atualizado na Central de segurança 1.3]	• Nova descrição resumida: Exigir autorização para solicitações do Excel • Descrição resumida antiga: Autorização de solicitação do Excel
Exigir autorização para solicitações de importação [Atualizado na Central de segurança 1.3]	• Nova descrição resumida: Exigir autorização para solicitações de importação • Descrição resumida antiga: Autorização de solicitação de importação
Exigir autorização para solicitações JSONv2 [Atualizado na Central de segurança 1.3]	• Nova descrição resumida: Exigir autorização para solicitação JSONv2 • Descrição resumida antiga: Autorização de solicitação JSONv2
Exigência de autorização para solicitações de pdf [Atualizado na Central de segurança 1.3]	• Nova descrição resumida: Exigir autorização para solicitações de PDF • Descrição resumida antiga: Autorização de solicitação de PDF
Exigir autorização para solicitações de RSS [Atualizado na Central de segurança 1.3]	• Nova descrição resumida: Exigir autorização para solicitações de RSS • Descrição resumida antiga: Autorização de solicitação de RSS

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Documentação	Atualizações
Exigir autorização para solicitações SCHEMA [Atualizado na Central de segurança 1.3]	• Nova descrição resumida: Exigir autorização para solicitações SCHEMA • Descrição resumida antiga: Autorização de solicitação SCHEMA
Exigência de autorização para solicitações SOAP [Atualizado na Central de segurança 1.3 e 1.5]	• Nova descrição resumida: Exigir autorização para solicitações SOAP • Descrição resumida antiga: Autorização de solicitação SOAP
Autorização de solicitação de descarregamento	• Nova descrição resumida: Exigir autorização para solicitações de descarregamento • Descrição resumida antiga: Autorização de solicitação de descarregamento
Exigir autorização para solicitações de WSDL [Atualizado na Central de segurança 1.3]	• Nova descrição resumida: Exigir autorização para solicitação WSDL • Descrição resumida antiga: Autorização de solicitação de WSDL
Exigência de autorização para solicitações XML [Atualizado na Central de segurança 1.3]	• Nova descrição resumida: Exigir autorização para solicitações de XML • Descrição resumida antiga: Autorização de solicitação de XML
Exigir autorizações para solicitações de saída de XML	• Nova descrição resumida: Exigir autorização para solicitações de saída de XML • Descrição resumida antiga: Autorização de saída de XML
Ativar sinalizador de cookie somente HTTP [Atualizado na Central de segurança 1.3]	• Nova descrição resumida: Habilitar sinalizador de cookie somente HTTP • Descrição resumida antiga: Sinalizador de cookie somente HTTP
Como desabilitar a execução de consultas brutas no banco de dados [Atualizado na Central de segurança 1.3]	• Nova descrição resumida: Desabilitar execução de consulta ao banco de dados brutos • Descrição resumida antiga: Requisitos de controle de acesso em nível de operação

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Documentação	Atualizações
Desativação de mensagens de erro de SQL [Atualizado na Central de segurança 1.3]	• Nova descrição resumida: Desabilitar mensagens de erro SQL • Descrição resumida antiga: Desabilitando mensagens de erro SQL
Como converter imagens de e-mails recebidos em anexos [Atualizado na Central de segurança 1.3 e removido na 1.5]	• Nova descrição resumida: Converter imagens de e-mails de entrada em anexos • Descrição resumida antiga: Converter HTML de e-mail de entrada
Como reduzir a quantidade de destinatários SMTP [Atualizado na Central de segurança 1.3]	• Nova descrição resumida: Minimizar a quantidade de destinatários SMTP • Descrição resumida antiga: Máximo de destinatários SMTP
Escapar fórmulas do Excel [Atualizado na Central de segurança 1.3]	• Nova descrição resumida: Escapar fórmulas do Excel • Descrição resumida antiga: Escapar fórmula do Excel
Como habilitar o Sanitizer de HTML [Atualizado na Central de segurança 1.3]	• Nova descrição resumida: Habilitar limpeza de HTML • Descrição resumida antiga: Limpeza de HTML
Valor do cabeçalho HTTP de controle de cache [Atualizado na Central de segurança 1.3]	• Nova descrição resumida: Valor do cabeçalho HTTP de controle de cache • Descrição resumida antiga: Valor do cabeçalho HTTP de controle de cache
Como impor o comportamento da instância de produção [Atualizado na Central de segurança 1.3 e 1.5]	• Nova descrição resumida: Aplicar comportamento da instância de produção • Descrição resumida antiga: Comportamento da instância de produção

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Documentação	Atualizações
Como definir endereços IP internos permitidos da ServiceNow [Atualizado na Central de segurança 1.3 e 1.5]	• Nova descrição resumida: Definir endereços IP internos da ServiceNow permitidos • Descrição resumida antiga: Lista de permissões de acesso a endereços IP
Desativação do comportamento legado de JQuery [Atualizado na Central de segurança 1.3]	• Nova descrição resumida: Desabilitar comportamento de JQuery legado • Descrição resumida antiga: Comportamento do JQuery legado
Nome distinto inicial do LDAP não definido [Atualizado na Central de segurança 1.3]	• Nova descrição resumida: Cancelar definição do nome diferenciado inicial do LDAP • Descrição resumida antiga: Nome diferenciado inicial do LDAP
Restrição do acesso a entradas personalizadas de registros [Atualizado na Central de segurança 1.3]	• Nova descrição resumida: Restringir o acesso a entradas de registro personalizadas • Descrição resumida antiga: Entradas de registro personalizadas seguras
Minimizar o tempo de vida do verificador único fora de banda [Atualizado na Central de segurança 1.3]	• Nova descrição resumida: Minimizar a duração do tempo de vida do verificador único fora de banda • Descrição resumida antiga: Tempo de vida curto do verificador único fora de banda
Desativação de conexões SSLv2/SSLv3 de saída [Atualizado na Central de segurança 1.3]	• Nova descrição resumida: Desabilitar conexões SSLv2/SSLv3 de saída • Descrição resumida antiga: Desabilitar SSLv2/SSLv3
Como desabilitar a criação de usuários a partir de e-mails recebidos [Atualizado na Central de segurança 1.3]	• Nova descrição resumida: Desabilitar a criação de usuários a partir de e-mails de entrada • Descrição resumida antiga: Restringir e-mails por domínio

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Documentação	Atualizações
Restringir o acesso à API com script GlideSystemUserSession [Atualizado na Central de segurança 1.3]	• Nova descrição resumida: Exigir autenticação por padrão para inclusões de script de cliente chamável • Descrição resumida antiga: Privacidade em inclusões de script de cliente chamável
Exigir autenticação por padrão para inclusões de script de cliente chamável [Atualizado na Central de segurança 1.3]	• Nova descrição resumida: Exigir autenticação por padrão para inclusões de script de cliente chamável • Descrição resumida antiga: Privacidade em inclusões de script de cliente chamável
Exigir a verificação de ACL de AJAXGlideRecord [Atualizado na Central de segurança 1.3]	• Nova descrição resumida: Exigir a verificação de ACL AJAXGlideRecord • Descrição resumida antiga: Habilitar a verificação de ACL AJAXGlideRecord
Como impor a área restrita de scripts gerados pelo cliente [Atualizado na Central de segurança 1.3]	• Nova descrição resumida: Aplicar a área restrita de scripts gerados pelo cliente • Descrição resumida antiga: Sandbox de scripts gerados pelo cliente
Restrição de tipos MIME carregados [Atualizado na Central de segurança 1.3]	• Nova descrição resumida: Restringir tipos de MIME carregados* Descrição resumida • Descrição resumida antiga: Carregar restrição de tipo MIME, VALOR PADRÃO ALTERADO DE VERDADEIRO PARA FALSO
Como habilitar ACLs da aplicação de administrador com escopo [Atualizado na Central de segurança 1.3]	• Nova descrição resumida: Ativar ACLs da aplicação de administrador com escopo • Descrição resumida antiga: Administrar ACLs da aplicação de administrador com escopo
Como habilitar o token anti-CSRF [Novo na Central de segurança 1.3 e removido na 1.5]	• Nova descrição resumida: Habilitar token anti-CSRF • Descrição resumida antiga: Token anti-CSRF

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Documentação	Atualizações
Implementação do cabeçalho de segurança x-frame-options: SAMEORIGIN [Atualizado na Central de segurança 1.3]	• Nova descrição resumida: Implementar o cabeçalho de segurança X-Frame-Options: SAMEORIGIN • Descrição resumida antiga: X-Frame-Options: SAMEORIGIN
Exigir desfoque da IU do aplicativo para celular [Atualizado na Central de segurança 1.3]	• Nova descrição resumida: Exigir ofuscação da IU do aplicativo para celular • Descrição resumida antiga: Ofuscação da IU do aplicativo para celular
Como negar por padrão com ACLs vazias [Atualizado na Central de segurança 1.3]	• Nova descrição resumida: Negar por padrão com ACLs vazias • Descrição resumida antiga: Negação padrão do gerenciador de segurança
Validação do tipo de conteúdo SOAP [Atualizado na Central de segurança 1.3]	• Nova descrição resumida: Validar tipo de conteúdo SOAP • Descrição resumida antiga: Verificação de tipo de conteúdo SOAP
Como impor a segurança estrita de solicitações SOAP [Atualizado na Central de segurança 1.3]	• Nova descrição resumida: Aplicar segurança estrita para solicitação SOAP • Descrição resumida antiga: Segurança estrita para solicitação SOAP
Como habilitar a recuperação de conta [Atualizado na Central de segurança 1.3 e 1.5]	• Nova descrição resumida: Habilitar recuperação de conta • Descrição resumida antiga: Recuperação de conta
Exigência de validação da entidade XMLdoc2 com expansão da entidade allowlistDisable [Atualizado na Central de segurança 1.3]	• Nova descrição resumida: Exigir validação de entidade XMLdoc2 com expansão de entidade allowlistDisable • Descrição resumida antiga: Validação de entidade XMLdoc2 com expansão de entidade allowlistDisable

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Documentação	Atualizações
Como aplicar a separação de domínios em campos de referência com pontos [Atualizado na Central de segurança 1.3 e 1.5]	• Nova descrição resumida: Aplicar separação de domínios em campos de referência com pontos • Descrição resumida antiga: Aplicar separação de domínios
Como definir tipos MIME para download restritos [Atualizado na Central de segurança 1.3]	• Nova descrição resumida: Restringir tipos MIME para download • Descrição resumida antiga: Lista de proibição de tipos de MIME para download
Tipos MIME para download	• Nova descrição resumida: Definir tipos MIME restritos para download • Descrição resumida antiga: Tipos MIME para download
Como fazer escape de scripts Jelly [Atualizado na Central de segurança 1.3]	• Nova descrição resumida: Escapar script Jelly • Descrição resumida antiga: Escapar Jelly
Como fazer escapes de HTML em exibições de lista [Atualizado na Central de segurança 1.3]	• Nova descrição resumida: Escapar HTML nas Exibições da lista • Descrição resumida antiga: Escapar HTML
Scripts de escape no bloco de anotações [Atualizado na Central de segurança 1.3]	• Nova descrição resumida: Escapar scripts no bloco de anotações • Descrição resumida antiga: Escapar no bloco de anotações
Como fazer escapes de marcação XML [Atualizado na Central de segurança 1.3]	• Nova descrição resumida: Escapar marcação XML • Descrição resumida antiga: Escapar XML
Como exigir a ofuscação da IU clássica do aplicativo para celular [Atualizado na Central de segurança 1.3]	• Nova descrição resumida: Exigir ofuscação da IU do aplicativo para celular clássico • Descrição resumida antiga: Ofuscação da IU do aplicativo para celular clássico

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Documentação	Atualizações
Desativação do acesso público aos favoritos	• Nova descrição resumida: Desativar o acesso público aos favoritos • Descrição resumida antiga: Acesso público aos favoritos
Como impor a segurança estrita de cookies de sessão [Atualizado na Central de segurança 1.3]	• Nova descrição resumida: Aplicar segurança estrita de cookies de sessão • Descrição resumida antiga: Cookies de sessão segura
Como desabilitar o código HTML integrado [Atualizado na Central de segurança 1.3]	• Nova descrição resumida: Desabilitar código HTML integrado • Descrição resumida antiga: Código HTML integrado
Desabilitar marcadores JavaScript no HTML incorporado [Atualizado na Central de segurança 1.3]	• Nova descrição resumida: Desativar tags JavaScript em HTML integrado • Descrição resumida antiga: Permitir tags Javascript em HTML integrado
Como minimizar a duração do tempo limite da atividade da sessão [Atualizado na Central de segurança 1.3]	• Nova descrição antiga: Minimizar a duração do tempo limite da atividade da sessão • Descrição resumida antiga: Tempo limite de atividade da sessão
Como restringir tipos de arquivos para download em conteúdo estático [Atualizado na Central de segurança 1.3]	• Nova descrição antiga: Restringir tipos de arquivos para download em conteúdo estático • Descrição resumida antiga: Restrições de download de tipos de arquivos de conteúdo estático
Como minimizar a duração do tempo limite da janela da sessão [Atualizado na Central de segurança 1.3]	• Nova descrição antiga: Minimizar a duração do tempo limite da janela da sessão • Descrição resumida antiga: Tempo limite da janela da sessão

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Documentação	Atualizações
Como minimizar a duração do tempo limite absoluto da sessão [Atualizado na Central de segurança 1.3]	• Nova descrição antiga: Minimizar a duração do tempo limite absoluto da sessão • Descrição resumida antiga: Tempo limite absoluto da sessão
Como maximizar a duração do tempo limite de desbloqueio para logins com falha [Atualizado na Central de segurança 1.3]	• Nova descrição resumida: Maximizar a duração do tempo limite de desbloqueio de login com falha • Descrição resumida antiga: Gerenciar o tempo limite de desbloqueio após login com falha
Restrição de entidades externas XML [Atualizado na Central de segurança 1.3]	• Nova descrição resumida: Restringir entidades externas de XML • Descrição resumida antiga: Lista de permissão de URL de validação de entidade XML
Como minimizar o limite de expansão da entidade [Atualizado na Central de segurança 1.3]	• Nova descrição resumida: Minimizar o limite de expansão da entidade • Descrição resumida antiga: Definindo limite de expansão da entidade
Como minimizar a duração da expiração da solicitação de redefinição de senha [Atualizado na Central de segurança 1.3]	• Nova descrição resumida: Minimizar a duração da expiração da solicitação de redefinição de senha • Descrição resumida antiga: Expiração da solicitação de redefinição de senha
Como minimizar a provisão de máximo de tentativas de solicitação de redefinição de senha [Atualizado na Central de segurança 1.3]	• Nova descrição resumida: Minimizar permissão de tentativas máximas de solicitação de redefinição de senha • Descrição resumida antiga: Tentativas máximas de solicitação de redefinição de senha
Como minimizar a duração da janela de máximo de tentativas de solicitação de redefinição de senha [Atualizado na Central de segurança 1.3]	• Nova descrição resumida: Minimizar a duração da janela de tentativas máximas de solicitação de redefinição de senha • Descrição resumida antiga: Janela de tentativas máximas de solicitação de redefinição de senha

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Documentação	Atualizações
Como maximizar a duração da janela de nova tentativa de solicitação de redefinição de senha [Atualizado na Central de segurança 1.3]	• Nova descrição resumida: Maximizar a duração da janela de nova tentativa de solicitação de redefinição de senha • Descrição resumida antiga: Janela de nova tentativa de solicitação de redefinição de senha
Como minimizar a duração da janela de sucesso na solicitação de redefinição de senha [Atualizado na Central de segurança 1.3]	• Nova descrição resumida: Minimizar a duração da janela de sucesso de solicitação de redefinição de senha • Descrição resumida antiga: Janela de sucesso de solicitação de redefinição de senha
Como maximizar a duração da janela de desbloqueio da solicitação de redefinição de senha [Atualizado na Central de segurança 1.3]	• Nova descrição resumida: Maximizar a duração da janela de desbloqueio de solicitação de redefinição de senha • Descrição resumida antiga: Janela de desbloqueio de solicitação de redefinição de senha
Maximizar a complexidade do SMS de redefinição de senha [Atualizado na Central de segurança 1.3]	• Nova descrição resumida: Maximizar a complexidade do SMS de redefinição de senha • Descrição resumida antiga: Complexidade do SMS de redefinição de senha
Como minimizar a duração da expiração do SMS de redefinição de senha [Atualizado na Central de segurança 1.3]	• Nova descrição resumida: Minimizar a duração da expiração do SMS de redefinição de senha • Descrição resumida antiga: Expiração do SMS de redefinição de senha
Como minimizar o máximo de SMS de redefinição de senha por dia [Atualizado na Central de segurança 1.3]	• Nova descrição resumida: Minimizar número máximo de SMS de redefinição de senha por dia • Descrição resumida antiga: Número máximo de SMS de redefinição de senha por dia

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Documentação	Atualizações
Como maximizar a duração da janela de pausa de SMS de redefinição de senha [Atualizado na Central de segurança 1.3]	• Nova descrição resumida: Maximizar a duração da janela de pausa de SMS de redefinição de senha • Descrição resumida antiga: Janela de pausa de SMS de redefinição de senha
Como ativar as notificações de código por SMS para inscrições e verificações [Atualizado na Central de segurança 1.3]	• Nova descrição resumida: Ativar notificação de código por SMS para inscrição e verificação • Descrição resumida antiga: Notificação de código por SMS para inscrição e verificação
Como maximizar a duração do atraso de verificação da redefinição de senha [Atualizado na Central de segurança 1.3]	• Nova descrição resumida: Maximizar a duração do atraso na verificação da redefinição de senha • Descrição resumida antiga: Atraso na verificação da redefinição de senha
Notificar usuários durante o processo de redefinição/mudança de senha	• Nova descrição resumida: Notificar usuários durante o processo de redefinição/mudança de senha • Descrição resumida antiga: Processo de notificação de redefinição/mudança de senha
Restrição de domínios de e-mail para registro de usuários externos [Atualizado na Central de segurança 1.5]	• Nova descrição resumida: Restringir domínios de e-mail para registro de usuário externo • Descrição resumida antiga: Lista de permissões de domínio de e-mail para registro de usuário externo
Como minimizar a duração da expiração do link de registro de usuário externo [Atualizado na Central de segurança 1.3 e 1.5]	• Nova descrição resumida: Minimizar a duração da expiração do link de registro de usuário externo • Descrição resumida antiga: Expiração do link de registro de usuário externo
Restrição de pacotes Java permitidos [Atualizado na Central de segurança 1.3]	• Nova descrição resumida: Restringir pacotes Java permitidos • Descrição resumida antiga: Lista de permissões de pacotes Java

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configurações de proteção excluídas da linha de base versão 4.0

Esta lista contém as configurações de proteção que foram removidas na linha de base versão 4.0 da Security Center.

- Impor restrições de escopo da aplicação
- Notificar usuários durante o processo de redefinição/mudança de senha
- Valor do cabeçalho HTTP de controle de cache
- Converter imagens de e-mails de entrada em anexos
- Ativar token anti-CSRF
- Aplicar a confiança do certificado
- Definir opções de tipo de conteúdo automaticamente

Configurações de proteção excluídas da linha de base versão 2.0

Esta lista contém as configurações de proteção que foram removidas na versão de linha de base Security Center 2.0.

- Habilitar assinatura de código para scripts e dados de configuração de aplicação
- Habilitar criptografador de KMF do Glide
- Desabilitar o uso do criptografador no nível da instância
- Registrar todos os campos de solicitação HTTP de saída

Controle de acesso

A categoria de controle de acesso audita o processo de proteção de recursos contra acesso não autorizado por meio de solicitações de concessão e negação com base em um modelo de permissão. Isso inclui garantir que uma entidade que acesse um recurso tenha credenciais válidas para isso, criando e protegendo um conjunto bem definido de funções ou permissões e garantindo que os controles de função ou permissão sejam protegidos contra reprodução e adulteração.

Os controles de acesso determinam se o acesso a um recurso específico deve ser concedido ou negado. Eles só permitem o acesso aos recursos aos usuários com permissão para usá-los.

Tempo de validação do token anti-CSRF [Novo na Central de segurança 1.3]

A propriedade *glide.security.csrf_previous.time_limit* especifica o tempo, em segundos, para um token de segurança expirar.

Quando a sessão do usuário expira, o token de segurança expira com ela, a menos que a propriedade **reutilização permitida de tokens expirados** esteja habilitada e esteja dentro do intervalo de tempo descrito por esta propriedade. Esse token é usado para impedir ataques de falsificação de solicitação entre sites.

Mais informações

Atributo	Descrição
Nome da configuração	*glide.security.csrf_previous.time_limit*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Tipo de dados	inteiro
Valor recomendado	86.400 segundos ou 1 dia
Valor padrão	86.400 segundos ou 1 dia
Categoria	Controle de acesso
Risco à segurança	• Pontuação de gravidade: 5,3 • Pontuação do CVSS: média • Detalhes do risco à segurança: não definir esta propriedade com o valor recomendado desabilita a validação de token usada para impedir ataques de falsificação de solicitação entre sites.
Dependências e pré-requisitos	Nenhum(a)
Impacto funcional	Esta propriedade determina a duração, em segundos, da validade de um token de segurança. O token de segurança e a sessão do usuário expiram juntos, a menos que a propriedade **reutilização permitida de tokens expirados** esteja habilitada e o token esteja dentro do intervalo de tempo descrito por esta propriedade. Este token evita ataques de falsificação de solicitação entre sites. Tem um valor padrão de 86.400 segundos ou 1 dia.

Como aplicar a separação de domínios em campos de referência com pontos [Atualizado na Central de segurança 1.3 e 1.5]

A propriedade *glide.sys.domain.include_domain_condition_on_join* controla se as consultas de junção recebem condições separadas por domínio ou não para garantir que elas apliquem a funcionalidade do Domain Separation para campos de referência com pontos.

Esta propriedade *glide.sys.domain.include_domain_condition_on_join* controla se as consultas de junção recebem condições separadas por domínio ou não, para garantir que elas apliquem a funcionalidade de separação de domínios para campos de referência com pontos. Se *glide.sys.domain.include_domain_condition_on_join* não estiver definido com o valor recomendado de verdadeiro em uma instância usando separação de domínios, poderão ser divulgadas informações confidenciais que não devem ser compartilhadas com um domínio específico.

Nota: Quando o plug-in Domain Separation é instalado, um registro sys_properties para essa propriedade é instalado com seu valor definido como **verdadeiro**, que é o valor não padrão. Caso contrário, no sistema de base sem a separação de domínios instalada, o registro de propriedade não existirá e terá seu valor não padrão.

Aviso: Esta é uma propriedade tipo porto seguro, o que significa que o valor não pode ser alterado após ser mudado. A reversão não é possível.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mais informações

Atributo	Descrição
Nome da propriedade	*glide.sys.domain.include_domain_condition_on_join*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	booliano
Valor recomendado	Verdadeiro, quando o Domain Separation estiver instalado, caso contrário, a propriedade não existirá.
Valor padrão	falso
Categoria	Controle de acesso
Finalidade	Controla se as consultas de junção recebem condições separadas por domínio ou não para garantir que elas apliquem a funcionalidade do Domain Separation para campos de referência com pontos.
Risco à segurança	• Pontuação de gravidade: 6,5 • Pontuação do CVSS: média • Detalhes do risco à segurança: se *glide.sys.domain.include_domain_condition_on_join* não estiver definida com o valor recomendado **verdadeiro**, as informações confidenciais, que não devem ser compartilhadas com um domínio específico, poderão ser divulgadas.
Referências	Domain Separation para provedores de serviço

Como habilitar ACLs da aplicação de administrador com escopo [Atualizado na Central de segurança 1.3]

O *glide.security.scoped_administration.honor_global_acl* determina se um app de administração de aplicações pode herdar regras de ACL (access control list, lista de controle de acesso) global.

Esta propriedade é especialmente útil quando não há ACLs de aplicação de administrador com escopo definidas para o escopo do registro.

Defina *glide.security.scoped_administration.honor_global_acl* como verdadeiro para impedir que um usuário com poucos privilégios e com permissões para a aplicação acesse registros confidenciais.

Mais informações

Atributo	Descrição
Nome da propriedade	*glide.security.scoped_administration.honor_global_acl*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Categoria	Controle de acesso

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Finalidade	Controla a regra de acesso da ACL na aplicação de administração com escopo.
Valor recomendado	Verdadeiro
Valor padrão	Verdadeiro
Tipo de configuração	Booliano
Risco à segurança	(Baixo) Quando o valor da propriedade for verdadeiro e não houver ACLs de aplicação de administrador com escopo definidas para o escopo do registro, as ACLs globais serão respeitadas. Se a propriedade for definida como falsa, sem ACLs de aplicação de administrador com escopo definidas para o escopo do registro, as verificações de ACL serão ignoradas.
Classificação de risco de segurança	3,8
Referências	Regras de controle de acesso em aplicações de administração de aplicações

Para saber mais sobre como ativar um plug-in, consulte Ativar um plug-in

Habilitar regras de consulta de gestão de pedidos de serviço para organizações de serviço [Novo na Central de segurança 1.5]

Use a propriedade *sn_fsm.use_query_rules* para aplicar regras e filtros às tabelas de Gestão de serviços de campo.

Quando a propriedade *sn_fsm.use_query_rules* for definida como verdadeira, as regras e os filtros da tabela sn_query_rule serão usados para determinar o acesso de leitura às tabelas de Gestão de serviços de campo de usuários autenticados. Isso é feito por regras de negócio de consulta e ACLs de leitura. Quando essa propriedade for definida como falsa, os registros não serão filtrados com base nas regras de consulta. As regras de negócio de consulta adicionam outras validações de segurança quando habilitadas nessa propriedade e filtram registros para agentes, qualificadores e expedidores com base no território atribuído ou na associação de territórios. Isso implementa o princípio do menor privilégio na leitura de registros.

Mais informações

Atributo	Descrição
Nome da configuração	*sn_fsm.use_query_rules*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	booliano
Valor recomendado	falso
Valor-padrão	falso
Categoria	Controle de acesso

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Risco à segurança	• Pontuação de gravidade: 4,3 • Pontuação do CVSS: média • Detalhes de risco à segurança: quando essa propriedade for definida como verdadeira, as regras e os filtros da tabela sn_query_rule serão usados para determinar o acesso de leitura às tabelas de Gestão de serviços de campo com implementação do princípio de menor privilégio. Quando definida como falsa, os registros não serão filtrados com base nas regras de negócio de consulta e podem ter um risco maior de exposição de dados pelas tabelas de Gestão de serviços de campo.
Dependências e pré-requisitos	Nenhum(a)
Impacto funcional	Quando for definida como verdadeira, as regras e os filtros da tabela sn_query_rule serão usados para determinar o acesso de leitura às tabelas relacionadas de Gestão de serviços de campo. Por exemplo, ordem de serviço (WO) e tabela de ordem de serviço (WOT) para o usuário conectado por regras de negócio de consulta e ACLs de leitura. Quando for definida como falsa, os registros não serão filtrados com base nas regras de consulta. Habilitar essa propriedade protege os dados, e nenhum dado (wm_task e wm_order) ficará visível para os usuários.
Referências	Referência da Gestão de serviços de campo

Bloqueio de acesso aos desenvolvedores delegados

Esta configuração afeta o acesso de desenvolvedores delegados que estão atualizando funções de usuário por meio de script. Quando a configuração está em conformidade, o desenvolvedor não poderá atualizar ou inserir registros na tabela sys_user_has_role sem também ter a função user_admin.

O valor desta propriedade afeta se um desenvolvedor delegado tem permissão para conceder ou receber acesso inesperado à funcionalidade na instância. Quando a propriedade contém funções, somente essas funções podem executar módulos de script.

Mais informações

Atributo	Descrição
Nome da propriedade	*com.glide.sys.security.delegateddev.block_grant_roles*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Categoria	Controle de acesso

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Finalidade	O valor desta propriedade afeta se um desenvolvedor delegado tem permissão para conceder ou receber acesso inesperado à funcionalidade na instância.
Tipo	comutador de alternância
Valor-padrão	verdadeiro
Valor recomendado	verdadeiro
Dependências de segurança	nenhum
Classificação de risco de segurança	6,7
Impacto funcional	(Alto) Quando um usuário com a função delegated_developer tenta modificar um registro na tabela sys_user_has_role, esta propriedade habilita verificações de segurança adicionais em relação à operação. As verificações de segurança adicionais validam que o usuário recebeu a função user_admin se ele tentar criar ou atualizar a tabela sys_user_has_role. Se ele não tiver a função user_admin, o acesso será negado. Quando a propriedade é falsa, essas verificações adicionais não são validadas.
Risco à segurança	(Moderado) Sem a autorização apropriada, usuários não autorizados podem acessar conteúdo/dados confidenciais na instância.
Referências	Controle de Acesso

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Bloqueio de tokens anti-CSRF expirados [Atualizado na Central de segurança 1.5]

Bloqueie tokens CSRF expirados para impedir ataques de falsificação de solicitação entre sites.

Visão geral

As falsificações de solicitação entre sites são um tipo de exploração mal-intencionada em que comandos não autorizados são executados em nome de um usuário autenticado.

Detalhes da configuração

Atributo	Descrição
Visão geral	Controla o uso de um token de segurança expirado para identificar e validar solicitações de entrada. Defina como **falso** para impedir que um token expirado anteriormente valide uma solicitação de entrada.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Nome da configuração	*glide.security.csrf_previous.allow*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	booliano
Valor recomendado	**falso**
Valor padrão	**verdadeiro**
Categoria	Controle de acesso
Risco à segurança	**Pontuação de gravidade**: 6,5
	Classificação de gravidade por pontuação do CVSS: média
	Detalhes do risco à segurança: impõe um forte mecanismo anti-CSRF para proteger a funcionalidade autenticada, e o mecanismo eficaz antiautomação ou anti-CSRF protege a funcionalidade não autenticada.
Dependências e pré-requisitos	Nenhum
Referências	Como habilitar o token anti-CSRF [Novo na Central de segurança 1.3 e removido na 1.5], falsificação de solicitação entre sites .

Verifique as condições da ação de IU antes da execução

Use a propriedade *glide.security.strict.actions* para habilitar a verificação das condições de ações de IU em formulários e listas antes de serem executados. Quando você define esta propriedade como verdadeira, ela adiciona uma camada extra de validação nas ações de IU da tabela antes que elas sejam executadas.

Mais informações

Atributo	Descrição
Nome da propriedade	*glide.security.strict.actions*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Categoria	Controle de acesso
Finalidade	Definir uma camada extra de validação nas ações de IU da tabela antes que elas sejam executadas.
Tipo de dados	booliano
Valor recomendado	verdadeiro
Valor-padrão	verdadeiro
Classificação de risco de segurança	3,3
Impacto funcional	(Baixo) Esta correção adiciona apenas uma camada extra de validação para verificar se há ações de IU na tabela/página de destino na instância.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
	Contanto que os controles de acesso sejam definidos corretamente na instância do cliente, não deve haver um impacto aqui.
Risco à segurança	(Baixo) A solicitação de acesso é sempre verificada quando ocorrem transações entre duas zonas. Esta operação valida qualquer ação de IU antes que o formulário seja renderizado para o usuário final.
Referências	Plug-in High Security

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Configurar funções de administrador de grupo de atribuição de gestão de eventos [Novo na Central de segurança 1.5]

Use a propriedade *evt_mgmt.connector_assignment_group_admin_roles* para definir quais funções estão autorizadas para acesso de administrador no campo do grupo de atribuição nas instâncias do conector.

A propriedade *evt_mgmt.connector_assignment_group_admin_roles* contém uma cadeia de caracteres separada por vírgulas que indica os nomes de funções que têm acesso de administrador ao campo de grupo de atribuição nas instâncias do conector. Mudar as funções padrão dessa lista pode permitir que usuários não autorizados alterem integrações de eventos na instância. Para impedir o acesso não autorizado às funções, defina *evt_mgmt.connector_assignment_group_admin_roles* com o valor de administrador, evt_mgmt_admin, sn_sow_srm.srm_admin. Revise todas as funções adicionais na cadeia de caracteres de valor recomendada para garantir que a função seja incluída.

Mais informações

Atributo	Descrição
Nome da configuração	*evt_mgmt.connector_assignment_group_admin_roles*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	cadeia de caracteres
Valor recomendado	admin, evt_mgmt_admin, sn_sow_srm.srm_admin
Valor padrão	admin, evt_mgmt_admin, sn_sow_srm.srm_admin
Categoria	Controle de acesso
Risco à segurança	• Pontuação de gravidade: 3,1 • Pontuação de CVSS: baixa • Detalhes do risco à segurança: mudar as funções padrão pode permitir que usuários não autorizados alterem integrações de eventos na instância.
Dependências e pré-requisitos	Nenhum
Referências	Criando grupos

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Negação de acesso interno a funções externas explícitas [Atualizado na Central de segurança 1.5]

Várias propriedades juntas compõem a configuração para a configuração de proteção **habilitar lista de proibições internas de funções explícitas**. A propriedade *glide.security.explicit_roles.enable_internal_user_blacklist* evita que usuários externos sejam atribuídos à função snc_internal e permite que a propriedade *glide.security.explicit_roles.internal_user_blacklist* atribua a função snc_external.

Glide.security.explicit_roles.enable_internal_user_blacklist

Você pode conceder acesso à sua instância a usuários internos e externos. Para fornecer segurança adicional, cada usuário deve ter pelo menos uma função para que a instância possa distinguir entre usuários internos e externos.

Defina a propriedade *glide.security.explicit_roles.enable_internal_user_blacklist* com o valor recomendado **verdadeiro** para habilitar a capacidade de atribuir a função snc_external.

Defina o valor como **falso** para desabilitar a capacidade de atribuir a função snc_external. Todos os usuários receberão a função snc_internal por padrão

Nota: Instâncias sem funções explícitas instaladas não são afetadas. A partir da versão Paris, novas instalações de funções explícitas obtêm a propriedade com um valor padrão de verdadeiro.

Mais informações

Atributo	Descrição
Nome da propriedade	*glide.security.explicit_roles.enable_internal_user_black*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Categoria	Controle de acesso
Finalidade	Permitir a atribuição de classes de usuário especificadas para a função snc_external em vez da função snc_internal.
Valor recomendado	Verdadeiro
Valor padrão	Verdadeiro
Tipo de configuração	Booliano
Risco à segurança	(Moderado) Desabilitar a propriedade pode resultar em atribuição de função padrão inadequada.
Classificação de risco de segurança	5,4
Referências	Funções explícitas em CSM

Glide.security.explicit_roles.internal_user_blacklist

O valor *glide.security.explicit_roles.internal_user_blacklist* determina quais classes de usuário (tabelas que estendem sys_user) devem ser atribuídas à função snc_external em vez da função snc_internal. O valor padrão csm_consumer_user,

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

customer_contact, é definido para se alinhar aos casos de uso nos plug-ins do Customer Service Management.

O valor da propriedade só precisa ser alterado se houver classes de usuário adicionais ou diferentes que precisem ser atribuídas à função snc_external por padrão, em vez da função snc_internal. Entre em contato com o suporte para alterar esses valores.

Atributo	Descrição
Nome da propriedade	*glide.security.explicit_roles.internal_user_blacklist*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Categoria	Controle de acesso
Finalidade	Permite a atribuição da função snc_external atribuída por padrão em vez da função snc_internal.
Valor recomendado	*csm_consumer_user*, *customer_contact*
Tipo de configuração	Cadeia de caracteres
Risco à segurança	(Moderado) Desabilitar a propriedade pode resultar em atribuição de função padrão inadequada.
Classificação de risco de segurança	5,4
Referências	Funções explícitas, Corrigir atribuições de função do usuário externo

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Negar acesso não autorizado para itens da solicitação

A propriedade *glide.sc.req_for.roles.default* define um comportamento padrão para a API *retrieveAddress*.

Esta propriedade é funcional somente quando *glide.sc.req_for.roles* não tem valores. Se *glide.sc.req_for.roles* tiver valores, esta propriedade não terá importância e os usuários com apenas funções definidas terão acesso à API.

Mais informações

Atributo	Descrição
Nome da propriedade	*glide.sc.req_for.roles.default*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Categoria	Controle de acesso
Finalidade	Quando não há funções fornecidas na propriedade, a inclusão de script do cliente chamável *ScriptServiceCatalogGetLocation* pode ser chamada por qualquer usuário logado sem privilégios e pode recuperar o endereço de qualquer outro usuário no sistema. Esta propriedade protege esta API de ser exposta a usuários sem privilégios.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Valor recomendado	negar
Valor padrão	negar
Tipo de configuração	Lista de seleção (permitir | negar)
Risco à segurança	(Moderado) Se *glide.sc.req_for.roles.default* não estiver definido com o valor recomendado de **negar** (permitir) e o valor de *glide.sc.req_for.roles* estiver vazio, qualquer usuário poderá solicitar itens para outros usuários permitindo o acesso a recursos não autorizado.
Referências	Script chamável pelo cliente inclui

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Como habilitar o token anti-CSRF [Novo na Central de segurança 1.3 e removido na 1.5]

Use a propriedade *glide.security.use_csrf_token* para garantir o uso de um token seguro para identificar e validar solicitações de entrada, que por sua vez são usadas para impedir esses ataques.

A CSRF (Cross-Site Request Forgery, falsificação de solicitação de site cruzado) é um ataque que força um usuário final a executar ações indesejadas em uma aplicação da Web na qual ele está autenticado no momento. Os ataques de CSRF visam especificamente solicitações de mudança de estado, e não o roubo de dados, já que o invasor não tem como ver a resposta à solicitação forjada.

As propriedades a seguir podem ser habilitadas para controles adicionais pelo token CSRF:

- *glide.security.csrf_previous.time_limit*
- *glide.security.csrf_previous.allow*
- *glide.security.csrf.strict.validation.mode*

Mais informações

Atributo	Descrição
Nome da propriedade	*glide.security.use_csrf_token*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Categoria	Controle de acesso
Finalidade	Proteger a aplicação de um possível ataque de CSRF.
Classificação de risco de segurança	8,1
Valor recomendado	verdadeiro
Valor-padrão	verdadeiro

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Impacto funcional	(Baixo) Esta correção permite uma etapa de validação extra antes que o usuário da instância envie uma solicitação de gravação para a instância. Cada solicitação de gravação contém um token CSRF (ou seja, um ID de validação/CSRF vinculado à sessão do usuário). Quando a sessão do usuário expira, o token de segurança expira também.
Risco à segurança	(Alto) A falsificação de solicitação de site cruzado é um risco de segurança significativo que viola a integridade dos dados da instância. Um invasor pode iniciar o ataque de CSRF abusando da confiança de um usuário da instância. Com a ajuda de ataques de engenharia social, um usuário pode enviar uma solicitação malformada em nome do invasor na instância.

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Garantir a verificação das ACLs da tabela de arquivamento [Novo na Central de segurança 1.3]

A propriedade *glide.security.enable_archive_table_acls* controla se as ACLs (access control lists, listas de controle de acesso) da tabela original, a tabela a partir da qual a tabela de arquivamento foi criada, são avaliadas como falsas.

A propriedade *glide.security.enable_archive_table_acls* não deve ser definida como falsa, pois as ACLs da tabela original serão avaliadas independentemente do seu valor. O cliente pode evitar ACLs adicionais para uma tabela de arquivamento simplesmente não as adicionando.

Mais informações

Atributo	Descrição
Nome da configuração	*glide.security.enable_archive_table_acls*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	booliano
Valor recomendado	verdadeiro
Valor-padrão	verdadeiro
Categoria	Controle de acesso
Risco à segurança	• Pontuação de gravidade: 3 • Pontuação de CVSS: baixa • Detalhes do risco à segurança: se a propriedade for definida como falsa, as ACLs adicionadas às tabelas arquivadas serão ignoradas, uma ação que é contraintuitiva e, portanto, pode levar ao desvio de autorização.
Dependências e pré-requisitos	Nenhum(a)
Impacto funcional	Quando a propriedade for definida como verdadeira, todas as ACLs de leitura ativas nas tabelas de arquivamento serão respeitadas. Se não

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
	houver ACLs de leitura ativas ou se a propriedade estiver definida como falsa, as ACLs da tabela original (a tabela a partir da qual os dados foram arquivados) serão aplicadas à tabela de arquivamento. **Nota:** Somente ACLs de leitura são permitidas em tabelas de arquivamento. Outras operações em tabelas de arquivamento são regidas internamente por um Manipulador de acesso.

Ativar o plug-in de segurança contextual [Atualizado na Central de segurança 1.3]de

Ativa o plug-in Contextual Security (*com.glide.role_management*) para habilitar a segurança contextual, que protege um registro/informações usando a funcionalidade de criação, leitura, gravação e exclusão.

Depois que ele é instalado e ativado, as funções de dicionário (criadas pelo gerenciador de segurança simples) não são mais testadas. Em vez disso, o Now Platform procura regras de ACL em campos e tabelas. Ele protege os dados com a ajuda de regras de ACL em vez das regras de dicionário tradicionais baseadas em funções implementadas pelo gerenciador de segurança simples. Mesmo se você configurar o formulário de dicionário e adicionar funções a uma entrada de dicionário, não ocorrerá nenhuma mudança nos direitos.

Mais informações

Atributo	Descrição
ID do plug-in	*com.glide.role_management*
Tipo de configuração	Definição do sistema > Plug-ins
Categoria	Controle de acesso
Finalidade	Ao contrário do gerenciador de segurança simples, o gerenciador de segurança contextual está ciente da hierarquia da tabela do sistema. Você pode ter regras de segurança diferentes para um campo com base em onde ele aparece na hierarquia.
Valor recomendado	Ativo
Valor padrão	Não há valor padrão pois esse é um plug-in, não uma propriedade do Glide.
Classificação de risco de segurança	8,1
Impacto funcional	(Médio) Esta correção impõe o nível funcional de controles de acesso, o que permite que a aplicação determine as restrições de acesso com base somente na tabela de ACL.
Risco à segurança	(Alto) Controles de acesso de nível funcional devem ser aplicados do lado do servidor antes da execução das operações CRUD, garantindo o nível apropriado de acesso aos usuários da instância.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Referências	Contextual Security Manager

Impor o Playbook para licenças e permissões ao escopo de segurança [Novo na Central de segurança 1.5]

Use esta propriedade para determinar se somente as ACLs (access control lists, listas de controle de acesso) do plug-in de licenças e permissões serão usadas para determinar o acesso ao escopo ou se as ACLs de todos os escopos serão consideradas.

Quando a propriedade *glide.enforce_security_scope.sn_gsm_lic_prmt* é definida com o valor recomendado de verdadeiro, somente as ACLs do plug-in de licenças e permissões são usadas para determinar o acesso ao escopo. Quando essa configuração é definida como falsa, os dados dos Playbooks para licenças e permissões nas tabelas mestres do escopo são expostos, porque as ACLs de todos os escopos recebem acesso. Para reduzir a exposição dos dados, defina *glide.enforce_security_scope.sn_gsm_lic_prmt* com o valor recomendado de verdadeiro.

Mais informações

Atributo	Descrição
Nome da configuração	*glide.enforce_security_scope.sn_gsm_lic_prmt*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	booliano
Valor recomendado	verdadeiro
Valor-padrão	verdadeiro
Categoria	Controle de acesso
Risco à segurança	• Pontuação de gravidade: 2,7 • Pontuação de CVSS: baixa • Detalhes do risco à segurança: definir esta configuração com o valor recomendado de verdadeiro protege os dados dos Playbooks para licenças e permissões nas tabelas mestres do escopo, por considerar somente as ACLs do escopo *sn_gsm_lic_prmt* para a concessão de acesso. Defini-la como falsa expõe os dados dos Playbooks para licenças e permissões nas tabelas mestres do escopo, por considerar as ACLs de todos os escopos para a concessão de acesso. Por exemplo, o administrador de TI pode acessar os dados dos Playbooks para licenças e permissões quando a configuração é falsa.
Dependências e pré-requisitos	Nenhum

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Referências	• Como usar o Playbook para licenças e permissões • Escopo da aplicação

Impor escopo de segurança para o Espaço do agente para Gestão de casos de RH [Novo na Central de segurança 1.5]

Configure o plug-in Espaço do agente para Gestão de casos de RH para que os dados das tabelas mestre do escopo sejam acessados apenas por usuários com as permissões corretas, de acordo com o princípio do menor privilégio.

Quando o plug-in *glide.enforce_security_scope.sn_hr_agent_ws* é configurado com o valor recomendado de verdadeiro, somente as ACLs (access control lists, listas de controle de acesso) do plug-in Espaço do agente para Gestão de casos de RH são usadas para determinar o acesso a um recurso. Quando essa configuração é definida como falsa, os dados do Espaço do agente para Gestão de casos de RH nas tabelas mestre do escopo são expostos, porque as ACLs de todos os escopos recebem acesso.Por exemplo, um administrador de TI pode acessar os dados do Espaço do agente para Gestão de casos de RH quando essa configuração é definida como falsa. Para evitar que isso aconteça, defina *glide.enforce_security_scope.sn_hr_agent_ws* com o valor recomendado de verdadeiro, o que garante o princípio do menor privilégio, já que os usuários só podem acessar os recursos para os quais têm permissão.

Mais informações

Atributo	Descrição
Nome da configuração	*glide.enforce_security_scope.sn_hr_agent_ws*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	booliano
Valor recomendado	verdadeiro
Valor-padrão	verdadeiro
Categoria	Controle de acesso
Risco à segurança	• Pontuação de gravidade: 2,7 • Pontuação de CVSS: baixa • Detalhes do risco à segurança: definir essa configuração como falsa faz com que os dados do Espaço do agente para Gestão de casos de RH nas tabelas mestre do escopo sejam expostos, porque as ACLs de todos os escopos recebem acesso.
Dependências e pré-requisitos	Espaço do agente para Gestão de casos de RH
Impacto funcional	Definir essa configuração como verdadeira faz com que as ACLs globais sejam executadas para uma tabela, se não houver ACLs com escopo para ela.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Referências	• https://owasp.org/www-project-proactive-controls/#div-numbering • Adicionar um componente a Espaço do agente

Aplicar a validação estrita do token CSRF

Use a propriedade *glide.security.csrf.strict.validation.mode* para habilitar a validação estrita do token CSRF. Se o token CSRF não corresponder, impedirá o reenvio da solicitação.

A propriedade *glide.security.csrf.strict.validation.mode* habilita a validação estrita do token CSRF, o que evita a reutilização de tokens CSRF. Se esta propriedade não estiver definida com o valor recomendado de verdadeiro, os tokens CSRF poderão ser reutilizados, o que abre uma porta para ataques de CSRF.

Mais informações

Atributo	Descrição
Nome da propriedade	*glide.security.csrf.strict.validation.mode*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Categoria	Controle de acesso
Finalidade	Impor a validação estrita do token CSRF e impedir sua reutilização.
Tipo de dados	booliano
Valor recomendado	verdadeiro
Valor-padrão	verdadeiro
Classificação de risco de segurança	(Médio) A falsificação de solicitação de site cruzado é um risco de segurança significativo que viola a integridade dos dados da instância. Um invasor pode iniciar o ataque de CSRF em qualquer usuário da instância abusando da confiança do usuário da instância. Com a ajuda de ataques de engenharia social, um usuário pode enviar uma solicitação malformada à instância em nome do invasor.
Impacto funcional	(Médio) Esta correção permite uma etapa de validação extra antes que o usuário da instância envie uma solicitação de gravação para a instância. Ela verifica se o token CSRF atual foi usado anteriormente. Se sim, impede o envio de outras solicitações de gravação.
Risco à segurança	(Médio) A falsificação de solicitação de site cruzado é um risco de segurança significativo que viola a integridade dos dados da instância. Um invasor pode iniciar o ataque de CSRF em qualquer usuário da instância abusando da confiança do usuário da instância. Com a ajuda de ataques de engenharia

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
	social, um usuário pode enviar uma solicitação malformada à instância em nome do invasor.

Retorne para Configure e carregue a chave fornecida pelo cliente para carregar sua chave encapsulada.

Restringir o acesso de leitura de desenvolvedores delegados [Atualizado na Central de segurança 1.3]

Se *com.glide.dd_allow_global_access_tables* não contiver o valor recomendado de wf_activity, wf_activity_definition, wf_workflow, wf_workflow_version, sp_portal, sp_widget e sp_page, essas tabelas poderão ser lidas por um desenvolvedor delegado. Isso pode oferecer ao desenvolvedor delegado acesso de leitura a informações confidenciais.

Mais informações

Atributo	Descrição
Nome da propriedade	*com.glide.dd_allow_global_access_tables*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	Cadeia de caracteres
Valor recomendado	wf_activity, wf_activity_definition, wf_workflow, wf_workflow_version, sp_portal, sp_widget, sp_page
Valor padrão	wf_activity, wf_activity_definition, wf_workflow, wf_workflow_version, sp_portal, sp_widget, sp_page
Categoria	Controle de acesso
Risco à segurança	• Pontuação de gravidade: 2,7 • Pontuação de CVSS: baixa • Detalhes do risco à segurança: a propriedade *com.glide.dd_allow_global_access_tables* deve ser definida como wf_activity, wf_activity_definition, wf_workflow, wf_workflow_version, sp_portal, sp_widget, sp_page.

Desabilitar e-mails de entrada para usuários bloqueados

Use a propriedade *glide.pop3.process_locked_out* para controlar as ações de e-mail de entrada para usuários ativos bloqueados.

Defina essa propriedade como **falsa** para desabilitar e-mails de entrada para usuários bloqueados.

Nota: Considere as implicações de segurança de permitir usuários de domínios não confiáveis e o motivo pelo qual eles foram bloqueados, antes de permitir que os e-mails deles acionem ações de e-mail de entrada.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mais informações

Atributo	Descrição
Nome da propriedade	*glide.pop3.process_locked_out*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Categoria	Controle de acesso
Finalidade	Esta propriedade controla as ações de e-mail de entrada para usuários ativos bloqueados.
Tipo de dados	booliano
Valor recomendado	falso
Valor-padrão	falso
Risco à segurança	(Alto) Quando você define esta propriedade como **verdadeira**, pode haver uma divulgação de informações, já que os e-mails de entrada são recebidos por usuários com contas bloqueadas.
Classificação de risco de segurança	7,5

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Verifique duas vezes as transações de entrada

Use a propriedade *glide.security.strict.updates* para habilitar a verificação dupla de segurança em transações de entrada durante o envio do formulário. Quando você define esta propriedade como **verdadeira**, ela adiciona uma camada extra de validação de tabela antes que formulário renderize no navegador.

Mais informações

Aviso: Esta é uma propriedade tipo porto seguro, o que significa que o valor não pode ser alterado após ser mudado. A reversão não é possível.

Atributo	Descrição
Nome da propriedade	*glide.security.strict.updates*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Categoria	Controle de acesso
Finalidade	Garantir uma camada adicional de verificação de permissões do usuário antes de apresentar o formulário no navegador.
Tipo de dados	booliano
Valor recomendado	verdadeiro
Valor-padrão	verdadeiro
Classificação de risco de segurança	8,1

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Impacto funcional	(Baixo) Esta correção adiciona apenas uma camada extra de validação para verificar se há permissões de usuário na tabela/página de destino na instância. Contanto que os controles de acesso sejam definidos corretamente na instância do cliente, não deve haver um impacto.
Risco à segurança	(Alto) Você sempre deve verificar a solicitação de acesso quando ocorrem transações entre duas zonas. Esta operação verifica se há permissões quando o formulário é solicitado e antes que a renderização do formulário ocorra.
Referências	

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Habilitar ACLs para controlar detalhes de perfil dinâmico

Use a propriedade *glide.live_profile.details* para designar se um usuário deve ser capaz de exibir todos os campos de detalhes, como nome da empresa e números de telefone, em um perfil dinâmico.

Dependendo da configuração da propriedade *glide.live_profile.details*, ocorre o seguinte:

- Se o valor for definido como Mostrar, o acesso às informações do perfil dinâmico será concedido, independentemente das ACLs criadas para o perfil do usuário.
- Se o valor for definido como ACL, o acesso às informações do perfil dinâmico será concedido, independentemente das ACLs criadas para o perfil do usuário.
- Se o valor for definido como Esconder, o acesso às informações do perfil dinâmico será restrito, independentemente das ACLs criadas para o perfil do usuário.

Mais informações

Atributo	Descrição
Nome da propriedade	*glide.live_profile.details*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Categoria	Controle de acesso
Finalidade	O objetivo é permitir que somente usuários autorizados acessem os detalhes de um Perfil dinâmico (como Nome da empresa, Números de telefone)
Tipo de dados	lista de seleção
Valor recomendado	ACL
Valor-padrão	ACL
Classificação de risco de segurança	4,3

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Impacto funcional	(Médio) Se a propriedade não estiver habilitada, os usuários não autorizados poderão acessar os detalhes do perfil dinâmico de todos os outros usuários.
Risco à segurança	(Moderado) As solicitações de API devem sempre respeitar as ACLs de tabela. A restrição deve ser aplicada para impedir que usuários não autorizados acessem detalhes de um Perfil dinâmico.

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Habilitar ACLs de exibição de relatório

Gerencie uma verificação de ACLs report_view de relatórios publicados.

Use a propriedade *glide.report.report_view.check_published* para gerenciar uma verificação de ACLs report_view para relatórios publicados. Se a propriedade não estiver definida com o valor recomendado de **verdadeira**, a verificação de ACLs report_view para relatórios publicados será desativada.

Aviso: Esta é uma propriedade tipo porto seguro, o que significa que o valor não pode ser alterado após ser mudado. A reversão não é possível.

Mais informações

Atributo	Descrição
Nome da configuração	*glide.report.report_view.check_published*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	booliano
Valor recomendado	verdadeiro
Valor-padrão	verdadeiro
Categoria	Controle de acesso
Risco à segurança	• Pontuação de gravidade: alta • Pontuações de CVSS: 7,5 • Detalhes do risco à segurança: se a propriedade não estiver definida como **verdadeira**, a verificação de ACLs report_view para relatórios publicados será desativada.
Dependências e pré-requisitos	Nenhum

Ativação da lista de permissões de URL para comunicação entre iframes de origens diferentes

Use a propriedade *glide.ui.concourse.onmessage_enforce_same_origin* para habilitar a comunicação de origem cruzada entre `iframes`.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O `OpenFrame` só pode processar mensagens de domínios confiáveis especificados na propriedade *glide.ui.concourse.onmessage_enforce_same_origin_whitelist*. Para obter mais informações, consulte Especificar a lista de permissões de UTL para comunicação de iframe de origem cruzada.

Mais informações

Atributo	Descrição
Nome da propriedade	*glide.ui.concourse.onmessage_enforce_same_origin*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	booliano
Categoria	Controle de acesso
Finalidade	Habilitar a lista de inclusões de domínios confiáveis para que eles possam se comunicar entre iframes para OpenFrame.
Valor recomendado	verdadeiro
Valor-padrão	verdadeiro
Classificação de risco de segurança	4,2
Impacto funcional	(Médio) Se você não colocar os domínios pretendidos na lista de inclusões, a capacidade de incorporar outras páginas em instâncias da Now Platform poderá ser limitada.
Risco à segurança	(Alto) Se uma página da Web contiver manipuladores de eventos que não executam a validação de origem apropriada, uma página da Web ou script de qualquer origem poderá se comunicar com ela. Ela também pode iniciar qualquer funcionalidade executada pelo manipulador de eventos.
Referências	Visão geral do OpenFrame

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Como impor restrições de escopo da aplicação [Novo na Central de segurança 1.3]

Use a propriedade *glide.record.legacy_cross_scope_access_policy_in_script* para controlar as permissões de apps com escopo.

Se a propriedade *glide.record.legacy_cross_scope_access_policy_in_script* estiver definida como verdadeira, os apps com escopo poderão chamar APIs que devem estar disponíveis somente para apps globais. Esta propriedade ignora os controles de acesso pretendidos para desenvolvedores desses apps com escopo, em termos de criação e atualização.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mais informações

Atributo	Descrição
Nome da configuração	*glide.record.legacy_cross_scope_access_policy_in_script*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	booliano
Valor recomendado	falso
Valor padrão	verdadeiro (quando a propriedade não existe na tabela sys_properties.)
Categoria	Controle de acesso
Risco à segurança	• Pontuação de gravidade: 3,5 • Pontuação de CVSS: baixa • Detalhes do risco à segurança: se esta propriedade não estiver definida com o valor recomendado, os apps com escopo e seus respectivos desenvolvedores delegados poderão criar e atualizar registros em tabelas globais, como Incidente.
Dependências e pré-requisitos	Nenhum

Como impor regras de segurança para compartilhar painéis [Novo na Central de segurança 1.3]

Use a propriedade *glide.cms.dashboards.sharing_with_secure_search* para controlar se os usuários podem compartilhar painéis.

Quando a propriedade *glide.cms.dashboards.sharing_with_secure_search* não está definida como **verdadeira**, ela permite que os usuários compartilhem grupos de painéis e funções aos quais eles não têm acesso. Ativar esta propriedade impõe as ACLs (access control lists, listas de controle de acesso) ao pesquisar as tabelas sys_user, sys_user_role e sys_user_group durante o processo de compartilhamento do painel. O compartilhamento excessivo de um painel pode fazer com que usuários, grupos ou funções acessem dados que não deveriam ter permissão para visualizar, comprometendo potencialmente as informações confidenciais. Portanto, é recomendável definir *glide.cms.dashboards.sharing_with_secure_search* como verdadeiro para que os painéis sejam compartilhados somente com aqueles que têm as permissões apropriadas.

Mais informações

Atributo	Descrição
Nome da configuração	*glide.cms.dashboards.sharing_with_secure_search*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	booliano
Valor recomendado	verdadeiro

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Valor-padrão	falso
Categoria	Controle de acesso
Risco à segurança	• Pontuação de gravidade: 3,5 • Pontuação de CVSS: baixa • Detalhes do risco à segurança: não definir esta propriedade com o valor recomendado de "verdadeiro" impede que as listas de controle de acesso sejam aplicadas ao pesquisar as tabelas sys_user, sys_user_role e sys_user_group. Isso pode fazer com que os painéis sejam compartilhados com usuários não autorizados, expondo informações confidenciais.
Dependências e pré-requisitos	Nenhum
Referências	Controle de acesso
Impacto funcional	Esta propriedade aplica regras de segurança a lista de usuários, grupos de usuários e funções que ficam visíveis durante o compartilhamento de painéis.

Impor a segurança de escopo para serviços digitais para setor público [Novo na Central de segurança 1.3]

Use a propriedade *glide.enforce_security_scope.sn_gsm* para controlar como os dados da aplicação Serviços digitais para setor público são acessados.

A aplicação ServiceNow Serviços digitais para setor público permite desenvolver aplicações do setor público que fornecem serviços digitais a constituintes, empresas e agências.

Quando *glide.enforce_security_scope.sn_gsm* é definido como falso, o acesso aos dados da aplicação nas tabelas globais do app Serviços digitais para setor público pode ser acessível com base nas listas de controle de acesso (ACLs) dessas tabelas globais. Quando esta propriedade está definida como verdadeira, o acesso aos dados que residem em tabelas globais é avaliado apenas com base nas ACLs enviadas diretamente no app Serviços digitais para setor público. Definir esta propriedade como falsa pode levar à divulgação de informações de ACLs excessivamente permissivas.

Para corrigir este risco de segurança, defina *glide.enforce_security_scope.sn_gsm* como verdadeiro.

Mais informações

Atributo	Descrição
Nome da configuração	*glide.enforce_security_scope.sn_gsm*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	booliano
Valor recomendado	verdadeiro
Valor-padrão	verdadeiro

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Categoria	Controle de acesso
Risco à segurança	• Pontuação de gravidade: 4,2 • Pontuação do CVSS: média • Detalhes do risco à segurança: não definir esta propriedade com o valor recomendado pode levar à divulgação de informações de ACLs excessivamente permissivas.
Dependências e pré-requisitos	Nenhum
Referências	Configuração da Serviços digitais para setor público

Impor o acesso por ACL com escopo definido para os Information Request Playbooks [Novo na Central de segurança 1.3]

Use a propriedade *glide.enforce_security_scope.sn_gsm_info_req* para controlar o acesso aos dados do playbook para o recurso Information Request Playbook.

A aplicação Information Request Playbook permite que os usuários finais do setor público enviem e rastreiem solicitações de registros públicos e fornece aos agentes do governo um processo predefinido para lidar e resolver essas solicitações. Se *glide.enforce_security_scope.sn_gsm_info_req* não estiver definido como verdadeiro, poderá ser concedido acesso inesperado aos dados do playbook para a aplicação Information Request Playbook. Defina esta propriedade como verdadeira para considerar somente as ACLs do escopo sn_gsm_info_req ao conceder acesso.

Mais informações

Atributo	Descrição
Nome da configuração	*glide.enforce_security_scope.sn_gsm_info_req*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	booliano
Valor recomendado	verdadeiro
Valor-padrão	verdadeiro
Categoria	Controle de acesso
Risco à segurança	• Pontuação de gravidade: 4,3 • Pontuação do CVSS: média • Detalhes do risco à segurança: se esta propriedade for definida como falsa, as ACLs de todos os escopos serão consideradas ao conceder acesso aos dados do playbook na tabela mestre do escopo. Isso exporia os dados do Information Request Playbook.
Dependências e pré-requisitos	Nenhum

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Referências	• Como usar o Information Request Playbook • Configurar canal de serviço de solicitações de informações

Impor privilégio de elevação estrita [Novo na Central de segurança 1.3]

Use a propriedade *glide.security.strict_elevate_privilege* para controlar se as funções marcadas como privilegiadas devem ser elevadas manualmente para que o usuário receba os recursos da função.

Configure esta propriedade como verdadeira para incluir uma camada extra de validação de segurança quando um usuário privilegiado elevar sua função.

Mais informações

Atributo	Descrição
Nome da configuração	*glide.security.strict_elevate_privilege*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	booliano
Valor recomendado	verdadeiro
Valor-padrão	verdadeiro
Categoria	Controle de acesso
Risco à segurança	• Pontuação de gravidade: 6,7 • Pontuação do CVSS: média • Detalhes do risco à segurança: quando *glide.security.strict_elevate_privilege* é definido como falso, as funções marcadas como privilegiadas são elevadas automaticamente na nova sessão de um usuário administrador e não precisam ser elevadas manualmente (com exceção de security_admin).
Dependências e pré-requisitos	Nenhum(a)
Impacto funcional	Esta propriedade requer estritamente que usuários com função de administrador elevem privilégios quando necessário.

Exigir a verificação de ACL de AJAXGlideRecord [Atualizado na Central de segurança 1.3]

Use a propriedade *glide.script.secure.ajaxglideracord* para executar a validação da regra de controle de acesso (ACL) quando registros do lado do servidor, como tabelas, forem acessados usando APIs GlideAjax em um script do cliente.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nos scripts do cliente, é possível consultar dados arbitrários do servidor usando a API AJAXGlideRecord (GlideAjax - Cliente) API, usando uma sintaxe como um registro de glide do lado do servidor É uma ferramenta poderosa e útil em muitas implantações.

Se você optar por aplicar ACLs (Access Control Lists, listas de controle de acesso) às chamadas de API GlideAjax, só será possível consultar os dados aos quais o usuário conectado no momento tem acesso. Por exemplo, se um usuário ESS que não tem direitos para ler a tabela cmn_location estiver conectado, qualquer chamada de API GlideAjax para essa tabela falhará.

Se o Now Platform estiver sendo executado sem a verificação de chamada da ACL GlideAjax, uma API poderá retornar informações que o usuário conectado no momento não poderia acessar.

Aviso: Esta é uma propriedade tipo porto seguro, o que significa que o valor não pode ser alterado após ser mudado. A reversão não é possível.

Mais informações

Atributo	Descrição
Nome da propriedade	*glide.script.secure.ajaxgliderecord*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Categoria	Controle de acesso
Finalidade	Garantir que as ACLs de segurança sejam verificadas e validadas mesmo quando os registros forem acessados por meio de APIs do lado do cliente.
Valor recomendado	verdadeiro
Valor-padrão	verdadeiro
Classificação de risco de segurança	8,1
Impacto funcional	(Alto) Esta correção impõe o relacionamento da ACL com registros do lado do servidor quando as solicitações são feitas usando as chamadas de API AJAXGlideRecord. Se a configuração da ACL não estiver configurada corretamente, há um possível impacto. Para obter mais detalhes sobre seu impacto e como identificá-lo, consulte o artigo Auditar e revisar transações GlideRecord do lado do cliente (AJAXGlideRecord) [KB0550828] em HI Base de conhecimento .
Risco à segurança	(Alto) Por meio de scripts do cliente, é possível consultar dados arbitrários do servidor por meio da API GlideAjax. Os recursos do lado do servidor podem ser acessados sem a autorização apropriada, portanto, o uso da validação de ACL ajuda a aplicação a validar a solicitação com base na autorização configurada.
Solução alternativa	Certifique-se de que as ACLs apropriadas sejam criadas para inclusões de script, processadores e outras entidades usadas por uma API GlideAjax

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
	(AJAXGlideRecord) para que elas sejam executadas com a devida autorização. Implemente métodos como `canRead()`, `canWrite()`, `canCreate()` e `canDelete()` para executar a autorização do usuário antes de acessar registros de tabela usando GlideRecord. Outro método é usar o GlideRecordSecure. A classe é herdada do servidor GlideRecord que executa as mesmas funções do GlideRecord e também impõe ACLs.
Referências	Aplicar ACLs ao AJAXGlideRecord (registro Glide do lado do cliente) Esta propriedade pertence à mesma família de propriedades que protegem e restringem a execução de scripts originados no cliente: • *glide.script.use.sandbox*: Consulte Área restrita de scripts gerados pelo cliente • *glide.script.allow.ajaxevaluate*: Consulte Habilitar AJAXEvaluate.

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Aplicar ACLs de nível de campo em GlideRecordSandbox

Gerencie ACLs de nível de campo no GlideRecordSandbox em sua instância.

Use a propriedade *glide.sandbox.fields.check_acl* para aplicar ACLs de nível de campo em GlideRecordSandbox. Um exemplo de aplicação dessa propriedade é quando um usuário pode fornecer um script, como em *sysparm_query*. Se essa propriedade não estiver definida com o valor recomendado de **verdadeiro**, as restrições de ACL poderão ser ignoradas, o que permite a violação de dados confidenciais, como um *sys_user.user_password* de um usuário não autorizado.

⚠ **Aviso:** O valor desta propriedade é uma substituição sem banco de dados. Não pode ser alterado ou substituído.

Mais informações

Atributo	Descrição
Nome da configuração	*glide.sandbox.fields.check_acl*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	booliano
Valor recomendado	verdadeiro
Valor-padrão	verdadeiro
Categoria	Controle de acesso

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Risco à segurança	• Pontuação de gravidade: 7,5 • Pontuação de CVSS: alta • Detalhes do risco à segurança: definir esta propriedade como **falsa** permite que as restrições de ACL sejam ignoradas, o que poderia expor dados confidenciais.
Dependências e pré-requisitos	Nenhum

Como impor o uso de alias de credencial [Novo na Central de segurança 1.3 e atualizado na 1.5]

Saiba como proteger suas credenciais contra uso não autorizado configurando a propriedade do MID Server.

O servidor de gestão, instrumentação e Descoberta (MID server) é uma aplicação Java executada como um serviço do Windows ou daemon UNIX em sua rede local. As propriedades do MID Server estão listadas na tabela [ecc_agent_property]. Você pode acessá-los em sua instância navegando até **MID Server** > **Propriedades**. Os aliases de credencial permitem que um administrador use credenciais específicas em Agendas de Descoberta. Os aliases de credenciais fornecem controle mais granular sobre qual credencial uma tabela de Descoberta pode usar. Para corrigir esta vulnerabilidade de segurança, defina *alias_filtering_behavior* como estrito para evitar a exposição desnecessária de credenciais com privilégios elevados. Consulte Propriedades do MID Server para obter mais detalhes.

Mais informações

Atributo	Descrição
Nome da configuração	*alias_filtering_behavior*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	cadeia de caracteres
Valor recomendado	estrito
Valor padrão	solto
Categoria	Controle de acesso
Risco à segurança	• Pontuação de gravidade: 2 • Pontuação de CVSS: baixa • Detalhes do risco à segurança: quando esta configuração de proteção não está definida como estrita, todas as credenciais são usadas, independentemente de seus aliases para tabelas de Descoberta, o que aumenta a chance de acesso não autorizado.
Dependências e pré-requisitos	Nenhum

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Referências	• MID Server • Aliases de credencial da Descoberta

Impor ACLs de GroupBy

Configure sua instância para conduzir verificações de ACL em colunas groupby.

Use esta propriedade para configurar sua instância para conduzir verificações de ACL em colunas groupby. Se esta propriedade for definida com o valor recomendado de **verdadeiro**, o atributo *groupby_acl_check* de uma tabela será definido para respeitar ACLs de groupby. Se a propriedade for definida como **falsa**, não haverá verificação de ACL nas colunas groupby de uma tabela, o que pode resultar no vazamento de informações.

Mais informações

Atributo	Descrição
Nome da configuração	*glide.security.groupby_acl_check*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	booliano
Valor recomendado	verdadeiro
Valor-padrão	verdadeiro
Categoria	Controle de acesso
Risco à segurança	• Pontuação de gravidade: 3,7 • Pontuação de CVSS: baixa • Detalhes do risco à segurança: a configuração desta propriedade como **falsa** desabilitará a verificação de ACLs nas colunas groupby, o que pode resultar no vazamento de informações.
Dependências e pré-requisitos	Nenhum

Garantir que a criação e a exclusão de painéis exijam verificação de acesso [Novo na Central de segurança 1.3]

A propriedade *glide.processors.check_access_before_process* habilita a imposição de ACLs (access control lists, listas de controle de acesso) para criar ou excluir painéis, enquanto o usuário estiver conectado. Esta propriedade deve ser sempre definida como verdadeira.

Mais informações

Atributo	Descrição
Nome da configuração	*glide.processors.check_access_before_process*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Tipo de dados	booliano
Valor recomendado	verdadeiro
Valor-padrão	falso
Categoria	Controle de acesso
Risco à segurança	• Pontuação de gravidade: 6,3 • Pontuação do CVSS: média • Detalhes do risco de segurança: desabilitar esta propriedade definindo-a como falsa habilita um desvio de ACL nos painéis. Isso permite que todos os usuários autenticados com baixos privilégios excluam e adicionem painéis.
Dependências e pré-requisitos	Nenhum(a)
Impacto funcional	Esta propriedade controla a capacidade de criar novos sys_dashboards e excluir painéis existentes quando um usuário não tiver os direitos de acesso necessários. Quando o valor está definido como falso, os usuários com funções inadequadas podem inserir e excluir entradas do sys_dashboard (mas a camada GlideRecord deve verificar novamente as ACLs existentes). Um valor verdadeiro restringe as operações de inserção e exclusão de usuários que não têm os direitos de acesso necessários.

Impor validação de parâmetro de estado do OAuth

Configure a propriedade *glide.oauth.state.parameter.required* para impedir que sua instância sofra ataques de CSRF (cross-site request forgery, falsificação de solicitação entre sites).

A propriedade *glide.oauth.state.parameter.required* permite que o parâmetro de estado seja obrigatório em uma solicitação OAuth para o fluxo de código de autorização. O parâmetro de estado é um valor de cadeia de caracteres e não deve conter caracteres especiais nem ser vazio. Definir esta propriedade como **verdadeira** impede que um invasor execute ataques de CSRF (cross-site request forgery, falsificação de solicitação entre sites) durante a autenticação, o que protege sua instância de ataques de um usuário representado.

Mais informações

Atributo	Descrição
Nome da configuração	*glide.oauth.state.parameter.required*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	booliano
Valor recomendado	verdadeiro
Valor-padrão	verdadeiro

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Categoria	Controle de acesso
Risco à segurança	• Pontuação de gravidade: 4,2 • Pontuação do CVSS: média • Detalhes do risco à segurança: defina esta propriedade como **verdadeira** para impedir os ataques de CSRF.
Dependências e pré-requisitos	Nenhum

Impor upload estrito de imagem do usuário

Use a propriedade *glide.security.strict.user_image_upload* para habilitar o Controle de acesso para carregar/atualizar uma imagem de perfil quando executada em um registro de usuário.

Esta configuração abre a possibilidade de um usuário não autorizado carregar uma imagem no perfil de outro usuário.

- Quando você define esta propriedade como **verdadeira**, as ACLs de tabelas são aplicadas ao carregar fotos, permitindo que somente usuários autorizados carreguem uma imagem.
- Quando você a define como **falsa**, as ACLs não são aplicadas nos carregamentos de imagem para o campo Foto.

Mais informações

Atributo	Descrição
Nome da propriedade	*glide.security.strict.user_image_upload*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Categoria	Controle de acesso
Finalidade	Restringir o carregamento da imagem do usuário somente a usuários autorizados.
Valor recomendado	verdadeiro
Classificação de risco de segurança	3,7
Impacto funcional	(Baixo) Nenhum impacto na funcionalidade, já que os usuários autorizados ainda podem carregar imagens em seus perfis de usuário.
Risco à segurança	(Baixo) Quando você define esta propriedade como **falsa**, um usuário autenticado pode carregar uma imagem na conta de outro usuário sem autorização.

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Restrição de domínios de e-mail para registro de usuários externos [Atualizado na Central de segurança 1.5]

Use a propriedade *sn_ext_usr_reg.allowed_email_domains* para listar domínios de e-mail externos aceitáveis.

Mais informações

Atributo	Descrição
Nome da propriedade	*sn_ext_usr_reg.allowed_email_domains*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do), Propriedades das Comunidades
Categoria	Controle de acesso
Finalidade	Listar os domínios de e-mail para permitir o e-mail do usuário para registro.
Valor recomendado	Definir como um valor não vazio
Tipo de configuração	Cadeia de caracteres
Risco à segurança	(Alto) Agentes mal-intencionados podem realizar o registro usando endereços de e-mail de domínios indesejados. Certifique-se de que *sn_ext_usr_reg.allowed_email_domains* não esteja definido como um valor vazio.
Classificação de risco de segurança	7,5
Referências	Comunidades

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Plug-in Alta segurança [Atualizado na Central de segurança 1.3]

Quando você ativa o plug-in High security, ele cria ou atualiza centenas de configurações diferentes para controlar o nível de segurança em sua instância. Essas configurações atenuam muitos dos principais ataques OWASP, permitindo controle de acesso estrito, validação de entrada e codificação de saída.

Essas configurações incluem:

- Controle de Acesso
- Regras de negócios
- Propriedades do sistema
- Ação de Política de IU
- ações de script
- Inclusões de script

Exemplo

Consulte os exemplos para as seguintes propriedades:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Propriedade	Tópico
glide.ui.escape_all_script	Escapar do Jelly
glide.security.strict.actions	Verifique a ação de IU antes da execução
glide.security.csrf_previous.allow	Token anti-CSRF
glide.security.csrf.strict.validation.mode	Validação estrita de CSRF

Mais informações

Atributo	Descrição
Nome do Plug-in	com.glide.high_security
Tipo de configuração	Definição do sistema > Plug-ins - Desenvolvimento
Categoria	Controle de acesso
Finalidade	É obrigatório ativar este plug-in. Ele aumenta o nível de segurança de uma instância, o que reduz a superfície de ataque ao atenuar os 10 principais ataques do owasp, incluindo CSRF, XSS, protegendo cookies de sessão e uploads de arquivo.
Valor recomendado	Ativo
Classificação de risco de segurança	9,8
Impacto funcional	(Alto) Este plug-in permite várias configurações de segurança do sistema, o que pode afetar a IU e a funcionalidade.
Risco à segurança	(Alto) Muitas configurações de segurança são acidentalmente deixadas em aberto, o que pode abrir a porta para algumas das vulnerabilidades críticas.
Referências	Ativar configurações de alta segurança Configurações de Alta Segurança

Para saber mais sobre como ativar um plug-in, consulte Ativar um plug-in

Aceitar ACLs de substituição de administrador

A propriedade *glide.security.admin.override.accessterm* controla os administradores para não conseguirem substituir a avaliação da ACL, mesmo onde a substituição deveria estar em vigor.

Mais informações

Atributo	Descrição
Nome da propriedade	*glide.security.admin.override.accessterm*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Categoria	Controle de acesso
Finalidade	Controla os administradores para que não consigam substituir a avaliação da ACL.
Tipo de dados	Booliano
Valor recomendado	Verdadeiro
Valor padrão	Verdadeiro
Risco à segurança	(Baixo) As ACLs são avaliadas cumulativamente. Se houver um número de ACLs em qualquer campo e a opção Substituições de Administrador for falsa (não selecionada) em um deles, as substituições de administrador efetivas para todas as ACLs serão consideradas falsas.
Classificação de risco de segurança	3,8
Referências	Regras da lista de controle de acesso

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Impedir que usuários inativos façam login [Novo na Central de segurança 1.5]

Configure esta propriedade para controlar se usuários inativos podem se autenticar em sua instância.

Defina o valor da propriedade *glide.authenticate.only.allow.active.user.login* como verdadeiro (recomendado). Isso garante que os usuários da tabela sys_user marcados como inativos não possam fazer login na instância e sejam bloqueados.

Se a configuração estiver definida como falsa, os usuários ainda poderão acessar a instância e os dados aos quais tinham acesso anteriormente.

Mais informações

Atributo	Descrição
Nome da configuração	*glide.authenticate.only.allow.active.user.login*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	booliano
Valor recomendado	verdadeiro
Valor-padrão	verdadeiro
Categoria	Controle de acesso
Risco à segurança	• Pontuação de gravidade: 7,5 • Pontuação de CVSS: alta • Detalhes do risco à segurança: não definir essa propriedade com o valor recomendado verdadeiro

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
	pode permitir que usuários inativos, como um funcionário demitido, ainda acessem a instância e os dados.
Dependências e pré-requisitos	Nenhum

Como restringir solicitações JSONP a URLs confiáveis [Atualizado na Central de segurança 1.3]

Especifique URLs confiáveis para o serviço AngularJS $http para permitir ou rejeitar solicitações JSONP.

A propriedade *angular.jsonp.inclusion_list.enabled* especifica URLs confiáveis para o serviço angularJS $http para permitir e/ou rejeitar solicitações JSONP. A propriedade é de suma necessidade por ser uma mudança potencialmente interruptiva para os clientes, por isso é preciso que haja uma maneira de eles adicionarem seus URLs confiáveis. Se não estiver definido com o valor recomendado de verdadeiro, as solicitações JSONP serão permitidas para qualquer URL.

Mais informações

Atributo	Descrição
Nome da configuração	*angular.jsonp.inclusion_list.enabled*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	booliano
Valor recomendado	verdadeiro
Valor-padrão	verdadeiro
Categoria	Controle de acesso
Risco à segurança	• Pontuação de gravidade: Média • Pontuação de CVSS: 5,4 • Detalhes do risco à segurança: definir esta propriedade como **falsa** habilita solicitações JSONP para qualquer URL.
Dependências e pré-requisitos	Nenhum

Como desabilitar a execução de consultas brutas no banco de dados [Atualizado na Central de segurança 1.3]

Controle se um usuário pode executar consultas SQL brutas no banco de dados.

A propriedade *glide.db.allow_unsafe_dbi_execute_sql* permite que os usuários executem consultas SQL brutas no banco de dados, o que pode dar acesso a tabelas e dados fora das restrições do GlideRecord. Se esta propriedade não estiver definida com o valor recomendado de *false*, isso permitirá a chamada de *dbi.executeStatement()* de um Glide programável que pode resultar na execução de instruções SQL mal-intencionadas.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Aviso: Esta propriedade é segura e não há substituição de banco de dados.

Mais informações

Atributo	Descrição
Nome da configuração	*glide.db.allow_unsafe_dbi_execute_sql*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	booliano
Valor recomendado	falso
Valor-padrão	falso
Categoria	Controle de acesso
Risco à segurança	• Pontuação de gravidade: 7,2 • Pontuação de CVSS: alta • Detalhes do risco à segurança: não definir esta propriedade como **falsa** permite a chamada de *dbi.executeStatement()* de um Glide programável.
Dependências e pré-requisitos	Nenhum
Referências	Regras da lista de controle de acesso

Ocultar comentários de usuários em artigos [Novo na Central de segurança 1.3]

Use a propriedade *glide.knowman.show_user_feedback* para controlar se os comentários de feedback ficam visíveis.

Quando *glide.knowman.show_user_feedback* não estiver definida como "nunca", os comentários de feedback ficarão visíveis nos artigos da base de conhecimento para usuários com as funções definidas na propriedade do Glide, *glide.knowman.show_user_feedback.roles*. Como os comentários de feedback podem conter informações confidenciais, talvez você não queira que o feedback fique visível. Se esta propriedade não estiver definida como “nunca”, poderá haver impactos de confidencialidade se informações confidenciais forem divulgadas no feedback.

Mais informações

Atributo	Descrição
Nome da configuração	*glide.knowman.show_user_feedback*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	lista de seleção
Valor recomendado	nunca
Valor padrão	onload
Categoria	Controle de acesso

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Risco à segurança	• Pontuação de gravidade: 3,5 • Pontuação de CVSS: baixa • Detalhes do risco à segurança: não definir esta propriedade como "nunca" pode resultar na divulgação de informações confidenciais nos comentários de feedback.
Dependências e pré-requisitos	Nenhum(a)
Impacto funcional	Mostra comentários de usuários em artigos da base de conhecimento de acordo com as opções mencionadas na configuração.

Exigir autenticação por padrão para inclusões de script de cliente chamável [Atualizado na Central de segurança 1.3]

Por padrão, as inclusões de script de cliente chamável que não definem explicitamente a visibilidade são públicas. Se necessário, adicione a propriedade *glide.script.ccsi.ispublic* para habilitar o controle de privacidade sobre todas as inclusões de script de cliente chamável acessadas por páginas públicas.

Ao adicionar esta propriedade, você deve definir seu valor como **falso**, o que indica que todas as inclusões de script de cliente chamável são privadas e mudam sua visibilidade nas páginas públicas.

Nota: Você não pode adicionar a propriedade com um valor **verdadeiro** ou alterar seu valor de **falso** para **verdadeiro**. Se você tentar fazer isso, será exibida uma mensagem de erro.

Se necessário, você pode alterar a configuração de privacidade de uma inclusão de script de cliente chamável adicionando a função `isPublic ()`.

- A configuração `isPublic ()` tem precedência sobre a propriedade *glide.script.ccsi.ispublic*.
- Por exemplo, se você definir `isPublic ()` como **verdadeira** em um script individual, ele será público, o que substituirá a propriedade *glide.script.ccsi.ispublic* que torna privadas todas as outras inclusões de script de cliente chamável.

Aviso: Esta é uma propriedade tipo porto seguro, o que significa que o valor não pode ser alterado após ser mudado. A reversão não é possível.

Mais informações

Atributo	Descrição
Nome da propriedade	*glide.script.ccsi.ispublic*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Categoria	Controle de acesso
Finalidade	Tornar privadas as inclusões de script de cliente chamável significa que os convidados que acessam páginas públicas não podem acessar a inclusão

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
	de script de cliente chamável. Um usuário não conectado não pode executar um script privado.
Valor recomendado	falso
Valor-padrão	falso
Classificação de risco de segurança	7,5
Impacto funcional	(Alto) Se as inclusões de script de cliente chamável forem designadas como públicas (ou seja, esta propriedade estiver ausente), os usuários não autenticados poderão executar scripts de cliente. Adicionar a propriedade restringe a execução de scripts por um usuário não logado.
Risco à segurança	(Alto) Se você não adicionar esta propriedade, as inclusões de script do lado do cliente contornarão as ACLs, o que pode resultar em funcionalidade pública não intencional. Se o script do cliente fornecer informações confidenciais, ele poderá representar um risco potencial adverso à segurança.
Solução alternativa	Definir a propriedade *glide.script.ccsi.ispublic* como **falsa** torna privadas todas as inclusões de script de cliente chamável. Você pode alterar a configuração de privacidade de uma inclusão de script de cliente chamável adicionando a função `isPublic ()`. A função `isPublic ()` tem precedência sobre a propriedade *glide.script.ccsi.ispublic*. Adicione a seguinte sintaxe à inclusão de script: `isPublic:function(){return[true/false];},`

Como impor o comportamento da instância de produção [Atualizado na Central de segurança 1.3 e 1.5]

Configure se sua instância deve ser tratada como uma instância de produção ou de não produção.

Se a propriedade *glide.installation.production* não estiver definida com o valor recomendado de **verdadeiro**, a instância não será tratada como uma instância de produção, permitindo assim a execução do zboot e de outros scripts potencialmente perigosos. Permitir que uma instância de produção seja avaliada como uma instância de não produção pode levar a vazamentos de informações ou ataques DoS (Denial of Service, negação de serviço).

Mais informações

Atributo	Descrição
Nome da configuração	*glide.installation.production*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Tipo de dados	booliano
Valor recomendado	verdadeiro
Valor-padrão	verdadeiro
Categoria	Controle de acesso
Risco à segurança	• Pontuação de gravidade: 6,3 • Pontuação do CVSS: média • Detalhes do risco à segurança: definir este valor de propriedade como **falso** faz com que a instância seja tratada como uma instância de não produção, o que permite a execução do zboot e de outros scripts potencialmente perigosos.
Dependências e pré-requisitos	Nenhum

Restringir o acesso ao script em segundo plano

Configure a propriedade *glide.script_processor.admin* para definir a função necessária para acessar o módulo Script em segundo plano.

A propriedade *glide.script_processor.admin* armazena a função necessária para acessar o módulo Script em segundo plano. Se esta propriedade não estiver definida com o valor recomendado de **administrador**, qualquer usuário, independentemente da função, poderá executar scripts em segundo plano na instância. Isso permite que agentes mal-intencionados ignorem o sistema de ACL, concedendo-lhes acesso total às tabelas.

⚠ **Aviso:** Esta é uma propriedade tipo porto seguro, o que significa que o valor não pode ser alterado após a mudança. A reversão não é possível.

Mais informações

Atributo	Descrição
Nome da configuração	*glide.script_processor.admin*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	cadeia de caracteres
Valor recomendado	admin
Valor-padrão	admin
Categoria	Controle de acesso
Risco à segurança	• Pontuação de gravidade: 8,8 • Pontuação de CVSS: alta • Detalhes do risco à segurança: não definir esta propriedade com o valor recomendado de **administrador** permite que qualquer usuário execute scripts em segundo plano na instância.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Dependências e pré-requisitos	Nenhum

Restringir o acesso a e-mails com tabela de destino vazia

Ative a propriedade *glide.email.email_with_no_target_visible_to_all* para restringir o acesso do usuário a e-mails, a menos que ele tenha enviado o e-mail ou tenha uma função de administrador.

Usuários não autorizados podem acessar e-mails na tabela sys_email_list que não tenham um registro de destino. Em vez de impor ACLs em entradas de e-mail, esta propriedade restringe o acesso somente ao remetente do e-mail e aos usuários com a função de administrador.

Nota: Os e-mails enviados e recebidos pela instância aparecem na tabela sys_email_list. No entanto, somente os e-mails recebidos que foram marcados com um estado de Erro e Ignorado devem ter uma tabela de destino vazia.

Mais informações

Atributo	Descrição
Nome da propriedade	*glide.email.email_with_no_target_visible_to_all*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Configurar	Controle de acesso
Finalidade	Bloquear o cliente de e-mail de mostrar e-mails quando o usuário não autorizar o acesso.
Valor recomendado	falso
Valor-padrão	verdadeiro
Classificação de risco de segurança	5,4
Impacto funcional	(Baixo) Os usuários não podem mais ver e-mails cuja tabela de destino esteja vazia, a menos que sejam um administrador ou o remetente do e-mail.
Risco à segurança	(Moderado) Se a propriedade não estiver habilitada, os usuários não autorizados poderão acessar qualquer e-mail em que o campo target_table esteja vazio.
Referências	Propriedades avançadas de e-mail https://support.servicenow.com/kb_view.do?sysparm_article=KB0690043

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Plug-in Restringir o acesso a intervalos de IP específicos

Use a propriedade *com.snc.ipauthenticator* plug-in para restringir o acesso a intervalos de IP específicos. A menos que o acesso público seja destinado à instância, os administradores devem limitar o acesso aos blocos de rede IP atribuídos.

Pré-requisitos

Antes de definir esta propriedade, você deve ativar o plug-in Autenticação baseada no intervalo de IP (com.snc.ipauthenticator) *com.snc.ipauthenticator*. Para saber mais, consulte Autenticação baseada no intervalo de IP e vá à seção Etapas para configurar (abaixo).

Mais informações

Atributo	Descrição
Nome do Plug-in	*com.snc.ipauthenticator*
Tipo de configuração	Segurança do sistema > Controle de acesso de endereço IP
Categoria	Controle de acesso
Finalidade	Adicionar o intervalo de endereços IP que podem ou não acessar a instância às listas de domínios confiáveis e não confiáveis.
Valor recomendado	Ativo
Valor-padrão	Nenhum. Este é um plug-in, não uma propriedade do Glide. Portanto, não há nenhum valor padrão.
Classificação de risco de segurança	5,3
Impacto funcional	(Baixo) Intervalos de IP negados pelo cliente são usados para este item de correção. Nenhum impacto conforme o cliente define a lista de destino.
Risco à segurança	(Baixa) A exposição desnecessária à instância de destino na Internet deve ser restrita com a ajuda da funcionalidade de controles de acesso por IP.
Referências	Autenticação baseada no intervalo de IP

Etapas para configurar

1. Certifique-se de que o plug-in com.snc.ipauthenticator esteja ativo.
2. Navegue até **Segurança do sistema** > **Controle de acesso de endereços IP**.
3. Clique em **Novo** para criar uma lista de exclusões (Negar) ou uma lista de inclusões (Permitir) de endereços IP.
4. Clique em **Enviar**.

Restringir o acesso às bases de conhecimento [Novo na Central de segurança 1.3]

A propriedade *glide.knowman.block_access_with_no_user_criteria* é usada para controlar o acesso de leitura/gravação de usuários em artigos baseados em conhecimento.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mais informações

Atributo	Descrição
Nome da configuração	*glide.knowman.block_access_with_no_user_criteria*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	booliano
Valor recomendado	verdadeiro
Valor-padrão	falso
Categoria	Controle de acesso
Risco à segurança	• Pontuação de gravidade: 9,1 • Pontuação de CVSS: Crítica • Detalhes do risco de segurança: Se esta propriedade não estiver configurada com o valor recomendado de verdadeiro, qualquer usuário poderá ler e contribuir com uma base de conhecimento.
Dependências e pré-requisitos	Nenhum(a)
Impacto funcional	Nega o acesso a uma base de conhecimento quando "Pode ler" ou "Pode contribuir" não forem especificados.

Restringir permissões para o modelo CMDB

Use a propriedade do sistema *csm_cmdb_model.customer_visible_flag* para limitar o acesso do cliente aos dados na tabela Modelos de produto como um controle de acesso adicional ao modelo CMDB.

Defina a propriedade *csm_cmdb_model.customer_visible_flag* como **verdadeira** para habilitar o campo Visível ao cliente para as tabelas listadas abaixo:

- Tabela de modelos do produto [cmdb_model]
- Tabela de modelos de software [cmdb_software_product_model]
- Tabela de modelos de aplicação [cmdb_application_product_model]
- Tabela de modelos de consumíveis [cmdb_consumable_product_model]
- Tabela de modelos de instalação [cmdb_facility_product_model]
- Tabela de modelos de hardware [cmdb_hardware_product_model]

Definir esta propriedade como **verdadeira** oculta todos os valores cmdb_model por padrão.

Defina a propriedade como **falsa** para não considerar a coluna/o atributo customer_visible na tabela cmdb_model e para contar com as bases de ACL de cmdb_model que são acessíveis para sn_esm_user.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mais informações

Atributo	Descrição
Nome da propriedade	*csm_cmdb_model.customer_visible_flag*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Categoria	Controle de acesso
Finalidade	Quando definido como **verdadeiro**, o sistema usa a configuração no campo Visível ao cliente para determinar o acesso aos dados do modelo do produto no Portal de atendimento ao cliente.
Valor recomendado	verdadeiro
Valor-padrão	falso
Tipo de dados	Booliano
Risco à segurança	(Moderado) Qualquer usuário com a função sn_esm_user e ACLs prontas para uso pode ter permissões para o modelo do CMDB. **Nota:** esta função tende a ser concedida a usuários externos. Usuários externos podem receber involuntariamente permissões para o modelo CMDB.
Referências	Limitar o acesso aos dados do modelo de produto no Portal de atendimento ao cliente

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Restringir o acesso não autenticado aos anexos

Use a propriedade *glide.image_provider.security_enabled* para controlar as configurações de segurança das imagens. Se definida como **verdadeira**, as imagens serão visíveis somente para usuários autenticados e autorizados. Se definida como **falsa**, as imagens ficarão visíveis para qualquer pessoa com um URL para o anexo.

Mais informações

Atributo	Descrição
Nome da propriedade	*glide.image_provider.security_enabled*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Categoria	Controle de acesso
Finalidade	Impedir o acesso não autenticado ao anexo quando renderizado usando o formato *.iix*.
Valor recomendado	verdadeiro
Valor-padrão	verdadeiro

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Impacto funcional	(Baixo) Nenhum impacto significativo na funcionalidade. A experiência do usuário pode ser um pouco afetada porque o usuário que acessava diretamente o .iix deve passar pela autenticação.
Risco à segurança	(Alto) A restrição deve ser aplicada para usuários não autenticados, pois alguns anexos podem conter informações confidenciais.
Referências	Administrar anexos Propriedades do sistema disponíveis

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Restrição do acesso a entradas personalizadas de registros [Atualizado na Central de segurança 1.3]

Use a propriedade *glide.live_feed.custom_journal.acl_check_enabled* para respeitar as ACLs em campos de diário personalizados.

Se *glide.live_feed.custom_journal.acl_check_enabled* não estiver definido com o valor recomendado de verdadeiro, todos os usuários poderão ver todas as entradas de registro no recurso de feed. Definir a propriedade como verdadeira respeitará as ACLs em campos de diário personalizados, e isso é bastante útil.

Mais informações

Atributo	Descrição
Nome da propriedade	*glide.live_feed.custom_journal.acl_check_enabled*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Categoria	Controle de acesso
Finalidade	Controlar quais usuários veem quais entradas de registro com base em ACLs.
Valor recomendado	verdadeiro
Valor-padrão	verdadeiro
Tipo de configuração	Booliano.
Risco à segurança	(Moderado) Quando definido como verdadeiro, somente as entradas de registro personalizadas aprovadas na ACL serão mostradas no Feed de atividades. Caso contrário, todos os usuários poderão ver todas as entradas de registro.

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Restringir o acesso de leitura ao contexto de fluxo [Novo na Central de segurança 1.5]

Use a propriedade *com.snc.process_flow.reporting.require_flow_access* para determinar se uma verificação de acesso adicional é necessária para que um usuário leia uma verificação de fluxo.

Quando a propriedade *com.snc.process_flow.reporting.require_flow_access* é definida com o valor recomendado de verdadeiro, há uma verificação de acesso adicional para um usuário que tenta ler um contexto de fluxo. Se a propriedade for definida como falsa, informações secundárias podem ser divulgadas.

Mais informações

Atributo	Descrição
Nome da configuração	*com.snc.process_flow.reporting.require_flow_access*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	booliano
Valor recomendado	verdadeiro
Valor-padrão	verdadeiro
Categoria	Controle de acesso
Risco à segurança	• Pontuação de gravidade: 2,7 • Pontuação de CVSS: baixa • Detalhes do risco à segurança: definir essa propriedade como falsa mantém o comportamento existente. Definir essa propriedade como verdadeira aplica a camada de segurança adicional de acesso de leitura.
Dependências e pré-requisitos	Nenhum(a)
Impacto funcional	Quando essa propriedade está habilitada, a segurança para os registros de contexto de fluxo de leitura é aumentada. A instância determina que um usuário que tente ler o contexto de fluxo também tenha acesso de leitura ao fluxo primário.

Habilitar o plug-in Security Jump Start (regras de ACL) [Atualizado na Central de segurança 1.3]

Ative o plug-in Security Jump Start (regras de ACL) (com.snc.system_security*com.snc.system_security*) para criar várias ACLs importantes que validam os Controles de acesso em algumas das principais tabelas do sistema na Now Platform.

Essas regras fornecem um salto na proteção de muitas tabelas do sistema, facilitando para uma organização colocar uma instância em produção. O plug-in Security Jump Start (regras de ACL) é instalado automaticamente em todas as novas instâncias.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mais informações

Atributo	Descrição
ID do plug-in	*com.snc.system_security*
Tipo de configuração	Definição do sistema > Plug-ins
Categoria	Controle de acesso
Finalidade	Ativar o plug-in Security Jump Start (regras de ACL) para obter a conformidade de segurança apropriada. Ele fornece algumas ACLs básicas que protegem as tabelas do sistema em primeiro lugar, em vez de criar manualmente para cada tabela do sistema que vem com o provisionamento padrão de uma instância. Essas ACLs são úteis quando a instância recém-criada deve passar rapidamente para a produção.
Valor recomendado	Ativo
Valor padrão	Nenhum. Esse é um plug-in, não uma propriedade do Glide; portanto, não há valor padrão. O plug-in é instalado por padrão no zBoot (redefinições).
Classificação de risco de segurança	8,1
Impacto funcional	(Médio) Há um impacto funcional significativo se este plug-in for instalado sem auditoria das ACLs existentes na instância. A divulgação e as definições do cliente são necessárias antes que a correção ocorra.
Risco à segurança	(Alto) O controle de acesso deve ser aplicado para bloquear o acesso não intencional à instância. As regras de ACL jumpstart fornecem um ponto de partida para proteger muitas tabelas do sistema, facilitando para uma organização entrar rapidamente na produção.
Referências	Security jump start - regras de ACL

Etapas para configurar

Se este plug-in não estiver ativado em sua instância, entre em contato com o suporte da ServiceNow. Ativar o plug-in neste ponto pode modificar o acesso de segurança a tabelas já em uso em um ambiente de produção. Se um administrador estiver interessado nas novas regras de ACL fornecidas pelo plug-in, você poderá criar manualmente uma ou mais delas em uma instância existente, se necessário. Esta lista de ACLs pode ser usada como diretriz nesse caso.

Uso da operação segura de inserção múltipla na API de conjuntos para importação [Novo na Central de segurança 1.3]

Use a propriedade *com.glide.import_set_api.insert_multiple_optimize* para controlar se *GlideRecordSecure* ou *GlideRecord* é usado para a operação de inserção múltipla na API de conjuntos para importação.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Se *com.glide.import_set_api.insert_multiple_optimize* for definida com o valor recomendado de falsa, o *GlideRecordSecure* será usado para inserir registros, e as ACLs (access control lists, listas de controle de acesso) no nível da tabela serão avaliadas. Se esta propriedade estiver configurada como verdadeira, *GlideRecord* será utilizado para inserir registros, e as ACLs no nível de tabela não serão avaliadas. Além disso, você deve garantir que API de Conjunto para importação Insert Multiple REST Endpoint ACL (sys_id: 3101b770ff2211105cf343d0653bf182) esteja ativo e que os usuários tenham a função import_transformer.

Mais informações

Atributo	Descrição
Nome da configuração	*com.glide.import_set_api.insert_multiple_optimize*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	booliano
Valor recomendado	falso
Valor-padrão	falso
Categoria	Controle de acesso
Risco à segurança	• Pontuação de gravidade: 6,5 • Pontuação do CVSS: média • Detalhes do risco à segurança: se esta propriedade não estiver definida como "falsa", um usuário com baixos privilégios poderá inserir dados em tabelas fora do escopo de suas funções privilegiadas.
Comportamento reversível	Substituição de banco de dados segura e Nenhuma substituição de banco de dados.
Dependências e pré-requisitos	Nenhum(a)
Impacto funcional	Esta propriedade otimiza o desempenho da API do Conjunto para importação usando o GlideRecord para salvar dados. Ao ser definido, o parâmetro requer que um usuário de integração tenha a função import_transformer para acessar a API.
Referências	https://developer.servicenow.com/blog.do?p=/post/gliderecord-vs-gliderecordsecure

Como impor a segurança estrita de solicitações SOAP [Atualizado na Central de segurança 1.3]

Use a propriedade *glide.soap.strict_security* para impor a segurança do serviço da Web.

Esta propriedade usa uma combinação de:

- Desafio/resposta da autenticação básica sobre o protocolo HTTP e
- Controles de acesso no nível do sistema no Plug-in Contextual Security: Role Management.

Se você definir esta propriedade como **verdadeira**, ela executará as seguintes ações:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Se o usuário tiver a função apropriada para executar a operação, ela verificará a solicitação de entrada do SOAP para validação da autorização da função. Isso ocorre durante chamadas/solicitações do SOAP Web Services feitas em relação a tabelas da Now Platform ao executar operações CRIAR, LER, ATUALIZAR ou EXCLUIR.
- Verifica as ACLs no nível do sistema ao recuperar dados na forma de dados SOAP na tabela.
- Verifica as ACLs no nível de campo para qualquer operação CRUD executada em um campo de tabela.

As verificações de ACL são concluídas somente para chamadas padrão de API da tabela, e não para serviços da Web.

Mais informações

Atributo	Descrição
Nome da propriedade	*glide.soap.strict_security*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Categoria	Controle de acesso
Valor padrão	verdadeiro
Valor recomendado	verdadeiro
Impacto funcional	(Alto) Esta correção impõe o controle de acesso no nível do sistema ao recuperar dados de tabelas/ páginas na forma de dados SOAP na instância. Se houver usuários acessando esses dados, eles serão restritos/terão permissão para acessar os dados com base nas regras de ACL. Para obter as funções padrão que têm acesso aos dados SOAP, consulte SOAP Web Services.
Risco à segurança	(Moderado) Sem a autorização apropriada configurada nas solicitações SOAP recebidas, um usuário não autorizado pode obter acesso a conteúdo/dados confidenciais na instância de destino.
Referências	Impor segurança estrita para SOAP de entrada SOAP Web Services

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Fábricas exigidas de conexão JMS [Novo na Central de segurança 1.3 e atualizado na 1.5]

A propriedade *mid.property.jms.command.allowed_factory_names* controla as fábricas de conexão JMS (Java Messaging Service) que o MID Server pode usar.

Ela é destinada a algumas fábricas selecionadas exigidas pelos plug-ins para atividade ou ação do JMS. A inclusão de fábricas adicionais pode ser uma etapa em uma cadeia

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

de ataques para vulnerabilidades, como a inserção de JDNI, que depende de recursos que um invasor pode aproveitar em fábricas permitidas. Para evitar qualquer possível aproveitamento de vulnerabilidade, não inclua fábricas além dos padrões necessários.

Para corrigir esse risco à segurança, revise a lista de nomes informados para a propriedade MID, *mid.property.jms.command.allowed_factory_names*. Certifique-se de que sejam necessários os nomes de fábrica Java adicionais além do padrão connectionFactory, queueConnectionFactory e topicConnectionFactory.

Mais informações

Atributo	Descrição
Nome da configuração	*mid.property.jms.command.allowed_factory_names*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	Cadeia de caracteres
Valor padrão	*connectionFactory*, *queueConnectionFactory*, *topicConnectionFactory*
Valor recomendado	*connectionFactory*, *queueConnectionFactory*, *topicConnectionFactory*
Categoria	Controle de acesso
Risco à segurança	• Pontuação de gravidade: 4,1 • Pontuação do CVSS: média • Detalhes do risco à segurança: se o plug-in do MID Server (*com.glideapp.agent*) estiver ativo, analise a lista de nomes informados para a propriedade do MID *mid.property.jms.command.allowed_factory_names*. Certifique-se de que sejam necessários os nomes de fábrica adicionais além do padrão connectionFactory, queueConnectionFactory e topicConnectionFactory.
Dependências e pré-requisitos	Nenhum

Revisão das condições desnecessárias de controle de acesso a funções explícitas [Removido na Central de segurança 1.5]

Recomendamos o plug-in Funções explícitas para determinar que todos os usuários devem ter a função snc_internal para acessar recursos internos ou a função snc_external para acessar recursos externos.

Após a instalação desse plug-in, todos os usuários existentes recebem a função snc_internal, e as ACLs (access control lists, listas de controle de acesso) existentes são preenchidas com as condições da função. Devido à lógica de automação ou à intervenção de um administrador de instância, as funções snc_internal ou snc_external podem ser adicionadas incorretamente a uma ACL que já contém um requisito de função mais estrito. Como a avaliação da função da ACL é aprovada para qualquer usuário com uma função mapeada para uma ACL, a adição de snc_internal ou snc_external pode ser muito ampla para a finalidade pretendida de uma ACL. Isso pode causar o vazamento de dados se um usuário com poucos privilégios receber acesso pela ACL.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por exemplo, é desnecessário que as funções snc_internal e de administrador sejam mapeadas para a mesma ACL de uma tabela. A ACL deve conceder acesso a administradores. Nesse caso, a função snc_internal é um erro. Por outro lado, a ACL deve conceder acesso a todos os usuários snc_internal, o que torna a função de administrador desnecessária. Quando o plug-in Funções explícitas estiver instalado, analise as ACLs que contêm uma condição de função para snc_internal ou snc_external, além de uma condição para outra função. Se as funções funcionarem para um caso de uso específico, a descoberta deve ser analisada periodicamente.

Importante: Na próxima linha de base da proteção da GSI (versão 1.6), uma verificação chamada "Pacote de verificação de configuração de ACL de funções explícitas" substituirá a verificação anterior. Atualmente, a verificação pode resultar em muitas descobertas para revisão.

Mais informações

Atributo	Descrição
Nome da configuração	*com.glide.explicit_roles*, *sys_security_acl* e *sys_security_acl_role*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	Nenhum tipo de dados
Valor recomendado	Nenhum valor recomendado
Valor padrão	Nenhum valor padrão
Categoria	Controle de acesso
Risco à segurança	• Pontuação de gravidade: 4,2 • Pontuação do CVSS: média • Detalhes do risco à segurança: devido à automação ou à intervenção de um administrador de instância, as funções snc_internal ou snc_external podem ser adicionadas a uma ACL que já contém um requisito de função mais estrito. Como a avaliação da função da ACL é aprovada para qualquer usuário com uma função mapeada para uma ACL, a adição de qualquer função é muito ampla para a finalidade de uma ACL e pode causar o vazamento dos dados se um usuário com poucos privilégios receber acesso por ela.
Referências	Funções explícitas

Definição de usuário convidado para solicitações SOAP [Atualizado na Central de segurança 1.3]

Configure esta propriedade para controlar o nível de acesso de solicitações SOAP não autenticadas.

Esta propriedade controla o nível de acesso de solicitações SOAP não autenticadas. Se ela não estiver definida com o valor recomendado de *soap.guest* ou estiver definida para um usuário com privilégios limitados, as solicitações SOAP serão executadas em nome do usuário. Se esta propriedade estiver em branco, ela permitirá o acesso não autenticado às

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

operações no nível do administrador ou da manutenção, o que nega todos os controles de segurança na instância.

Mais informações

Atributo	Descrição
Nome da configuração	*com.glide.soap.guest_user*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	cadeia de caracteres
Valor recomendado	soap.guest
Valor-padrão	soap.guest
Categoria	Controle de acesso
Risco à segurança	• Pontuação de gravidade: 8,1 • Pontuação de CVSS: alta • Detalhes do risco à segurança: definir esta propriedade como em branco permite o acesso não autenticado às operações no nível do administrador ou da manutenção.
Dependências e pré-requisitos	Nenhum

Como ativar o plug-in Controle de acesso de SNC [Atualizado na Central de segurança 1.3]

Ative o plug-in SNC Access Control (com.snc.snc_access_control*com.snc.snc_access_control*) para controlar o acesso às suas instâncias pela equipe de Suporte e atendimento ao cliente.

A configuração padrão da Now Platform permite que Suporte e atendimento ao cliente acesse instâncias por meio de um processo interno que cria credenciais de suporte de curto prazo. Embora todo o acesso seja auditado, alguns clientes preferem controlar esse acesso.

Este plug-in permite que o Atendimento ao cliente e o Suporte proíbam funcionários da Suporte e atendimento ao cliente de acessar a instância. Esta decisão tem impacto nos ANSs de suporte porque você deve habilitar o acesso a Now Platform para que as atividades de suporte possam começar. Para saber mais, consulte ServiceNow controle de acesso.

Mais informações

Atributo	Descrição
Nome do Plug-in	*com.snc.snc_access_control*
Tipo de configuração	Definição do sistema > Plug-ins
Categoria	Controle de acesso
Finalidade	Proibir os funcionários de Suporte e atendimento ao cliente de acessar a instância

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Valor recomendado	Ativo
Valor padrão	Nenhum. Esse é um plug-in, não uma propriedade do Glide; portanto, não há valor padrão. O plug-in não é instalado por padrão.
Função necessária	O administrador cliente não pode ativar esse plug-in. Ele deve ser solicitado explicitamente porque ativar o plug-in requer privilégios elevados.
Classificação de risco de segurança	8,2
Impacto funcional	(Baixo) Se este plug-in estiver inativo, todos os funcionários de Suporte e atendimento ao cliente poderão acessar a instância do cliente. Habilitar o plug-in permite que o cliente restrinja o acesso apenas a funcionários autorizados de Suporte e atendimento ao cliente.
Risco à segurança	(Alta) Exposição desnecessária de acesso à instância para um grupo maior de pessoas.
Referências	ServiceNow controle de acesso

Etapas para configurar

1. Para solicitar o plug-in, siga as etapas em Ativar o controle do acesso ao ServiceNow. Os clientes devem solicitar o plug-in SNC Access Control (com.snc.snc_access_control) do HI.
2. Para habilitar o controle de acesso SNC, siga as etapas em Configurar o controle de acesso ao ServiceNow. Configure um registro de controle de acesso para especificar um ou mais funcionários de Suporte e atendimento ao cliente que tenham permissão para fazer login em sua instância.

API e serviço Web

A categoria API e serviço Web garante que as aplicações tenham autenticação, autorização e gestão de sessão apropriadas, validem todas as entradas que ultrapassam um limite de confiança e incluam controles de segurança para todos os tipos de API.

Os controles específicos nesta categoria tratam da validação de entrada por tipo de serviço, como validação de esquema XDS serviços web SOAP ou proteção de negação de serviço para APIs graphQL.

Validação do tipo de conteúdo SOAP [Atualizado na Central de segurança 1.3]

Use a propriedade *glide.soap.require_content_type_xml* para habilitar a validação de um tipo de conteúdo como texto/xml e proteger contra solicitações SOAP inválidas.

- Quando definida como **verdadeira**, Now Platform valida o tipo de conteúdo como texto/xml e protege contra solicitações SOAP inválidas.
- Se definida como **falsa**, qualquer valor de tipo de conteúdo será permitido.

⚠ **Aviso:** Esta é uma propriedade tipo porto seguro, o que significa que o valor não pode ser alterado após ser mudado. A reversão não é possível.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mais informações

Atributo	Descrição
Nome da propriedade	*glide.soap.require_content_type_xml*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Categoria	API e serviço Web
Finalidade	Proteger contra solicitações SOAP inválidas
Valor recomendado	verdadeiro
Valor-padrão	verdadeiro
Classificação de risco de segurança	8,8
Impacto funcional	(Baixo) Esta correção permite a validação do tipo de conteúdo SOAP para todas as solicitações SOAP de entrada. • Se você estiver usando um tipo de conteúdo diferente de texto/xml para solicitações de entrada, isso poderá causar falha nas transações SOAP. • Se você não estiver usando o tipo MIME correto, isso poderá interromper as integrações de terceiros.
Risco à segurança	(Moderado) Ao aceitar solicitações SOAP de entrada, a validação apropriada é realizada para garantir que o tipo de conteúdo relevante seja definido como parte da solicitação. Ela restringe as respostas SOAP inválidas que podem ser vistas como um risco à segurança.
Referência	Tipos de conteúdo

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Exigência de autorização para solicitações de pdf [Atualizado na Central de segurança 1.3]

Use a propriedade *glide.basicauth.required.pdf* para designar se as solicitações de PDF recebidas devem exigir autenticação básica.

Mais informações

⚠ **Aviso:** Esta é uma propriedade tipo porto seguro, o que significa que o valor não pode ser alterado após ser mudado. A reversão não é possível.

Atributo	Descrição
Nome da propriedade	*glide.basicauth.required.pdf*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Categoria	API e serviço Web
Finalidade	Impor autenticação básica em solicitações de PDF.
Valor recomendado	verdadeiro
Valor-padrão	verdadeiro
Classificação de risco de segurança	7,5
Impacto funcional	(Baixo) Esta correção impõe uma combinação de métodos de autenticação na forma de autenticação básica e controle de acesso no nível do sistema. • Ela executa essa autenticação ao recuperar dados de tabelas/páginas na forma de dados de PDF na instância. • Ela restringe todos os usuários convidados que estão acessando esses dados. Se for o caso, você poderá criar uma nova conta para usuários que precisam acessar o conteúdo com as permissões de controle de acesso necessárias. Para saber mais, consulte Conjuntos para importação de serviços web.
Risco à segurança	(Alto) Sem a autorização apropriada configurada nas solicitações de PDF recebidas, um usuário não autorizado pode obter acesso a conteúdo/dados confidenciais na instância de destino.

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Exigir autenticação no processador HTTP da Gestão de eventos [Novo na Central de segurança 1.3]

Saiba como estabelecer autenticação básica segura para solicitações de entrada do Amazon Simple Notification Service (SNS) quando o plug-in Gestão de eventos (*com.glideapp.itom.snac*) está habilitado.

Se a propriedade *glide.basicauth.required.evtmgmthttpprocessor* não estiver definida com o valor recomendado de **verdadeiro** e se o plug-in Gestão de eventos (*com.glideapp.itom.snac*) estiver ativo, a autenticação básica não será exigida para todas as solicitações de entrada do Amazon Simple Notification Service (SNS). Isso pode resultar em acesso não autenticado aos dados da instância.

Para corrigir este risco à segurança, certifique-se de que *glide.basicauth.required.evtmgmthttpprocessor* esteja definido como **verdadeiro** e de que *com.glideapp.itom.snac* esteja ativo.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mais informações

Atributo	Descrição
Nome da configuração	*glide.basicauth.required.evtmgmthttpprocessor*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	Booliano
Valor recomendado	verdadeiro
Valor-padrão	verdadeiro
Categoria	API e serviço Web
Risco à segurança	• Pontuação de gravidade: 7 • Pontuação de CVSS: alta • Detalhes do risco à segurança: não definir *glide.basicauth.required.evtmgmthttpprocessor* com o valor recomendado de "verdadeiro" e não ativar o plug-in *com.glideapp.itom.snac* faz com que a autenticação básica não seja habilitada para solicitações de entrada do SNS. Isso pode resultar em acesso não autenticado aos dados da instância.
Dependências e pré-requisitos	Nenhum
Referências	• https://docs.aws.amazon.com/sns/latest/dg/welcome.html • Controle de acesso
Impacto funcional	Se *glide.basicauth.required.evtmgmthttpprocessor* não estiver definido com o valor recomendado de "verdadeiro", e se o plug-in Gestão de eventos (com.glideapp.itom.snac) estiver ativo, a autenticação básica não será exigida para todas as solicitações de entrada do Amazon Web Services (SNS). Isso pode resultar em acesso não autenticado aos dados da instância.

Exigência de autorização para solicitações SOAP [Atualizado na Central de segurança 1.3 e 1.5]

Use a propriedade *glide.basicauth.required.soap* para designar se as solicitações SOAP recebidas devem exigir autorização básica.

Mais informações

⚠ **Aviso:** Esta é uma propriedade tipo porto seguro, o que significa que o valor não pode ser alterado após ser mudado. A reversão não é possível.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Nome da propriedade	*glide.basicauth.required.soapglide.soap.require_ws_secur*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Categoria	API e serviço Web
Finalidade	Impor autorização de solicitações SOAP
Valor recomendado	verdadeiro
Classificação de risco de segurança	8,1
Impacto funcional	(Médio) Esta correção impõe uma combinação de métodos de autenticação na forma de autenticação básica e controle de acesso no nível do sistema. • Ela executa essa autenticação ao recuperar dados de tabelas/páginas na forma de dados SOAP na instância. • Ela restringe todos os usuários convidados que estão acessando esses dados. • Crie uma conta para um usuário que precisa de acesso a este conteúdo com as permissões de controle de acesso necessárias. Para saber mais, consulte SOAP Web Service e Credenciais de autenticação de MID Server e solicitações SOAP.
Risco à segurança	(Médio) Sem a autorização apropriada configurada nas solicitações de fonte de dados SOAP, um usuário não autorizado pode obter acesso a conteúdo/ dados confidenciais na instância de destino.
Referências	Autenticação

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Exigir autorização para solicitações de descarregamento [Atualizado na Central de segurança 1.3]

Use a propriedade *glide.basicauth.required.unl* (useUnloadFormat) para designar se as solicitações de descarregamento recebidas devem exigir autenticação básica.

Mais informações

Atributo	Descrição
Nome da propriedade	*glide.basicauth.required.unl*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Categoria	API e serviço Web

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Finalidade	Impor autenticação básica em solicitações de descarregamento
Valor recomendado	verdadeiro
Classificação de risco de segurança	7,5
Impacto funcional	(Médio) Esta correção impõe uma combinação de métodos de autenticação na forma de autenticação básica e controle de acesso no nível do sistema. Ela executa essa autenticação ao recuperar dados de tabelas/páginas na forma de dados de descarregamento na instância.
Risco à segurança	(Alto) Sem a autorização apropriada configurada nas solicitações de fonte de dados de descarregamento, um usuário não autorizado pode obter acesso a conteúdo/dados confidenciais na instância de destino. Certifique-se de que *glide.basicauth.required.unl* exista em sys_properties_table e esteja definido como verdadeiro.
Referências	Autenticação

Exigir autorização para solicitações de CSV [Atualizado na Central de segurança 1.3]

Use a propriedade *glide.basicauth.required.csv* para designar se as solicitações de entrada de CSV (Comma-Separated Values, Valores separados por vírgula) devem exigir autenticação básica.

Mais informações

⚠ **Aviso:** Esta é uma propriedade tipo porto seguro, o que significa que o valor não pode ser alterado após ser mudado. A reversão não é possível.

Atributo	Descrição
Nome da propriedade	*glide.basicauth.required.csv*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Categoria	API e serviço Web
Finalidade	Impor autenticação básica em solicitações de CSV.
Valor recomendado	verdadeiro
Classificação de risco de segurança	7,5
Impacto funcional	(Baixo) Esta correção impõe uma combinação de métodos de autenticação na forma de autenticação básica e controle de acesso no nível do sistema.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
	• Ela executa essa autenticação ao recuperar dados de tabelas/páginas na forma de dados CSV na instância. • Ela restringe todos os usuários convidados que estão acessando esses dados. Se for o caso, você poderá criar uma nova conta para usuários que precisam acessar o conteúdo com as permissões de controle de acesso necessárias. Para saber mais, consulte Recuperar dados de um arquivo no formato CSV.
Risco à segurança	(Alto) Sem a autorização apropriada configurada nas solicitações de CSV de entrada, um usuário não autorizado pode obter acesso a conteúdo e dados confidenciais na instância de destino. Certifique-se de que *glide.basicauth.required.csv* exista na tabela sys_properties e esteja definido como verdadeiro.
Referências	Segurança de serviços da Web

Exigir autorização para solicitações do Excel [Atualizado na Central de segurança 1.3]

Use a propriedade *glide.basicauth.required.excel* para designar se as solicitações de Excel recebidas devem exigir autenticação básica.

Mais informações

⚠ **Aviso:** Esta é uma propriedade tipo porto seguro, o que significa que o valor não pode ser alterado após ser mudado. A reversão não é possível.

Atributo	Descrição
Nome da propriedade	*glide.basicauth.required.excel*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Categoria	API e serviço Web
Finalidade	Impor autenticação básica em solicitações de Excel.
Valor recomendado	verdadeiro
Classificação de risco de segurança	7,5
Impacto funcional	(Baixo) Esta correção impõe uma combinação de métodos de autenticação na forma de autenticação básica e controle de acesso no nível do sistema. • Ela executa essa autenticação ao recuperar dados de tabelas/páginas na forma de dados de Excel na instância. • Ela restringe todos os usuários convidados que estão acessando esses dados. Se for o caso, você

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
	poderá criar uma nova conta para usuários que precisam acessar o conteúdo com as permissões de controle de acesso necessárias.
Risco à segurança	(Alto) Sem a autorização apropriada configurada nas solicitações de Excel recebidas, um usuário não autorizado pode obter acesso a conteúdo/dados confidenciais na instância de destino.

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Exigir autorização para solicitações de importação [Atualizado na Central de segurança 1.3]

Use a propriedade *glide.basicauth.required.importprocessor* para designar se as solicitações de importação recebidas devem exigir autenticação básica.

Mais informações

Aviso: Esta é uma propriedade tipo porto seguro, o que significa que o valor não pode ser alterado após ser mudado. A reversão não é possível.

Atributo	Descrição
Nome da propriedade	*glide.basicauth.required.importprocessor*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Categoria	API e serviço Web
Finalidade	Impor autenticação básica em solicitações de importação.
Valor recomendado	verdadeiro
Classificação de risco de segurança	5,3
Impacto funcional	(Baixo) Esta correção impõe uma combinação de métodos de autenticação na forma de autenticação básica e controle de acesso no nível do sistema. • Ela executa essa autenticação ao importar fontes de dados para as tabelas/páginas de instância. • Ela restringe todos os usuários convidados que estão acessando esses dados. Se for o caso, você poderá criar uma nova conta para usuários que precisam acessar o conteúdo com as permissões de controle de acesso necessárias. Para saber mais, consulte Recuperar dados de um arquivo no formato CSV.
Risco à segurança	(Moderado) Sem a autorização apropriada configurada nas solicitações de importação da fonte de dados, um usuário não autorizado pode obter

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
	acesso a conteúdo/dados confidenciais na instância de destino.
Referências	Segurança de serviços web SOAP Serviço web SOAP

Exigir autorização para solicitações JSONv2 [Atualizado na Central de segurança 1.3]

Use a propriedade *glide.basicauth.required.jsonv2* para designar se as solicitações de JSONv2 recebidas devem exigir autorização básica.

Mais informações

Aviso: Esta é uma propriedade tipo porto seguro, o que significa que o valor não pode ser alterado após ser mudado. A reversão não é possível.

Atributo	Descrição
Nome da propriedade	*glide.basicauth.required.jsonv2*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Categoria	API e serviço Web
Finalidade	Impor autorização de solicitações de JSONv2
Classificação de risco de segurança	7,5
Valor recomendado	verdadeiro
Impacto funcional	(Médio) Esta correção impõe uma combinação de métodos de autenticação na forma de autenticação básica e controle de acesso no nível do sistema. • Ela executa essa autenticação ao recuperar dados de tabelas/páginas na forma de dados JSON na instância. • Ela restringe todos os usuários convidados que estão acessando esses dados. • Crie uma conta para um usuário que precisa de acesso a este conteúdo com as permissões de controle de acesso necessárias. Para saber mais, consulte Serviço Web JSONv2 Serviço Web JSONv2.
Risco à segurança	(Alto) Sem autorização apropriada configurada nas solicitações JSON da fonte de dados, um usuário não autorizado pode acessar conteúdo/dados confidenciais na instância de destino.
Referências	Autenticação Requer autenticação básica para solicitações de JSONv2 recebidas

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exigir autorização para solicitações de WSDL [Atualizado na Central de segurança 1.3]

Use a propriedade *glide.basicauth.required.wsdl* para designar se as solicitações de WSDL (Web Services Description Language, Linguagem descritiva de Web Services) recebidas devem exigir autenticação básica.

Nota: Se optar por não exigir autenticação básica para solicitações de WSDL recebidas, você deverá modificar as regras de controle de acesso (ACL) para permitir que usuários convidados acessem o conteúdo de WSDL.

Mais informações

Aviso: Esta é uma propriedade tipo porto seguro, o que significa que o valor não pode ser alterado após ser mudado. A reversão não é possível.

Atributo	Descrição
Nome da propriedade	*glide.basicauth.required.wsdl*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Categoria	API e serviço Web
Finalidade	Impor autenticação básica em solicitações de WSDL.
Valor recomendado	verdadeiro
Classificação de risco de segurança	4,3
Impacto funcional	(Baixo) Esta correção impõe uma combinação de métodos de autenticação na forma de autenticação básica e controle de acesso no nível do sistema. • Ela executa essa autenticação ao recuperar dados de tabelas/páginas na forma de dados de WSDL na instância. • Ela restringe todos os usuários convidados que estão acessando esses dados. Se for o caso, você poderá criar uma nova conta para usuários que precisam acessar o conteúdo com as permissões de controle de acesso necessárias.
Risco à segurança	(Médio) Sem a autorização apropriada configurada nos serviços Web WSDL, um usuário não autorizado pode obter acesso a conteúdo/dados confidenciais WSDL na instância de destino.
Referências	Segurança de serviços da Web

Exigência de autorização para solicitações XML [Atualizado na Central de segurança 1.3]

Use a propriedade *glide.basicauth.required.xml* para designar se as solicitações de XML recebidas devem exigir autenticação básica.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mais informações

Aviso: Esta é uma propriedade tipo porto seguro, o que significa que o valor não pode ser alterado após ser mudado. A reversão não é possível.

Atributo	Descrição
Nome da propriedade	*glide.basicauth.required.xml*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Categoria	API e serviço Web
Finalidade	Impor autenticação básica em solicitações de XML.
Classificação de risco de segurança	7,5
Valor recomendado	verdadeiro
Impacto funcional	(Baixo) Esta correção impõe uma combinação de métodos de autenticação na forma de autenticação básica e controle de acesso no nível do sistema. • Ela executa essa autenticação ao recuperar dados de tabelas/páginas na forma de dados de XML na instância. • Ela restringe todos os usuários convidados que estão acessando esses dados. Se for o caso, você poderá criar uma nova conta para usuários que precisam acessar o conteúdo com as permissões de controle de acesso necessárias. Para saber mais, consulte Etapa do analisador de XML.
Risco à segurança	(Alto) Sem a autorização apropriada configurada nas solicitações XML recebidas, um usuário não autorizado pode obter acesso a conteúdo/dados confidenciais na instância de destino.
Referências	Autenticação

Exigir autorizações para solicitações de saída de XML

Configure esta propriedade para que a autorização básica seja necessária para todas as solicitações de entrada de XMLOutputProcessor.

Se a propriedade *glide.basicauth.required.xmloutputprocessor* não estiver definida com o valor recomendado de **verdadeiro**, a autorização básica não será necessária para solicitações de entrada de XMLOutputProcessor. Isso pode levar à divulgação de informações não autenticadas da instância.

Aviso: Esta é uma propriedade tipo porto seguro, o que significa que o valor não pode ser alterado após ser mudado. A reversão não é possível.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mais informações

Atributo	Descrição
Nome da configuração	*glide.basicauth.required.xmloutputprocessor*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	booliano
Valor recomendado	verdadeiro
Valor-padrão	verdadeiro
Categoria	API e serviço Web
Risco à segurança	• Pontuação de gravidade: 7,5 • Pontuação de CVSS: alta • Detalhes do risco à segurança: não definir a propriedade com o valor recomendado de **verdadeiro** pode levar ao vazamento de informações confidenciais da instância.
Dependências e pré-requisitos	Nenhum

Exigir autorização para solicitações de XSD

Use a propriedade *glide.basicauth.required.xsd* para designar se as solicitações de XSD (XML Schema Definition, Definição de esquema XML) recebidas devem exigir autenticação básica.

Mais informações

⚠ **Aviso:** Esta é uma propriedade tipo porto seguro, o que significa que o valor não pode ser alterado após ser mudado. A reversão não é possível.

Atributo	Descrição
Nome da propriedade	glide.basicauth.required.xsd *glide.basicauth.required.xsd*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Categoria	API e serviço Web
Finalidade	Impor autenticação básica em solicitações de XSD.
Valor recomendado	verdadeiro
Classificação de risco de segurança	5,3
Impacto funcional	(Baixo) Esta correção impõe uma combinação de métodos de autenticação na forma de autenticação básica e controle de acesso no nível do sistema.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
	• Ela executa essa autenticação ao recuperar dados de tabelas/páginas na forma de dados de XSD na instância. • Ela restringe todos os usuários convidados que estão acessando esses dados. Se for o caso, você poderá criar uma nova conta para usuários que precisam acessar o conteúdo com as permissões de controle de acesso necessárias. Para saber mais, consulte Sessões não interativas.
Risco à segurança	(Moderado) Sem a autorização apropriada configurada nas solicitações XSD recebidas, um usuário não autorizado pode obter acesso a conteúdo/dados confidenciais na instância de destino.
Referências	Autenticação

Exigir autorização para solicitações de script

Use a propriedade *glide.basicauth.required.scriptedprocessor* para designar se as solicitações de script recebidas devem exigir autenticação básica.

Mais informações

Aviso: Esta é uma propriedade tipo porto seguro, o que significa que o valor não pode ser alterado após ser mudado. A reversão não é possível.

Atributo	Descrição
Nome da propriedade	*glide.basicauth.required.scriptedprocessor*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Categoria	API e serviço Web
Finalidade	Impor autenticação básica em solicitações de script.
Valor recomendado	verdadeiro
Classificação de risco de segurança	7,2
Impacto funcional	(Médio) Esta correção impõe a autenticação na forma de autorização básica. • Ela executa essa autenticação ao processar solicitações de script na instância. • Ela restringe todos os usuários convidados que estão acessando esses dados. Se for o caso, você poderá criar uma nova conta para usuários que precisam acessar o conteúdo com as permissões de controle de acesso necessárias.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Risco à segurança	(Alto) Sem a autorização apropriada configurada nas solicitações de script recebidas, um usuário não autorizado pode obter acesso a conteúdo/dados confidenciais na instância de destino.
Referências	Autenticação

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Exigir autorização para solicitações SCHEMA [Atualizado na Central de segurança 1.3]

Use a propriedade *glide.basicauth.required.schema* para exigir autorização básica para todas as solicitações do Processador Schema de tabela de entrada.

O Processador Schema de tabela de entrada lida com solicitações de esquema recebidas para a plataforma.

Defina *glide.basicauth.required.schema* com o valor recomendado **verdadeiro** para exigir autorização básica para todas as solicitações do Processador Schema de tabela de entrada. Defina o valor como **falso** para exigir autorização básica para todas as solicitações do Processador Schema de tabela de entrada.

Aviso: Esta é uma propriedade tipo porto seguro, o que significa que o valor não pode ser alterado após ser mudado. A reversão não é possível.

Mais informações

Atributo	Descrição
Nome da propriedade	*glide.basicauth.required.schema*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Categoria	API e serviço Web
Finalidade	Exigir autorização básica para todas as solicitações do Processador Schema de tabela de entrada.
Valor recomendado	Verdadeiro (valor padrão)
Tipo de configuração	Booliano
Risco à segurança	(Moderado) Omitir a autenticação deste processador levará ao acesso não autenticado aos dados da instância.

Exigir autorização para solicitações de RSS [Atualizado na Central de segurança 1.3]

Use a propriedade *glide.basicauth.required.rss* para designar se as solicitações de RSS recebidas devem exigir autenticação básica.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mais informações

Aviso: Esta é uma propriedade tipo porto seguro, o que significa que o valor não pode ser alterado após ser mudado. A reversão não é possível.

Atributo	Descrição
Nome da propriedade	*glide.basicauth.required.rss*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Categoria	API e serviço Web
Finalidade	Impor autenticação básica em solicitações de RSS.
Valor recomendado	verdadeiro
Classificação de risco de segurança	7,5
Impacto funcional	(Baixo) Esta correção impõe uma combinação de métodos de autenticação na forma de autenticação básica e controle de acesso no nível do sistema. • Ela executa essa autenticação ao processar solicitações de RSS na instância. • Ela restringe todos os usuários convidados que estão acessando esses dados. Se for o caso, você poderá criar uma nova conta para usuários que precisam acessar o conteúdo com as permissões de controle de acesso necessárias. Para saber mais, consulte Gerador de feed RSS.
Risco à segurança	(Alto) Sem a autorização apropriada configurada nas solicitações de RSS recebidas, um usuário não autorizado pode obter acesso a conteúdo/dados confidenciais na instância de destino.
Referências	Autenticação básica RSS

Exigir autorização para solicitações de API [Atualizado na Central de segurança 1.3]

Use a propriedade *glide.basicauth.required.api* para aprimorar a segurança de autorização básica para solicitações REST de entrada.

Defina a propriedade *glide.basicauth.required.api* como **verdadeira** para exigir autorização para todas as solicitações REST. Defina a propriedade como **falsa** para ignorar autorização para todas as solicitações REST.

Aviso: Esta é uma propriedade tipo porto seguro, o que significa que o valor não pode ser alterado após ser mudado. A reversão não é possível.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mais informações

Atributo	Descrição
Nome da propriedade	*glide.basicauth.required.api*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Categoria	API e serviço Web
Finalidade	Autorização básica para solicitações REST de entrada.
Valor recomendado	Verdadeiro (padrão)
Tipo de configuração	Cadeia de caracteres
Risco à segurança	(Alto) Se "glide.basicauth.required.api" não estiver definido com o valor recomendado "verdadeiro", isso desabilitará a autenticação básica na solicitação de API e levará ao acesso não autenticado aos dados da instância.
Classificação de risco de segurança	8,6

Arquitetura, design e modelagem de ameaças

Este controle amplo aborda considerações de design de alto nível e elementos-chave para implementar uma aplicação segura. Ele cobre os locatários de disponibilidade, integridade de processamento de confidencialidade, não repúdio e privacidade. Além disso, elementos de um ciclo de vida de desenvolvimento de software seguro estão incluídos.

Autenticação baseada em certificado não imposta [Novo na Central de segurança 1.3]

A propriedade *glide.authenticate.mutual.enabled* habilita a autenticação baseada em certificados, um tipo de autenticação mútua para conexões REST de entrada com as APIs REST e SOAP na Now Platform.

A autenticação mútua estabelece confiança entre o servidor e o cliente por meio da troca de certificados SSL (Secure Socket Layer, Camada de soquetes seguros) para validar o certificado com uma autoridade de certificação confiável. Isso permite verificar se uma fonte confiável está se conectando à Now Platform. Se esta instância não estiver definida com o valor recomendado de verdadeiro, uma instância poderá ficar vulnerável a ataques de intermediários (MitM, man-in-the-middle).

Para remediar esta ameaça de segurança, habilite a autenticação mútua para serviços da web de entrada. Se esta for a primeira vez que você instala o plug-in de autenticação baseada em certificados *com.glide.auth.mutual)* para Now Platform, siga as instruções Como configurar autenticação baseada em certificados. Além disso, certifique-se de que a propriedade *glide.authenticate.mutual.enabled* esteja definida como verdadeira para ativar o plug-in.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mais informações

Atributo	Descrição
Nome da configuração	*glide.authenticate.mutual.enabled*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	booliano
Valor recomendado	verdadeiro
Valor-padrão	verdadeiro
Categoria	Arquitetura, design e modelagem de ameaças
Risco à segurança	• Pontuação de gravidade: 5,3 • Pontuação do CVSS: média • Detalhes do risco de segurança: Se esta propriedade não estiver configurada com o valor recomendado de verdadeiro, a autenticação baseada em certificados não validará certificados com uma Autoridade de Certificação confiável. Isso aumenta as chances de um agente mal-intencionado atacar uma instância usando ataques MitM.
Dependências e pré-requisitos	Nenhum
Referências	• https://csrc.nist.gov/glossary/term/man_in_the_middle_attack • Autenticação baseada em certificados • Configurar autenticação mútua

Verificação da representação na avaliação de ACL no app de RH [Novo na Central de segurança 1.3 e atualizado na 1.5]

Use a propriedade *sn_hr_core.impersonateCheck* para impedir que um usuário represente outro usuário e acesse as informações de RH dele.

Uma configuração segura evita que um administrador veja as informações de RH de outro usuário enquanto estiver usando a representação. Uma configuração insegura para esta propriedade permite que um administrador represente um usuário e acesse dados de RH, como resultados de pesquisa ou registros de auditoria, com o acesso do usuário representado. Devido à natureza desse tipo de dados (por exemplo, informações que devem estar disponíveis somente para o próprio usuário, como e-mail), isso não é recomendado. Definir *sn_hr_core.impersonateCheck* como verdadeiro só permite o acesso às informações de RH quando o usuário não está representando outras pessoas.

Mais informações

Atributo	Descrição
Nome da configuração	*sn_hr_core.impersonateCheck*

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	booliano
Valor recomendado	verdadeiro
Valor-padrão	falso
Categoria	Arquitetura, design e modelagem de ameaças
Risco à segurança	• Pontuação de gravidade: 2,7 • Pontuação de CVSS: baixa • Detalhes do risco à segurança: uma configuração insegura para esta propriedade permite que um administrador represente um usuário e acesse dados de RH, como resultados de pesquisa ou registros de auditoria, com o acesso do usuário representado.
Dependências e pré-requisitos	Nenhum(a)
Impacto funcional	Quando esta propriedade está definida com verdadeira, ela evita que um administrador veja as informações de RH de outro usuário enquanto estiver usando a representação. Quando definida como falsa, ela permite que um administrador represente um usuário e acesse dados de RH, como resultados de pesquisa ou registros de auditoria, com o acesso do usuário representado. Devido à natureza desse tipo de dados (por exemplo, informações que devem estar disponíveis somente para o próprio usuário, como e-mail), isso não é recomendado. Definir sn_hr_core.impersonateCheck como verdadeiro só permite o acesso às informações de RH quando o usuário não está representando outras pessoas.

Desabilitar relatórios publicados não autenticados

Desative esta propriedade para impedir que o usuário publique ou acesse relatórios. Esta propriedade desabilita o recurso de emissão de relatórios publicados em relatórios.

Habilite a publicação de relatórios definindo *glide.report.published_reports.enabled* como **verdadeiro**.

Impor segurança em relatórios é compatível se *glide.report.published_reports.enabled* estiver definido como **falso**.

Mais informações

Atributo	Descrição
Nome da propriedade	*glide.report.published_reports.enabled*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Categoria	Arquitetura, design e modelagem de ameaças

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Finalidade	Desabilitar o recurso de emissão de relatórios publicados em relatórios.
Tipo	verdadeiro | falso
Valor recomendado	**falso**
Classificação de risco de segurança	6,5
Impacto funcional	(Médio) O usuário não pode publicar relatórios.
Risco à segurança	(Moderado) Se esta propriedade não estiver habilitada, os usuários poderão acessar ou publicar relatórios expondo dados confidenciais. Publicar um relatório cria um URL que qualquer pessoa pode usar para acessar o relatório, incluindo pessoas que não são usuários. Quando alguém navega até o URL, o relatório é gerado com os dados atuais da instância.
Referências	Publicar um relatório

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Impor ACLs de campo para solicitações de consulta de entrada

Gerencie como as consultas de entrada são validadas em sua instância.

Use a propriedade *glide.report.report_view.check_published* para verificar como as consultas de entrada são validadas em sua instância. Se a propriedade estiver definida com o valor recomendado **verdadeiro**, as ACLs de campo serão verificadas em relação às consultas de entrada e rejeitadas se o usuário não for autorizado. Se a propriedade for definida como **falsa**, as ACLs não serão verificadas em relação às consultas de entrada e continuarão sendo executadas, o que pode levar à divulgação de informações para partes não autorizadas.

Mais informações

Atributo	Descrição
Nome da configuração	*glide.export.query.enforce_field_acl*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	booliano
Valor recomendado	verdadeiro
Valor-padrão	verdadeiro
Categoria	Arquitetura, design e modelagem de ameaças
Risco à segurança	• Pontuação de gravidade: 4,4 • Pontuação do CVSS: média

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
	• Detalhes do risco à segurança: se a propriedade for definida como **falsa**, as ACLs não serão verificadas em relação às consultas de entradas, o que pode levar à divulgação de informações.
Dependências e pré-requisitos	Nenhum

Impor ACLs de leitura em exibições de relatório

Gerencie como as ACLs de leitura são aplicadas em sua instância.

Use a propriedade *glide.report.report_view.read_acl* para impor a ACL de leitura (nível de tabela) em funções de emissão de relatórios quando não houver ACL de exibição de relatório na tabela ou no campo. Se essa propriedade não estiver definida para **impor**, as ACLs poderão ser ignoradas, levando ao vazamento de informações confidenciais.

Mais informações

Atributo	Descrição
Nome da configuração	*glide.report.report_view.read_acl*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	cadeia de caracteres
Valor recomendado	impor
Valor-padrão	impor
Categoria	Arquitetura, design e modelagem de ameaças
Risco à segurança	• Pontuação de gravidade: 7,1 • Pontuação de CVSS: alta • Detalhes do risco à segurança: não definir essa propriedade como **impor** pode fazer com que as ACLs sejam ignoradas.
Dependências e pré-requisitos	Nenhum

Como definir endereços IP internos permitidos da ServiceNow [Atualizado na Central de segurança 1.3 e 1.5]

Use a propriedade *glide.ip.authenticate.strict* para especificar intervalos de IP que podem fazer conexões de entrada em uma instância.

Se *glide.ip.authenticate.strict* estiver definido como verdadeiro, somente os intervalos de IP especificados no *glide.ip.authenticate.allow.secured* poderão fazer conexões de entrada em uma instância. Esta propriedade contém uma lista somente dos intervalos de IP internos essenciais da ServiceNow (Secure VPN, DC).

Se *glide.ip.authenticate.allow.secured* não estiver definido com o valor recomendado de "`10.0.0.0/8`, `37.98.232.0/21`, `103.23.64.0/22`, `149.96.0.0/17`, `149.96.0.0/16`, `199.91.136.0/21`, `148.139.0.0/16`, `127.0.0.1`, `0:0:0:0:0:0:0:1`",

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

poderá permitir que fontes não confiáveis fora do DataCenter da ServiceNow e VPN segura acessem pontos de extremidade de monitoramento confidenciais em instâncias.

Aviso: O valor desta propriedade é uma substituição sem banco de dados. Não pode ser alterado ou substituído.

Mais informações

Atributo	Descrição
Nome da propriedade	*glide.ip.authenticate.strict*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Categoria	Arquitetura, design e modelagem de ameaças
Finalidade	Permitir que os funcionários da ServiceNow acessem a instância somente por meio de um conjunto seguro de intervalos de IP
Valor recomendado	verdadeiro
Classificação de risco de segurança	4,3
Impacto funcional	(Baixo) Se esta propriedade não estiver habilitada, os funcionários da ServiceNow poderão acessar a instância do cliente por meio de todos os intervalos de IP. Habilitar a propriedade restringe o acesso a um conjunto seguro de intervalos de IP (Secure VPN, DC). **Nota:** Se você definir esta propriedade como `verdadeira`, o Now Platform usará uma propriedade *glide.ip.authenticate.allow.secured* mais restritiva em vez da propriedade de restrição de IP de monitoramento de desempenho (*glide.ip.authenticate.allow.secured*) para um conjunto de intervalos de IP que possam acessar a instância.
Risco à segurança	(Baixo) Exposição desnecessária de acesso à instância para um grupo maior de pessoas.
Referência	Autenticação baseada no intervalo de IP

Nota: Uma regra de negar tudo é necessária para ser adicionada ao controle de acesso IP para restringir o acesso de qualquer IP não adicionado ao controle de acesso IP. Todos os IPs permitidos necessários devem ser adicionados ao controle de acesso IP.

Desativação do comportamento legado de JQuery [Atualizado na Central de segurança 1.3]

O *glide.jquery.legacy* é usado para impedir que versões pré-patch mais antigas do JQuery sejam usadas, o que introduzirá vulnerabilidades sem patch na biblioteca.

Defina *glide.jquery.legacy* com o valor recomendado **falso** para impedir que versões pré-patch mais antigas do JQuery sejam usadas, o que introduzirá vulnerabilidades sem

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

patch na biblioteca. Defina o valor como **verdadeiro** para permitir versões pré-patch do JQuery.

Mais informações

Atributo	Descrição
Nome da propriedade	*glide.jquery.legacy*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Categoria	Arquitetura, design e modelagem de ameaças
Finalidade	Prevenir possíveis riscos de segurança decorrentes de ataques a vulnerabilidades descobertas em versões desatualizadas da biblioteca do JQuery.
Valor recomendado	Falso
Tipo de configuração	Booliano
Risco à segurança	(Alto) Impede que versões pré-patch mais antigas do JQuery sejam usadas, o que introduzirá vulnerabilidades sem patch na biblioteca. A propriedade do sistema é à prova de falhas caso alguma organização dependa das versões sem patch do AngularJS para executar suas implementações personalizadas.
Classificação de risco de segurança	7,1

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Como desativar o comportamento legado de limitação do escopo do GlideRecord [Novo na Central de segurança 1.3]

A propriedade *glide.record.legacy_cross_scope_access_policy_in_script* desabilita a limitação de escopo, permitindo que as aplicações com escopo acessem interfaces de script global. Ele foi criado como um patch para o acesso entre escopos do GlideRecord.

O GlideRecord fornece acesso de criação e atualização de escopo cruzado para tabelas que não foram configuradas com esse nível de acesso. A propriedade *glide.record.legacy_cross_scope_access_policy_in_script* foi criada para impedir a interrupção de aplicações de clientes legados quando esse comportamento de acesso com escopo fosse corrigido. Quando esta propriedade é definida como verdadeira, o acesso entre escopos retorna ao comportamento legado, que é inseguro.

Essa propriedade desativa a limitação de escopo, permitindo que os apps com escopo acessem interfaces globais de script. A imposição da limitação de escopo garante que as aplicações só possam acessar recursos que estão no seu escopo designado ou aos quais elas receberam acesso explicitamente. Isso, por sua vez, aplica o princípio do menor privilégio.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mais informações

Atributo	Descrição
Nome da configuração	*glide.record.legacy_cross_scope_access_policy_in_script*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	booliano
Valor recomendado	falso
Valor padrão	verdadeiro (quando a propriedade não existe na tabela sys_properties.)
Categoria	Arquitetura, design e modelagem de ameaças
Risco à segurança	• Pontuação de gravidade: 5 • Pontuação do CVSS: média • Detalhes do risco à segurança: a definição de escopo garante que as aplicações só possam acessar recursos com acesso explícito ou dentro de seu escopo, seguindo o princípio do menor privilégio. Desabilitar este recurso pode causar impactos na confidencialidade, disponibilidade e integridade.
Dependências e pré-requisitos	Nenhum

Desabilitar o comportamento do AngularJS legado [Atualizado na Central de segurança 1.3]

Use a propriedade *glide.angular.legacy* para se proteger contra possíveis riscos de segurança decorrentes de ataques a vulnerabilidades descobertas em versões desatualizadas da biblioteca do AngularJS.

Defina *glide.angular.legacy* com o valor recomendado **falso** para impedir que versões pré-patch mais antigas do AngularJS sejam usadas. Defina a propriedade como **verdadeira** para usar versões pré-patch mais antigas do AngularJS.

Mais informações

Atributo	Descrição
Nome da propriedade	*glide.angular.legacy*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Categoria	Arquitetura, design e modelagem de ameaças
Finalidade	A propriedade do sistema é à prova de falhas caso alguma organização dependa das versões sem patch do angularJS para executar suas implementações personalizadas.
Valor recomendado	Falso
Tipo de configuração	Booliano

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Risco à segurança	(Alto) Usar versões antigas do AngularJS pode trazer riscos de segurança decorrentes de ataques a vulnerabilidades descobertas em versões desatualizadas da biblioteca do AngularJS.
Classificação de risco de segurança	7,1

Exigir autorização da REST API do agente de dados [Atualizado na Central de segurança 1.3]

Use a propriedade *glide.basicauth.required.databrokerrestapiprocessor* para exigir autorização básica para todas as solicitações de entrada da REST API do agente de dados.

Se esta propriedade for definida como **verdadeira**, a autorização será aplicada. Se for definida como **falsa**, nenhuma autorização será usada, o que pode levar ao vazamento de informações confidenciais de sua instância.

⚠ **Aviso:** Esta é uma propriedade tipo porto seguro, o que significa que o valor não pode ser alterado após ser mudado. A reversão não é possível.

Mais informações

Atributo	Descrição
Nome da configuração	*glide.basicauth.required.databrokerrestapiprocessor*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	booliano
Valor recomendado	verdadeiro
Valor-padrão	verdadeiro
Categoria	Arquitetura, design e modelagem de ameaças
Risco à segurança	• Pontuação de gravidade: 8,6 • Pontuação de CVSS: alta • Detalhes do risco à segurança: se a propriedade for definida como **falsa**, a autenticação de API não será aplicada, permitindo que um agente mal-intencionado acesse dados confidenciais.
Dependências e pré-requisitos	Nenhum

Como negar por padrão com ACLs vazias [Atualizado na Central de segurança 1.3]

Use a propriedade *glide.sm.default_mode* para controlar o comportamento padrão do gerenciador de segurança quando ele descobrir que as regras de ACL existentes fazem parte das regras de ACL da tabela curinga.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Quando o plug-in Configurações de Alta Segurança (com.glide.high_security) é ativado durante a instalação da instância inicial, ele cria esta propriedade e as regras de ACL curinga passam a existir. Para fornecer acesso baseado em função a tabelas do sistema, estas regras controlam um número significativo de ACLs e operações baseadas em registro mais comuns:

- Leitura
- Gravar
- Criar
- Excluir

A menos que você use o plug-in Alta segurança com a opção de negação padrão habilitada, muitas tabelas não serão protegidas. O Now Platform usa um modelo de segurança de negação padrão que evita que usuários não administradores acessem objetos, a menos que atendam a uma regra de ACL correspondente. Usar este modelo remove muitos vetores de ataque, como scripts não seguros.

Aviso: Esta é uma propriedade tipo porto seguro, o que significa que o valor não pode ser alterado após ser mudado. A reversão não é possível.

Mais informações

Atributo	Descrição
Nome da propriedade	*glide.sm.default_mode*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Categoria	Arquitetura, design e modelagem de ameaças
Finalidade	A prática recomendada de segurança é restringir um acesso às tabelas por um usuário não autorizado. • Se não houver regras de ACL em vigor para tabelas, esta propriedade garantirá que pelo menos ACLs curinga sejam validadas para qualquer operação CRUD realizada na tabela/campo. • Essas regras restringem as operações de leitura, gravação, criação e exclusão em todas as tabelas, a menos que o usuário tenha a função de administrador ou atenda aos requisitos de outra regra de ACL de tabela.
Valor recomendado	negar
Impacto funcional	(Alto) Se você definir esta propriedade como **Permitir**, as regras de ACL da tabela curinga permitirão operações CRUD em todas as tabelas, a menos que haja regras de ACL de tabela específicas para restringir essas operações. **Nota:** Este plug-in não é destinado a instâncias existentes, já que pode modificar o acesso de segurança a tabelas já em uso em um ambiente de produção.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Risco à segurança	8,8
Referências	Propriedade de negação padrão

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Autenticação

A categoria de autenticação cobre os principais elementos da autenticação moderna para confirmar que uma entidade e suas declarações são autênticas e corretas, resistentes à representação e impedem a interceptação de senhas.

O padrão ASVS é baseado na especificação NIST 800-63b (https://pages.nist.gov/800-63-3/sp800-63b.html) para esta seção.

A autenticação inclui política de senha, controles e armazenamento, implementação apropriada de autenticadores e implementação apropriada de verificadores fora de banda ou únicos.

Ativação da autenticação multifator baseada em função [Atualizado na Central de segurança 1.3]

Use a propriedade *glide.authenticate.multifactor* para impor a MFA (multi-factor authentication, autenticação multifator) baseada em função para todos os usuários atribuídos a funções específicas.

Imponha autenticação multifator com base nas funções atribuídas ao usuário. Se um usuário tiver sido atribuído à função "admin", "security_admin" ou "user_admin" na lista de funções multifator, a MFA será aplicada

- Defina essa propriedade como **verdadeira** para impor a autenticação multifator baseada em função a todos os usuários atribuídos a funções específicas.
- Defina essa propriedade como **falsa** para impor a autenticação multifator baseada em função a todos os usuários atribuídos a funções específicas.

Mais informações

Atributo	Descrição
Nome da propriedade	*glide.authenticate.multifactor*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Categoria	Autenticação
Finalidade	Impor a autenticação multifator baseada em função a todos os usuários atribuídos a funções específicas.
Tipo	verdadeiro/falso
Valor recomendado	*verdadeiro*
Dependências de segurança	Ativar **Autenticação multifator baseada em função** junto à tabela **Critérios de multifator**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Classificação de risco de segurança	7,2
Impacto funcional	(Médio) Habilitar esta propriedade melhora a experiência do usuário. Ela atua como uma camada extra de proteção e segurança contra credenciais comprometidas.
Risco à segurança	(Moderado) Se esta propriedade não estiver habilitada, há um risco de acesso não autorizado a dados confidenciais.
Referências	Configuração dos critérios multifatores baseados em função

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Como habilitar a recuperação de conta [Atualizado na Central de segurança 1.3 e 1.5]

A propriedade *glide.sso.acr.enabled* controla o recurso de recuperação de conta.

Defina *glide.sso.acr.enabled* com o valor recomendado de **verdadeiro** para permitir a recuperação de conta por ID de usuário. Defina o valor como **falso** para não permitir a recuperação de conta por ID de usuário.

Mais informações

Atributo	Descrição
Nome da propriedade	*glide.sso.acr.enabled*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Categoria	Autenticação
Finalidade	Controlar o recurso de recuperação de conta por id de usuário.
Valor recomendado	Verdadeiro (padrão)
Tipo de configuração	Booliano
Risco à segurança	(Crítico) Sem esta propriedade habilitada, os usuários não terão permissão para recuperar suas contas por ID de usuário.
Classificação de risco de segurança	9,1
Referências	Consulte Recuperação de conta (ACR) para obter informações adicionais.

Como exigir a ofuscação da IU clássica do aplicativo para celular [Atualizado na Central de segurança 1.3]

Use a propriedade *glide.ui.m.blur_ui_when_backgrounded* para ofuscar todos os campos do snapshot enquanto a imagem é salva durante o processo em segundo plano.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Em dispositivos Android, o sistema operacional Android faz uma captura de tela para uso no menu de tarefas recentes quando a aplicação é enviada para segundo plano. Os usuários também podem fazer capturas de tela manuais da aplicação, que são armazenadas publicamente no dispositivo.

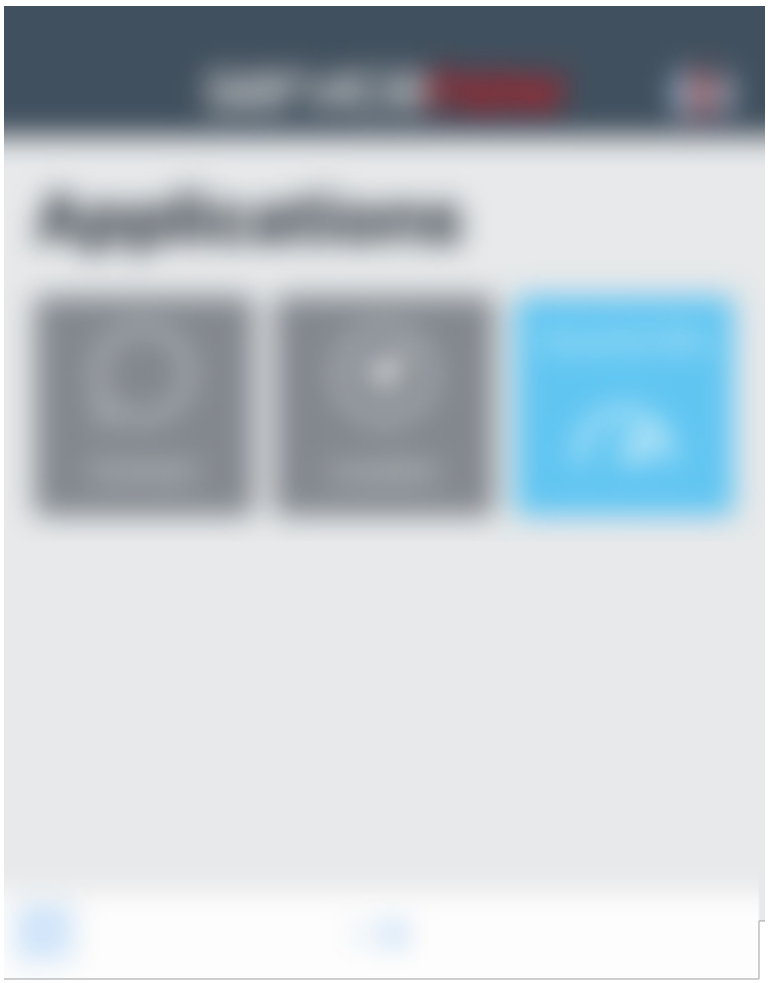
Em dispositivos iOS, o sistema operacional iOS também permite que as aplicações salvem um arquivo de imagem. Este arquivo representa a última tela vista pelo usuário quando a aplicação é enviada para segundo plano. Embora a intenção seja fornecer uma melhor experiência do usuário, isso também cria um risco à segurança porque as imagens são salvas como arquivos de imagem PNG.

Nota: Esta definição ou configuração é por instância, portanto, o usuário deve se conectar à instância com a propriedade configurada.

Para ofuscar todos os campos do snapshot no app ServiceNow Classic, consulte Configurar a opção do app de desfoque para melhorar a segurança.

Exemplo

Quando você define essa propriedade como verdadeira, a aplicação em segundo plano fica ofuscado para dispositivos iOS e escurecido para dispositivos Android iOS.



© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mais informações

Atributo	Descrição
Nome da propriedade/plug-in	*glide.ui.m.blur_ui_when_backgrounded*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Categoria	Autenticação
Finalidade	Ofuscar todos os campos do snapshot enquanto a imagem é salva durante o processo em segundo plano.
Valor recomendado	verdadeiro
Classificação de risco de segurança	2,4
Impacto funcional	(Baixo) Se a propriedade *glide.ui.m.blur_ui_when_backgrounded* estiver definida como verdadeira, os apps nativos usarão o parâmetro definido no servidor para desfocar a tela quando o aplicativo entrar em segundo plano. • As capturas de tela tiradas pelo iOS e pelo Android são desfocadas quando o aplicativo entra em segundo plano. • A experiência do usuário pode ser afetada negativamente porque ele não poderá ver o conteúdo quando o app for enviado para segundo plano.
Risco à segurança	(Médio) Um dispositivo comprometido (desbloqueado) permite que um invasor tenha acesso total ao sistema de arquivos, com acesso a esses arquivos/snapshots com informações confidenciais incorporadas a eles.

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Desabilitar autenticação sem senha

Use a propriedade *glide.login.no_blank_password* para impedir que os usuários efetuem login na NOW Platform com senhas em branco ou deixando o campo **Senha** vazio.

Mesmo que o administrador atribua intencionalmente um valor nulo ou uma senha em branco nos registros do usuário, um usuário não poderá fazer login sem fornecer um valor no campo **Senha**.

Mais informações

Atributo	Descrição
Nome da propriedade	*glide.login.no_blank_password*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Configurar na Central de segurança da instância	Sim
Finalidade	Garantir uma autenticação forte, já que às vezes o nome de usuário é fácil de adivinhar em uma organização.
Valor recomendado	verdadeiro
Impacto funcional	(Baixo) Operações não devem usar senhas em branco porque isso é visto como um risco de segurança crítico. No entanto, se houver um caso válido para esse uso, há a possibilidade de uma indisponibilidade. Usuários com senhas em branco não poderão fazer login na instância.
Risco à segurança	(Alto) Um invasor pode fazer login na instância com os nomes de usuário padrão ou por indivíduo/grupo específico (geralmente nome.sobrenome) sem qualquer senha. Isso é visto como um risco de segurança crítico, pois permitiria que um usuário público violasse a confidencialidade e a integridade dos dados da instância.

Não aplicar política de senha no login

Gerencie como a complexidade de senha é tratada em sua instância.

Use a propriedade *glide.apply.password_policy.on_login* para gerenciar a complexidade da senha. Se esta propriedade for definida como **falsa**, não haverá imposição de complexidade de senha durante o login. Se estiver definida como **verdadeira**, ela imporá a complexidade da senha, o que pode levar a problemas de conformidade com a política da organização. Em vez de impor a complexidade da senha, o padrão de verificação de segurança de aplicações (ASVS) sugere impor um tamanho mínimo de 12 caracteres para o tamanho da senha.

Mais informações

Atributo	Descrição
Nome da configuração	*glide.apply.password_policy.on_login*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	booliano
Valor recomendado	falso
Valor-padrão	falso
Categoria	Autenticação
Risco à segurança	• Pontuação de gravidade: 4,4 • Pontuação do CVSS: média

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
	• Detalhes do risco à segurança: definir esta propriedade como **verdadeira** pode impor a complexidade da senha e causar problemas de conformidade da organização.
Dependências e pré-requisitos	Nenhum

Habilitar verificação de validação de senhas na lista de proibições

Gerencie as senhas na lista de proibições na tabela Senha excluída.

Use a propriedade *glide.enable.blacklist_password* para monitorar senhas na lista de proibições. Quando a propriedade é definida como **verdadeira**, a senha do usuário é verificada em uma lista de senhas na lista de proibições, o que o impede de usar uma senha de um conjunto de senhas violadas. O administrador pode manter a lista inserindo senhas na tabela Senha excluída.

Mais informações

Atributo	Descrição
Nome da configuração	*glide.enable.blacklist_password*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	booliano
Valor recomendado	verdadeiro
Valor-padrão	falso
Categoria	Autenticação
Dependências e pré-requisitos	Nenhum
Referências	Exclusão de senhas por meio de políticas de senha em sua instância

Como habilitar CAPTCHA para registro de usuário externo [Atualizado na Central de segurança 1.5]

O *sn_ext_usr_reg.captchaEnabled* controla se o CAPTCHA será validado para registro de usuário externo.

Defina *sn_ext_usr_reg.captchaEnabled* como o valor recomendado **verdadeiro** para ajudar a impedir que ataques de criação automática de conta exijam CAPTCHA para registro de usuário externo. Defina o valor como **falso** para não exigir CAPTCHA para registro de usuário externo.

Mais informações

Atributo	Descrição
Nome da propriedade	*sn_ext_usr_reg.captchaEnabled*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Categoria	Autenticação
Finalidade	Esta propriedade é usada para habilitar ou desabilitar a validação de CAPTCHA ao fazer o registro de usuário externo em portais como CSP, Community. Isso também é usado em aplicativos da store como VAM e CSM Guest Walkup para habilitar/desabilitar o captcha.
Valor recomendado	Verdadeiro
Tipo de configuração	Booliano
Risco à segurança	(Baixo) A propriedade controla a habilitação de CAPTCHA no registro de usuário externo. Valor unideal pode resultar em vulnerabilidade de segurança.
Classificação de risco de segurança	3,7

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Habilitar CAPTCHA na redefinição de senha

Use a propriedade *password_reset.captcha.ignore* para habilitar ou desabilitar a solicitação de um desafio CAPTCHA quando um usuário redefinir a senha.

Defina *password_reset.captcha.ignore* com o valor recomendado **falso** para exigir um desafio CAPTCHA para um usuário redefinir a senha. Defina o valor como **verdadeiro** para ignorar a opção CAPTCHA para uma redefinição de senha.

Os CAPTCHAs ajudam a impedir ataques de automação, solicitando ao usuário uma resposta de desafio que não é respondida facilmente por sistemas automatizados. Se o CAPTCHA estiver desabilitado, um invasor poderá ser mais bem-sucedido durante ataques automatizados contra o recurso de redefinição de senha.

Nota: Esta propriedade é usada somente para automação de redefinição de senha.

Mais informações

Atributo	Descrição
Nome da propriedade	*password_reset.captcha.ignore*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Categoria	Autenticação
Finalidade	Esta propriedade é usada para habilitar ou desabilitar a validação de CAPTCHA durante a redefinição de senha.
Valor recomendado	falso
Tipo de configuração	Booliano
Risco à segurança	(Moderado) Valor unideal pode resultar em vulnerabilidade de segurança.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Classificação de risco de segurança	5,5

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Habilitar envio de OTP por e-mail para a autenticação multifator

Gerencie como a autenticação de dois fatores é aplicada em sua instância.

Use a propriedade *glide.authenticate.multifactor.email.otp.enabled* para controlar se um token para autenticação de dois fatores é enviado por e-mail. O e-mail é considerado um fator de MFA fraco, ao qual um invasor tem mais chances de obter acesso para ignorar a MFA. Ao definir esta propriedade como **falsa**, o risco de um invasor ignorar a MFA quando a senha de um usuário for comprometida é reduzido.

Mais informações

Atributo	Descrição
Nome da configuração	*glide.authenticate.multifactor.email.otp.enabled*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	booliano
Valor recomendado	falso
Valor padrão	verdadeiro
Categoria	Autenticação
Risco à segurança	• Pontuação de gravidade: 3,1 • Pontuação de CVSS: baixa • Detalhes do risco à segurança: definir esta propriedade como **falsa** reduz o risco de um agente mal-intencionado ignorar a autenticação de dois fatores.
Dependências e pré-requisitos	Nenhum
Referências	Autenticação multifator com e-mail

Habilitar verificações de política de redefinição de senha

Use a propriedade **glide.enable.password_policy** para habilitar verificações de política de senha sempre que um usuário mudar a senha usando a interface do usuário.

Para definir qual política de senha usar quando esta propriedade estiver habilitada, consulte Habilitação das políticas de senha na sua instância.

Nota: A **glide.enable.password_policy** não se aplica quando um administrador muda uma senha ou adiciona um usuário por meio de script.

Aviso: Esta é uma propriedade tipo porto seguro, o que significa que o valor não pode ser alterado após ser mudado. A reversão não é possível.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mais informações

Atributo	Descrição
Nome da propriedade	*glide.enable.password_policy*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Categoria	Autenticação
Finalidade	Aplicar a política de senha no momento da mudança de senha.
Valor recomendado	verdadeiro (para senhas de maior força)
Classificação de risco de segurança	7,4
Impacto funcional	(Médio) Definir a propriedade como verdadeira ativa as verificações de política de senha quando um usuário redefine a senha.
Risco à segurança	(Moderado) Sem uma política de senha, um usuário pode criar uma senha fraca, o que aumenta a probabilidade de um adversário obter acesso à instância.

Etapas para configurar

Se você definir esta configuração na página de Configuração de conformidade de proteção na Central de segurança da instância:

1. Em **Médio**, selecione **Gestão de sessões**.
2. Na configuração **Habilitar verificações da política de Redefinição de senha**, selecione **Média** para senhas de força média ou **Alta** para senhas mais robustas e de maior força. Selecionar uma dessas opções define a propriedade **glide.enable.password_policy** como verdadeira e inicia um fluxo de trabalho que atualiza automaticamente sua política de senha.

Além disso, você pode definir a propriedade do sistema *glide.apply.password_policy.on_login* para habilitar verificações de política de senha no momento do login.

Habilitar acesso à sessão baseado em política para dispositivos móveis [Novo na Central de segurança 1.5]

Use o plug-in de acesso à sessão baseado em política com abordagem zero trust para controlar se os usuários que se autenticam por um aplicativo para celular terão suas funções reduzidas.

O plug-in de acesso à sessão baseado em política com abordagem zero trust permite que os administradores de segurança reduzam o acesso do usuário em uma sessão com base em parâmetros como endereço IP, local, atributos do provedor de identidade e atributos do usuário com políticas de autenticação adaptável. Quando esse plug-in é habilitado ou definido como verdadeiro, as funções dos usuários que se autenticam por um dispositivo móvel ficam restritas de acordo com as políticas do plug-in. Os administradores de instâncias podem restringir o acesso de alto privilégio quando os usuários se autenticam por um dispositivo móvel, porque isso pode indicar um ambiente inseguro para operações confidenciais.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mais informações

Atributo	Descrição
Nome da configuração	*glide.authenticate.session_access.mobile.enabled*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	booliano
Valor recomendado	verdadeiro
Valor-padrão	verdadeiro
Categoria	Controle de acesso
Risco à segurança	• Pontuação de gravidade: 4,7 • Pontuação do CVSS: média • Detalhes do risco à segurança: se essa configuração de proteção for definida como verdadeira, o acesso à sessão baseado em política será aplicado na instância para logins por dispositivos móveis, e o privilégio das funções dos usuários que não forem provenientes de um ambiente confiável ou que não usarem dispositivos confiáveis será reduzido. "Verdadeiro" é a configuração segura. Se essa configuração for definida como falsa, o acesso à sessão baseado em política será desabilitado, e os usuários continuarão a ter funções completas o tempo todo, incluindo as funções com privilégios altos, como administrador.
Dependências e pré-requisitos	Nenhum(a)
Impacto funcional	Se o administrador configurar a política de acesso à sessão na instância, as funções dos usuários serão reduzidas após o login por dispositivo móvel se não forem provenientes de um ambiente confiável ou não usarem um dispositivo confiável.
Referências	Autenticação adaptável

Habilitar SSL na Autenticação LDAP

Gerencie a criptografia de solicitações da Autenticação LDAP em sua instância.

Use a propriedade *glide.ldap.use.ssl* para habilitar ou desabilitar a criptografia TLS para solicitações de Autenticação LDAP enviadas pela rede. Se essa propriedade não estiver definida com o valor recomendado de **verdadeiro**, a Autenticação LDAP ficará suscetível a um ataque de intermediário.

Mais informações

Atributo	Descrição
Nome da configuração	*glide.ldap.use.ssl*

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	booliano
Valor recomendado	verdadeiro
Valor-padrão	verdadeiro
Categoria	Autenticação
Risco à segurança	• Pontuação de gravidade: 8,1 • Pontuação de CVSS: alta • Detalhes do risco à segurança: a configuração dessa propriedade como **falsa** torna a Autenticação LDAP vulnerável a um ataque de intermediário.
Dependências e pré-requisitos	Nenhum
Referências	Integração LDAP

Como minimizar a duração da expiração do link de registro de usuário externo [Atualizado na Central de segurança 1.3 e 1.5]

Gerencie o número de dias que um link de registro pode ser acessado.

Use a propriedade *sn_ext_usr_reg.Reg_link_expiration_days* para gerenciar quem pode acessar um link de registro. Se o link de registro estiver definido com o valor recomendado **3**, ele poderá ser usado por alguém diferente do usuário pretendido, caso seja descoberto posteriormente.

Mais informações

Atributo	Descrição
Nome da configuração	*sn_ext_usr_reg.Reg_link_expiration_days*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	Inteiro
Valor recomendado	3
Valor padrão	3
Categoria	Autenticação
Risco à segurança	• Pontuação de gravidade: média • Pontuação de CVSS: 6,6 • Detalhes do risco à segurança: não definir esta propriedade como o número inteiro “3” possibilita que o link de registro seja usado por um usuário não pretendido.
Dependências e pré-requisitos	Nenhum

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Gerenciar tentativas de login sem êxito

Há duas ações de script disponíveis que permitem a um administrador de site gerenciar o número de vezes que um usuário pode fornecer uma senha incorreta antes de ser bloqueado em Now Platform. Você pode habilitar qualquer uma dessas ações de script para gerenciar tentativas de login sem êxito.

Mais informações

Atributo	Descrição
Nome da propriedade/plug-in	N/D
Tipo de configuração	Política do Sistema > Ações de Script
Categoria	Autenticação
Finalidade	Impor uma política rígida para tentativas de login com falha para evitar ataques de força bruta de credenciais.
Valor recomendado	Ativo
Classificação de risco de segurança	7,3
Impacto funcional	(Baixo) Esta correção permite ao administrador da instância monitorar e relatar qualquer acesso de usuário mal-intencionado. Nenhum impacto na funcionalidade, somente mudança na experiência do usuário.
Risco à Segurança	(Moderado) Aplique uma estratégia de registro em log e auditoria definida para que você possa identificar e agir em atividades suspeitas em tempo hábil.

Etapas para configurar

1. Navegue até **Política do sistema** > **Ações de Script.**
2. Pesquise o nome *`*SNC User`*.
3. Para habilitar o gerenciamento de tentativas de login sem êxito, altere o estado Ativo das ações de script *`SNC User Lockout Check with Auto Unlock`* ou *`SNC User Lockout Check`* de **falso** para **verdadeiro**.
4. Para redefinir o contador de login sem êxito após um login bem-sucedido, você pode ativar a ação de script *`SNC User Clear`*.

Como maximizar a duração do tempo limite de desbloqueio para logins com falha [Atualizado na Central de segurança 1.3]

Há duas ações de script disponíveis que permitem a um administrador de site gerenciar o número de vezes que um usuário pode fornecer uma senha incorreta antes de ser bloqueado em Now Platform. Você pode habilitar qualquer uma dessas ações de script para gerenciar tentativas de login sem êxito.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mais informações

Atributo	Descrição
Nome da propriedade	*glide.user.unlock_timeout_in_mins*
Tipo de configuração	Política do Sistema > Ações de Script
Categoria	Autenticação
Finalidade	Impor uma política rígida para tentativas de login com falha para evitar ataques de força bruta de credenciais.
Valor recomendado	Ativo
Impacto funcional	(Baixo) Esta correção permite ao administrador da instância monitorar e relatar qualquer acesso de usuário mal-intencionado. Nenhum impacto na funcionalidade, somente mudança na experiência do usuário.
Risco à Segurança	(Moderado) Aplique uma estratégia de registro em log e auditoria definida para que você possa identificar e agir em atividades suspeitas em tempo hábil.

Etapas para configurar

1. Navegue até **Política do sistema** > **Ações de Script.**
2. Pesquise o nome **SNC User*.
3. Para habilitar o gerenciamento de tentativas de login sem êxito, altere o estado Ativo das ações de script *SNC User Lockout Check with Auto Unlock* ou *SNC User Lockout Check* de **falso** para **verdadeiro**.
4. Para redefinir o contador de login sem êxito após um login bem-sucedido, você pode ativar a ação de script *SNC User Clear*.

Exigir desfoque da IU do aplicativo para celular [Atualizado na Central de segurança 1.3]

Configure a propriedade *glide.sg.blur_ui_when_backgrounded* para que a IU do aplicativo fique desfocada quando o aplicativo estiver sendo executado em segundo plano.

Se esta propriedade não estiver definida com o valor recomendado de **verdadeiro**, a interface do usuário do aplicativo para celular ficará visível quando exibida no alternador de aplicativos. A IU ainda está visível mesmo quando o aplicativo está sendo executado em segundo plano, o que fornece um nível mais baixo de segurança e confidencialidade para os usuários finais.

Mais informações

Atributo	Descrição
Nome da configuração	*glide.sg.blur_ui_when_backgrounded*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Tipo de dados	booliano
Valor recomendado	verdadeiro
Valor-padrão	falso
Categoria	Arquivo e recursos
Risco à segurança	• Pontuação de gravidade: 2.4 • Pontuação de CVSS: baixa • Detalhes do risco de segurança: definir o valor como **verdadeiro** fornece um nível mais alto de confidencialidade e privacidade no dispositivo local ao desfocar a IU quando o aplicativo está sendo executado em segundo plano.
Dependências e pré-requisitos	Nenhum
Referências	Ofuscação da IU para celular

Notificar usuários durante o processo de redefinição/mudança de senha

Use essa propriedade para permitir que os usuários finais redefinam ou mudem senhas usando um processo de autoatendimento.

Essa propriedade permite que um usuário final redefina ou mude uma senha usando um processo de autoatendimento. Como alternativa, sua organização pode implementar um processo que requer um agente da central de serviços para redefinir as senhas dos usuários finais. Se um processo de mudança e/ou redefinição de senha não notificar os usuários sobre a atualização da senha, um agente mal-intencionado poderá bloquear o acesso desse usuário à própria conta, sem que ele saiba. Isso daria ao agente mal-intencionado mais tempo para realizar atividades mal-intencionadas. Certifique-se de que o processo de redefinição de senha notifique os usuários sobre a mudança ou redefinição da senha.

Mais informações

Atributo	Descrição
Nome da configuração	*pwd_process.change, pwd_process.reset*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	booliano
Valor recomendado	verdadeiro
Valor-padrão	verdadeiro
Categoria	Autenticação
Risco à segurança	• Pontuação de gravidade: 8,1 • Pontuação de CVSS: alta • Detalhes do risco à segurança: se o usuário não receber nenhuma notificação após a redefinição

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
	ou a mudança de uma senha, um agente mal-intencionado poderá bloquear o acesso desse usuário à própria conta, sem que ele saiba.
Dependências e pré-requisitos	Nenhum

Remover credenciais da página de boas-vindas

Modifique o conteúdo padrão na página de boas-vindas para remover as credenciais padrão.

Dois registros de **Como fazer login** são instalados como parte dos dados de demonstração do plug-in CMS.

Nota: Se você não instalar os dados de demonstração para uma instância, esses registros não existirão. Nesse caso, a configuração é considerada em conformidade com as práticas de segurança recomendadas.

Mais informações

Atributo	Descrição
Nome	*How to login*
Tipo de configuração	Tabela: sys_home
Categoria	Autenticação
Finalidade	Remover credenciais padrão da página de boas-vindas que foram adicionadas com dados de demonstração.
Valor recomendado	"Falso" ou "nulo" se nenhum dado de demonstração tiver sido utilizado.
Valor padrão	Nenhum. Essa é uma configuração de tabela, não uma propriedade do Glide. Portanto, não há valor padrão.
Tipo de configuração	Booliano
Risco à segurança	(Moderado) Os dados de demonstração são informados para o plug-in CMS, que inclui duas senhas padrão na página de boas-vindas. Se não forem removidas, um invasor não autorizado poderá obter acesso à instância.
Referências	https://support.servicenow.com/kb_view.do?sysparm_article=KB0550107 Páginas de boas-vindas

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Como minimizar o máximo de SMS de redefinição de senha por dia [Atualizado na Central de segurança 1.3]

Gerencie o número máximo de códigos SMS que o usuário pode enviar para verificação por dia.

A propriedade *password_reset.sms.max_per_day* representa o número máximo de códigos SMS que um usuário pode enviar para verificação.

Mais informações

Atributo	Descrição
Nome da configuração	*password_reset.sms.max_per_day*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	inteiro
Valor recomendado	10
Valor-padrão	10
Categoria	Autenticação
Risco à segurança	• Pontuação de gravidade: 5,9 • Pontuação do CVSS: média • Detalhes do risco à segurança: se esta propriedade não estiver definida com o valor recomendado de **10** ou menos, será mais fácil obter o código SMS por meio de ataques de força bruta.
Dependências e pré-requisitos	Nenhum

Como minimizar a duração da expiração da solicitação de redefinição de senha [Atualizado na Central de segurança 1.3]

O *password_reset.request.expiry* denota o período de tempo em minutos durante o qual um usuário deve executar o processo de redefinição de senha.

Nota: A configuração da propriedade *password_reset.request.expiry* tem precedência sobre a configuração da propriedade *glide.pwd_reset.onetime.token.validity* que tem um padrão de 12 horas.

Mais informações

Atributo	Descrição
Nome da propriedade	*password_reset.request.expiry*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Categoria	Autenticação
Finalidade	Denota o período de tempo em minutos durante o qual um usuário deve executar o processo de redefinição de senha.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Valor recomendado	Defina como um número inteiro de **10** ou menos. O valor padrão é 10.
Tipo de configuração	Valores inteiros
Risco à segurança	(Moderado) Se a propriedade não estiver definida com o valor recomendado de 10 ou menos, ela aumentará a oportunidade de alguém adivinhar e usar a solicitação e tentar redefinir a senha.
Classificação de risco de segurança	4,2
Referências	Configurar as propriedades do Redefinição de senha

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Como minimizar a provisão de máximo de tentativas de solicitação de redefinição de senha [Atualizado na Central de segurança 1.3]

O *password_reset.request.max_attempt* é usado para controlar o número máximo de tentativas malsucedidas que um usuário pode redefinir ou alterar sua senha antes de ser bloqueado por um período de tempo especificado.

Mais informações

Atributo	Descrição
Nome da propriedade	*password_reset.request.max_attempt*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Categoria	Autenticação
Finalidade	Indica o número máximo de tentativas de redefinição de senha malsucedidas que podem ser realizadas antes que o usuário seja bloqueado no processo de redefinição de senha. O período de bloqueio é determinado pelo valor em *password_reset.request.max_attempt_window*.
Valor recomendado	Defina como um valor inteiro positivo menor que três. O valor padrão é **3**. Ao determinar o limite do intervalo superior da propriedade, considere a tarefa que o usuário está executando.
Tipo de configuração	Valores inteiros positivos
Risco à segurança	(Alto) Se a propriedade não estiver definida com o valor recomendado de "**3**" ou outro valor pequeno, um ataque de força bruta pode ser executado contra o processo de redefinição de senha.
Classificação de risco de segurança	7,5
Referências	Configurar as propriedades do Redefinição de senha

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Como minimizar a duração da janela de máximo de tentativas de solicitação de redefinição de senha [Atualizado na Central de segurança 1.3]

A propriedade *password_reset.request.max_attempt_window* controla o número de minutos que um usuário deve esperar para redefinir ou mudar sua senha depois de exceder o número máximo de tentativas malsucedidas que é definido com a propriedade *password_reset.request.max_attempt*.

Mais informações

Atributo	Descrição
Nome da propriedade	*password_reset.request.max_attempt_window*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Categoria	Autenticação
Finalidade	Indica o período de bloqueio em minutos após o número máximo de tentativas de redefinição de senha malsucedidas.
Valor recomendado	1.440
Valor padrão	1.440
Tipo de configuração	Valores inteiros positivos
Risco à segurança	(Alto) Se a propriedade não estiver definida com o valor recomendado de 1440 ou menos, será possível executar a força bruta da conta, já que a conta não será bloqueada após um número máximo de tentativas de autenticação incorretas.
Classificação de risco de segurança	7,5
Referências	Configurar as propriedades do Redefinição de senha

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Como maximizar a duração da janela de nova tentativa de solicitação de redefinição de senha [Atualizado na Central de segurança 1.3]

A propriedade *password_reset.request.retry_window* controla o número de minutos antes que a contagem de tentativas de redefinição de senha seja atualizada.

Mais informações

Atributo	Descrição
Nome da propriedade	*password_reset.request.retry_window*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Categoria	Autenticação
Finalidade	Indica o período de tempo em minutos antes que a contagem de tentativas de senha seja atualizada a partir da última solicitação antes que a contagem de novas tentativas seja redefinida para zero.
Valor recomendado	Defina como um valor inteiro positivo de **1440** ou mais. O valor padrão é **1440** minutos.
Tipo de configuração	Valores inteiros positivos.
Risco à segurança	(Alto) Se a propriedade não estiver definida com o valor recomendado de 1440 ou mais, um ataque de força bruta pode ser executado contra o processo de redefinição de senha.
Classificação de risco de segurança	7,5
Referências	Configurar as propriedades do Redefinição de senha

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Como minimizar a duração da janela de sucesso na solicitação de redefinição de senha [Atualizado na Central de segurança 1.3]

A propriedade *password_reset.request.success_window* controla o número de minutos que um usuário deve esperar para redefinir ou mudar sua senha depois redefinir a senha com êxito. O usuário será bloqueado para redefinir a senha novamente pela duração especificada.

Mais informações

Atributo	Descrição
Nome da propriedade	*password_reset.request.success_window*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Categoria	Autenticação
Finalidade	Ele denota o período de tempo em minutos que um usuário deve aguardar após redefinir a senha com êxito para redefinir a senha novamente.
Valor recomendado	1.440
Valor padrão	1.440
Tipo de configuração	Valores inteiros positivos
Risco à segurança	(Alto) Se a propriedade não estiver definida com o valor recomendado de 1440 ou menos, isso aumentará a oportunidade de alguém abusar da funcionalidade de redefinição de senha para obter acesso não autorizado a uma conta de usuário.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Classificação de risco de segurança	4,9
Referências	Configurar as propriedades do Redefinição de senha

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Como maximizar a duração da janela de desbloqueio da solicitação de redefinição de senha [Atualizado na Central de segurança 1.3]

A propriedade *password_reset.request.unlock_window* controla o número de minutos que um usuário precisa esperar para iniciar uma solicitação de redefinição após o último desbloqueio de conta bem-sucedido.

Mais informações

Atributo	Descrição
Nome da propriedade	*password_reset.request.unlock_window*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Categoria	Autenticação
Finalidade	Ele denota o período de tempo em minutos que um usuário deve aguardar após redefinir a senha com êxito para redefinir a senha novamente.
Valor recomendado	1.440
Valor padrão	1.440
Tipo de configuração	Valores inteiros positivos
Risco à segurança	(Alto) Se a propriedade não estiver definida com o valor recomendado de 1440 ou mais, isso aumentará a oportunidade de um agente mal-intencionado de acessar a senha com força bruta usando ferramentas automáticas.
Classificação de risco de segurança	5,9
Referências	Configurar as propriedades do Redefinição de senha

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Maximizar a complexidade do SMS de redefinição de senha [Atualizado na Central de segurança 1.3]

A propriedade *password_reset.sms.default_complexity* controla o tamanho mínimo de verificação do código SMS necessário durante a redefinição de senha.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mais informações

Atributo	Descrição
Nome da propriedade	*password_reset.sms.default_complexity*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Categoria	Autenticação
Finalidade	Denota o tamanho de verificação do código SMS necessário durante a redefinição de senha.
Valor recomendado	6
Valor padrão	4
Tipo de configuração	Valor inteiro maior que zero
Risco à segurança	(Baixo) Se a propriedade não estiver definida com o valor recomendado, um token de validação de SMS fraco será usado. Isso aumenta a possibilidade de adivinhação de token, o que pode levar à aquisição de conta.
Classificação de risco de segurança	3,8

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Como minimizar a duração da expiração do SMS de redefinição de senha [Atualizado na Central de segurança 1.3]

Controle o número de minutos restantes antes de o código SMS expirar.

A propriedade *password_reset.sms.expiry* representa o número de minutos restantes antes de o código SMS expirar.

Mais informações

Atributo	Descrição
Nome da configuração	*password_reset.sms.expiry*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	inteiro
Valor recomendado	5
Valor-padrão	5
Categoria	Autenticação
Risco à segurança	• Pontuação de gravidade: 5,6 • Pontuação do CVSS: média • Detalhes do risco à segurança: se esta propriedade não estiver definida com o valor recomendado de

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
	5 ou menos, aumentam as chances de um agente mal-intencionado adivinhar e usar o código SMS para redefinir a senha.
Dependências e pré-requisitos	Nenhum

Como maximizar a duração da janela de pausa de SMS de redefinição de senha [Atualizado na Central de segurança 1.3]

Gerencie quantos minutos um usuário deve esperar antes de poder solicitar um novo código de redefinição de senha.

Se esta propriedade não estiver definida com o valor recomendado de **2** minutos ou mais, um usuário mal-intencionado poderá iniciar vários códigos de redefinição de senha em uma breve janela de tempo. Isso aumenta a chance de um agente mal-intencionado prever o código de redefinição via SMS.

Mais informações

Atributo	Descrição
Nome da configuração	*password_reset.sms.pause_window*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	inteiro
Valor recomendado	2
Valor-padrão	2
Categoria	Autenticação
Risco à segurança	• Pontuação de gravidade: 4,8 • Pontuação do CVSS: média • Detalhes do risco de segurança: certifique-se de que *password_reset.sms.pause_window* esteja definido com um valor de 2 ou mais.
Dependências e pré-requisitos	Nenhum

Como maximizar a duração do atraso de verificação da redefinição de senha [Atualizado na Central de segurança 1.3]

Configure o atraso, em milissegundos, que um usuário deve esperar antes de enviar uma nova solicitação de redefinição de senha.

Um agente mal-intencionado pode tentar forçar as credenciais de login usando ferramentas de automação, como bots, contra as quais a propriedade **Atraso na verificação de redefinição de senha** ajuda a proteger. O valor da propriedade representa o atraso, em milissegundos, que um usuário deve esperar antes de fazer uma solicitação para redefinir a senha. Se esta propriedade não estiver definida com o valor recomendado de **1000** ou mais, o login ficará mais vulnerável a ataques de força bruta.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mais informações

Atributo	Descrição
Nome da configuração	*password_reset.verification.delay*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	cadeia de caracteres
Valor recomendado	1000
Valor padrão	1000
Categoria	Autenticação
Risco à segurança	• Pontuação de gravidade: 5,9 • Pontuação do CVSS: média • Detalhes do risco à segurança: definir o valor da propriedade como inferior a 1000 torna seu login mais vulnerável a ataques de força bruta.
Dependências e pré-requisitos	Nenhum
Referências	Configurar senha para um usuário

Como minimizar a duração da restrição "notBefore" ou "notOnOrAfter" de SAML [Atualizado na Central de segurança 1.3 e 1.5]

Configure essa propriedade para adicionar um período de carência durante o qual as solicitações e respostas SAML são consideradas válidas.

Essa propriedade adiciona um período de carência durante o qual as solicitações e respostas SAML são consideradas válidas. O valor da propriedade representa o número de segundos a ser adicionado às restrições *NotBefore* e *NotOnOrAfter* para contabilizar as diferenças de horário entre o relógio do IdP (Identity Provider, provedor de identidade) e o relógio do SP (Service Provider, provedor de serviço). Essas restrições protegem contra ataques de repetição ao negar solicitações que não sejam feitas dentro do intervalo de tempo especificado. Se os relógios do IdP e do SP forem significativamente diferentes, a latência da rede poderá fazer com que a solicitação SAML seja não autorizada.

Mais informações

Atributo	Descrição
Nome da configuração	*glide.authenticate.sso.saml2.clockskew*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	cadeia de caracteres
Valor recomendado	Menos de 60
Valor padrão	180
Categoria	Autenticação

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Risco à segurança	• Pontuação de gravidade: 7,5 • Pontuação de CVSS: alta • Detalhes do risco à segurança: definir o valor da propriedade como “60” ou mais pode impedir o funcionamento das restrições de defesa contra ataques de repetição.
Dependências e pré-requisitos	Nenhum

Como desabilitar a criação de usuários a partir de e-mails recebidos [Atualizado na Central de segurança 1.3]

Use a propriedade *glide.user.trusted_domain* para especificar a lista separada por vírgulas de domínios confiáveis usados na criação de usuários de e-mails de entrada.

Um administrador pode definir uma propriedade de e-mail para criar usuários automaticamente a partir de e-mails de entrada. Se definir esta propriedade com o valor inseguro, a instância criará usuários automaticamente a partir do e-mail de entrada. Cada usuário criado terá a mesma senha padrão codificada, o que facilita ignorar a autenticação por força bruta.

Mais informações

Atributo	Descrição
Nome da propriedade	*glide.pop3readerjob.create_caller*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Categoria	Autenticação
Valor recomendado	falso
Valor-padrão	falso
Classificação de risco de segurança	5,4
Impacto funcional	(Médio) Depois que esta propriedade é configurada, a instância aceita somente e-mails de domínios confiáveis. Se você não incluir o domínio na lista confiável, haverá um impacto para os usuários convidados porque as contas serão criadas automaticamente.
Risco à segurança	(Moderado) Se a propriedade não estiver habilitada, um invasor poderá usar uma campanha de falsificação/spam de e-mail para enviar vários e-mails, resultando na criação de mais usuários convidados desnecessários.
Referências	Configuração de entrada de e-mails

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Ativar a autenticação multifator baseada em função [Atualizado na Central de segurança 1.3]

Use a propriedade *glide.authenticate.multifactor* para impor a MFA (multi-factor authentication, autenticação multifator) baseada em função para todos os usuários atribuídos a funções específicas.

Imponha autenticação multifator com base nas funções atribuídas ao usuário. Se um usuário tiver sido atribuído à função "admin", "security_admin" ou "user_admin" na lista de funções multifator, a MFA será aplicada

- Defina essa propriedade como **verdadeira** para impor a autenticação multifator baseada em função a todos os usuários atribuídos a funções específicas.
- Defina essa propriedade como **falsa** para impor a autenticação multifator baseada em função a todos os usuários atribuídos a funções específicas.

Mais informações

Atributo	Descrição
Nome da propriedade	*glide.authenticate.multifactor*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Categoria	Autenticação
Finalidade	Impor a autenticação multifator baseada em função a todos os usuários atribuídos a funções específicas.
Tipo	booliano
Valor recomendado	*verdadeiro*
Valor-padrão	falso
Dependências de segurança	Ativar **Autenticação multifator baseada em função** junto à tabela **Critérios de multifator**.
Classificação de risco de segurança	7,2
Impacto funcional	(Médio) Habilitar esta propriedade melhora a experiência do usuário. Ela atua como uma camada extra de proteção e segurança contra credenciais comprometidas.
Risco à segurança	(Moderado) Se esta propriedade não estiver habilitada, há um risco de acesso não autorizado a dados confidenciais.
Referências	Configuração dos critérios multifatores baseados em função

Definir comprimento mínimo da senha

Defina o comprimento mínimo de uma senha de usuário em sua instância.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A propriedade *set.password.length* define o comprimento mínimo necessário para uma senha e é usada para avaliar a conformidade em relação à política de senha atual. O valor da propriedade é um número inteiro com um valor mínimo recomendado de **12**. Definir um comprimento menor pode levar à falha de conformidade com as regulamentações recomendadas.

Mais informações

Atributo	Descrição
Nome da configuração	*set.password.length*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	inteiro
Valor recomendado	12
Valor-padrão	12
Categoria	Autenticação
Risco à segurança	• Pontuação de gravidade: 5,9 • Pontuação do CVSS: média • Detalhes do risco à segurança: definir a propriedade com um valor inferior a 12 pode levar a problemas de conformidade e aumenta o risco de um invasor obter senhas com ataques de força bruta.
Dependências e pré-requisitos	Nenhum

Definir a vida útil de OTP para redefinição de senha como 12 horas ou menos

Controle o tempo de duração do link no e-mail de redefinição de senha.

Esta propriedade faz com que o link no e-mail de redefinição de senha expire após o número de horas especificado na propriedade. O tempo de validade de um token de redefinição de senha deve ser o mais curto possível sem interromper a experiência normal do usuário.

Mais informações

Atributo	Descrição
Nome da configuração	*glide.pwd_reset.onetime.token.validity*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	inteiro
Valor recomendado	12
Valor-padrão	12
Categoria	Autenticação

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Risco à segurança	• Pontuação de gravidade: 5,6 • Pontuação do CVSS: média • Detalhes do risco à segurança: um longo tempo de validade para o token de redefinição de senha aumenta a chance de um agente mal-intencionado assumir o controle de uma conta.
Dependências e pré-requisitos	Nenhum

Minimizar o tempo de vida do verificador único fora de banda [Atualizado na Central de segurança 1.3]

Gerencie a duração dos verificadores fora de banda.

Um verificador fora de banda é um método de entrega alternativo para situações de código único. Por exemplo, redefinir um token multifator. Se este método for habilitado pelos administradores no plug-in Autenticação multifator (MFA), um código único será entregue por e-mail. Para limitar a janela de validade, defina os verificadores fora de banda únicos para expirar após 10 minutos. Uma janela de tempo maior dá mais tempo para que o código seja comprometido por meios ilícitos, como ataques de phishing, engenharia social ou shoulder-surfing.

Mais informações

Atributo	Descrição
Nome da configuração	*glide.multifactor.onetime.code.validity*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	inteiro
Valor recomendado	10
Valor-padrão	10
Categoria	Autenticação
Risco à segurança	• Pontuação de gravidade: 3,9 • Pontuação de CVSS: baixa • Detalhes do risco à segurança: defina os verificadores fora de banda únicos para expirar após 10 minutos. Qualquer intervalo maior aumenta o risco de o código ser comprometido por um agente mal-intencionado.
Dependências e pré-requisitos	Autenticação multifator (MFA)
Referências	

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Impor requisitos de criptografia e senha do dispositivo [Novo na Central de segurança 1.3]

A propriedade *glide.sg.device_encryption_enabled* impõe a criptografia FIPS 140-2 (Federal Information Processing Standard, Padrões de processamento de informações federais). A criptografia e a senha do dispositivo móvel evitam que um usuário não autorizado acesse o conteúdo do dispositivo, mesmo que tenha acesso físico a ele.

Quando *glide.sg.device_encryption_enabled* estiver definido como verdadeiro, o aplicativo para celular da ServiceNow verificará se a criptografia e a senha do dispositivo estão habilitadas.

Mais informações

Atributo	Descrição
Nome da configuração	*glide.sg.device_encryption_enabled*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	booliano
Valor recomendado	verdadeiro
Valor-padrão	falso
Categoria	Autenticação
Risco à segurança	• Pontuação de gravidade: 4,2 • Pontuação do CVSS: média • Detalhes do risco à segurança: se a criptografia ou a senha não estiverem habilitadas, o usuário não terá permissão para fazer login na instância no celular
Dependências e pré-requisitos	Nenhum(a)
Impacto funcional	Quando a propriedade for definida como verdadeira, o aplicativo para celular verificará se a criptografia do dispositivo está habilitada. Se a criptografia não estiver habilitada, os usuários não terão permissão para fazer login na instância atual no celular.

Exigência de captcha para walk-up experience de convidados na aplicação Atendimento ao cliente [Novo na Central de segurança 1.3 e atualizado na 1.5]

O captcha para Walk-up experience de convidado impede que usuários convidados não autenticados criem reservas, pois exige que os usuários concluam uma verificação de captcha.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mais informações

Atributo	Descrição
Nome da configuração	*sn_guest_walkup_cs.captcha.enabled*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	booliano
Valor recomendado	verdadeiro
Valor-padrão	verdadeiro
Categoria	Autenticação
Risco à segurança	• Pontuação de gravidade: 3,7 • Pontuação de CVSS: baixa • Detalhes do risco à segurança: se o captcha não estiver habilitado, isso poderá levar à criação automatizada de compromissos de spam para sobrecarregar o sistema ou preencher todos os pontos de reserva disponíveis, criando um ataque de DoS (Denial of Service, negação de serviço).
Dependências e pré-requisitos	Nenhum(a)
Impacto funcional	Esta propriedade habilita ou desabilita o captcha nos widgets de Check-in de balcão de serviços do convidado do CSM. Por padrão, é definido como verdadeiro.

Como ativar as notificações de código por SMS para inscrições e verificações [Atualizado na Central de segurança 1.3]

A propriedade *password_reset.sms.use_notify* controla o uso de notificações de código por SMS para redefinição de senha.

Se a propriedade *password_reset.sms.use_notify* estiver definida com o valor recomendado de **verdadeiro**, o usuário será notificado para redefinir a senha usando a verificação por SMS e a inscrição no novo dispositivo, que é mais segura do que o e-mail.

Mais informações

Atributo	Descrição
Nome da configuração	*password_reset.sms.use_notify*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	booleano
Valor recomendado	verdadeiro
Valor-padrão	verdadeiro
Categoria	Autenticação

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Risco à segurança	• Pontuação de gravidade: 3,7 • Pontuação de CVSS: baixa • Detalhes do risco à segurança: a configuração desta propriedade como **falsa** torna o e-mail o método padrão para recuperação de senha, que é menos seguro do que o SMS.
Dependências e pré-requisitos	Nenhum

Lógica de Negócios

Esta categoria analisa a lógica e o fluxo exclusivos de cada aplicação com princípios gerais de segurança. Garanta especificamente que a sequência pretendida do fluxo de lógica de negócios não possa ser ignorada, que existam limites para detectar e impedir ataques automatizados e que existam proteções contra falsificação, adulteração, divulgação de informações e ataques de elevação de privilégio.

A seguir estão alguns controles de segurança que um administrador pode configurar para restringir o acesso não autorizado a entidades confidenciais na Now Platform.

Limitar máximo de comentários diários por usuário

Configure a propriedade *sn_kb_social_qa.max_comments_per_user_daily* para restringir o número de comentários de CQ por dia.

Se essa propriedade não for definida com o valor recomendado de **500** ou menos, não haverá restrição no número de comentários de CQ por dia, o que pode levar ao esgotamento dos recursos.

Mais informações

Atributo	Descrição
Nome da configuração	*sn_kb_social_qa.max_comments_per_user_daily*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	inteiro
Valor recomendado	500
Valor-padrão	500
Categoria	Lógica de Negócios
Risco à segurança	• Pontuação de gravidade: 3,7 • Pontuação de CVSS: baixa • Detalhes do risco à segurança: não definir essa propriedade para o valor recomendado de “500” ou menos não impõe limite de comentários de CQ por dia, o que pode levar ao esgotamento dos recursos.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Dependências e pré-requisitos	Nenhum

Limitar máximo de assinaturas diárias por usuário

Configure a propriedade *sn_kb_social_qa.max_subscriptions_per_user_daily* para limitar o número máximo de assinaturas que um usuário pode realizar em um dia.

Se esta propriedade não estiver definida com o valor recomendado de **500** ou menos, não haverá restrição ao número máximo de perguntas e respostas que um usuário pode assinar em um dia. Esta ausência de limitação pode levar ao esgotamento de recursos e afetar a disponibilidade da instância.

Mais informações

Atributo	Descrição
Nome da configuração	*sn_kb_social_qa.max_subscriptions_per_user_daily*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	inteiro
Valor recomendado	500
Valor-padrão	500
Categoria	Lógica de Negócios
Risco à segurança	• Pontuação de gravidade: 3,7 • Pontuação de CVSS: baixa • Detalhes do risco à segurança: defina o valor da propriedade como 500 ou menos para evitar o esgotamento dos recursos.
Dependências e pré-requisitos	Nenhum

Como reduzir a quantidade de destinatários SMTP [Atualizado na Central de segurança 1.3]

O *glide.email.smtp.max_recipients* especifica o número máximo de destinatários que a instância pode listar na linha **Para:** para uma única notificação por e-mail.

Defina *glide.email.smtp.max_recipients* com o valor recomendado de **100 ou menos**. As notificações que excederiam este limite, em vez disso, criarão notificações por e-mail duplicadas endereçadas a um subconjunto da lista de destinatários. Cada notificação por e-mail tem o mesmo número máximo de destinatários.

Mais informações

Atributo	Descrição
Nome da propriedade	*glide.email.smtp.max_recipients*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Categoria	Lógica de Negócios
Finalidade	Se esta propriedade estiver definida com um valor inseguro acima do valor padrão de 100, é possível que uma negação de serviço aconteça na instância.
Valor recomendado	100
Valor padrão	100
Tipo de configuração	Inteiro
Risco à segurança	(Moderado) As notificações que excederiam este limite, em vez disso, criarão notificações por e-mail duplicadas endereçadas a um subconjunto da lista de destinatários.
Classificação de risco de segurança	4,9

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Validar host remoto

Defina a propriedade como verdadeira para impedir que agentes mal-intencionados usem a verificação de porta interna em sua rede.

Se a propriedade *glide.update_set.remote.check_host* não estiver definida com o valor recomendado de **verdadeiro**, o recurso de teste de instância remota Desenvolvimento da equipe permitirá a verificação de porta interna, que é um método que os agentes mal-intencionados podem usar para descobrir vulnerabilidades em uma rede. Em seguida, é possível enumerar todas as portas abertas em um determinado host e, em alguns casos, extrair dados de resposta que podem levar a vazamento de informações ou acesso a dados não autorizados.

⚠ **Aviso:** Esta é uma propriedade tipo porto seguro, o que significa que o valor não pode ser alterado após ser mudado. A reversão não é possível.

Mais informações

Atributo	Descrição
Nome da configuração	*glide.update_set.remote.check_host*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	booliano
Valor recomendado	verdadeiro
Valor-padrão	verdadeiro
Categoria	Lógica de Negócios
Risco à segurança	• Pontuação de gravidade: 6,3 • Pontuação do CVSS: média • Detalhes do risco à segurança: não definir a propriedade com o valor recomendado de

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
	verdadeiro pode permitir que agentes mal-intencionados usem a verificação de porta interna para obter acesso a dados não autorizados.
Dependências e pré-requisitos	Nenhum
Referências	https://support.servicenow.com/kb?id=kb_article_view&sysparm_article=KB0755132 Definir uma instância remota

Comunicação

Este controle garante a criptografia apropriada usando algoritmos e cifras fortes. Isso inclui garantir que a versão recomendada do TLS seja usada para conectividade do cliente, uso de pacotes de criptografia robustos, uso de certificados confiáveis e assinados, garantia de que as conexões sejam criptografadas entre os componentes e o registro em log de falhas de conexão.

Como impor a confiança de certificado [Atualizado na Central de segurança 1.3 e removido na 1.5]

Por padrão, a propriedade *com.glide.communications.trustmanager_trust_all* é definida como **falso**. A Now Platform confia somente em certificados que ela pode verificar na loja de certificados JVM. Certificados autoassinados e assinados pela empresa não são confiáveis.

Nota: Os valores dessas propriedades são e não podem ser alterados depois de mudados (eles não são reversíveis) Por motivos de segurança, não altere o valor desta propriedade. Se tiver alguma dúvida, entre em contato com Suporte e atendimento ao cliente.

Mais informações

Atributo	Descrição
Nome da propriedade	*com.glide.communications.trustmanager_trust_all*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Categoria	Comunicação
Finalidade	Impor a validação de certificado para solicitações de saída.
Valor recomendado	falso
Classificação de risco de segurança	6,6
Impacto funcional	(Médio) Esta correção impõe validação estrita no campo de CA (autoridade de certificação). Se uma entidade confiável (CA) emitir o certificado, a instância o aceitará para uso posterior.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Risco à segurança	(Médio) Por motivos de confidencialidade e integridade, a aplicação deve validar a CA do certificado antes de usar o certificado para qualquer operação transacional.
Referências	Certificados Verificação de nome de host do cliente HTTP

Desativação de conexões SSLv2/SSLv3 de saída [Atualizado na Central de segurança 1.3]

Use a propriedade *glide.outbound.sslv3.disabled* para forçar o MID Server a usar TLS ao fazer conexões de saída, como solicitações REST e SOAP. Normalmente, as conexões de saída de uma instância são forçadas a usar TLS em vez de SSL.

Mais informações

Atributo	Descrição
Nome da propriedade	*glide.outbound.sslv3.disabled*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Categoria	Comunicação
Finalidade	Para impor o uso de TLS durante todas as conexões de saída da instância do ServiceNow.
Valor recomendado	verdadeiro
Valor padrão	falso
Classificação de risco de segurança	6,5
Impacto funcional	(Médio) Esta correção impõe o uso da versão do protocolo TLS na comunicação em HTTPS. Se houver dispositivos que os clientes/usuários da instância estão usando e que não são compatíveis com a comunicação TLS, pode haver uma possível indisponibilidade.
Risco à segurança	(Moderado) Versões legadas de SSL foram comprovadas como inseguras quando utilizadas para implementação de shell seguro de HTTP, devido a ataques do lado do cliente, incluindo BEAST e heartbleed de SSL.

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Não usar certificados de demonstração para configurações SAML ativas [Atualizado na Central de segurança 1.5]

Controle se os certificados de demonstração são usados nas configurações de SAML de produção.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Os certificados de demonstração oferecidos pela ServiceNow não devem ser usados em configurações de SAML de produção porque são comuns entre todas as instâncias com uma senha conhecida. Se uma das propriedades de SAML que usa um repositório de chaves de certificado estiver ativa (*require_signed_authnrequest*, *require_signed_logoutrequest* ou *encrypt_assertion*), os dados de demonstração não deverão ser usados. Como os dados de demonstração são compartilhados entre todas as instâncias, não há garantia de integridade das solicitações assinadas com certificados compartilhados. Portanto, qualquer mensagem criptografada pelo IDP poderá ser descriptografada por um agente mal-intencionado se for interceptada.

Mais informações

Atributo	Descrição
Nome da configuração	*glide.authenticate.sso.saml2.keystore*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	cadeia de caracteres
Valor recomendado	sys_id de um repositório de chaves personalizado
Valor-padrão	cadeia de caracteres vazia
Categoria	Comunicação
Risco à segurança	• Pontuação de gravidade: 3,9 • Pontuação de CVSS: baixa
Dependências e pré-requisitos	Nenhum

Impor verificação do OCSP em caso de erro de rede [Novo na Central de segurança 1.3]

Aprenda a configurar a propriedade *com.glide.communications.httpclient.ocsp_allow_network_error* para impedir que agentes mal-intencionados burlem as verificações do OCSP (Online Certificate Status Protocol, Protocolo de status de certificado on-line).

Se o *com.glide.communications.httpclient.ocsp_allow_network_error* não estiver definido com o valor recomendado de "falso", e a verificação do OCSP (Online Certificate Status Protocol, Protocolo de status de certificado on-line) estiver encontrando um erro de rede (por exemplo, um tempo limite ou um problema ao obter as informações de revogação), a verificação de segurança do OCSP será ignorada e considerada bem-sucedida. Isso pode permitir que um invasor com um certificado revogado quebre a infraestrutura de chave pública (PKI) e a confiança do certificado digital que é fundamental para a Web. O uso de certificados revogados geralmente é um indicador de atividade mal-intencionada, a menos que os servidores estejam fora de sincronia.

Mais informações

Atributo	Descrição
Nome da configuração	*com.glide.communications.httpclient.ocsp_allow_network_e*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Tipo de dados	booliano
Valor recomendado	falso
Valor padrão	verdadeiro
Categoria	Comunicação
Risco à segurança	• Pontuação de gravidade: 5,9 • Pontuação do CVSS: média • Detalhes do risco à segurança: não definir esta propriedade como falsa pode permitir que um agente mal-intencionado ignore a verificação de segurança do OCSP.
Dependências e pré-requisitos	Nenhum(a)
Impacto funcional	Esta propriedade determina se uma solicitação em relação ao URI do OCSP (Online Certificate Status Protocol, Protocolo de status de certificado on-line) de AIA (Authority Information Access, acesso a informações de autoridade) resultará em um resultado de aprovação ou falha, em caso de erro de conexão ou erro de tempo limite. Quando definido como falso, o status de revogação do certificado do servidor apresentado não pode ser validado e levará a uma falha de comunicação com esse endpoint. Se ocorrer um erro de rede enquanto a propriedade estiver definida com o valor padrão verdadeiro, o certificado será tratado como válido do ponto de vista de revogação.

Verificar a cadeia de certificados e o nome do host [Novo na Central de segurança 1.3]

Configure a propriedade *com.glide.communications.httpclient.verify_hostname* para impedir ataques intermediários garantindo que o processo de verificação de certificação seja executado.

Se *com.glide.communications.httpclient.verify_hostname* não estiver definido como **verdadeiro**, poderão ocorrer ataques de intermediários, nos quais as comunicações entre duas partes são interceptadas. Definir esta propriedade como falsa desabilita o processo de verificação do certificado. Para corrigir esta ameaça à segurança, defina *com.glide.communications.httpclient.verify_hostname* como **verdadeiro** para impedir que o cliente http se conecte a um nome de host potencialmente prejudicial.

Mais informações

Atributo	Descrição
Nome da configuração	*com.glide.communications.httpclient.verify_hostname*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	booliano

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Valor recomendado	verdadeiro
Valor-padrão	falso
Categoria	Comunicação
Risco à segurança	• Pontuação de gravidade: Alta • Pontuação de CVSS: 7,4 • Detalhes do risco à segurança: não definir *com.glide.communications.httpclient.verify_hostname* com o valor recomendado de "verdadeiro" pode tornar sua instância vulnerável a ataques de intermediários.
Dependências e pré-requisitos	Nenhum(a)
Impacto funcional	Verifica o nome do host e a cadeia de certificados apresentados pelos hosts SSL (secure socket layer, camada de soquetes seguros) remotos. Defina esta propriedade como verdadeira para se proteger de ataques MITM (Man-in-the-middle, ataques de intermediários). **Nota:** Esta propriedade substitui a propriedade *com.glide.communications.trustmanager_trust_all*.

Verificar revogação de certificado [Novo na Central de segurança 1.3]

A propriedade *com.glide.communications.httpclient.verify_revoked_certificate* verifica a revogação do certificado durante o handshake do TLS (Transport Layer Security, Segurança da camada de transporte) para garantir que as verificações de segurança não sejam ignoradas.

Se *com.glide.communications.httpclient.verify_revoked_certificate* não estiver definido com o valor recomendado de **verdadeiro**, a revogação do certificado não será verificada durante o handshake da TLS. O TLS criptografa os dados enviados pela Internet para garantir que os agentes mal-intencionados não consigam ver informações confidenciais, como senhas ou números de cartão de crédito. Ignorar o handshake da TLS é um risco de segurança porque um invasor com um certificado revogado pode deixar de apresentar um certificado válido e violar a confiança da PKI (public key infrastructure, infraestrutura de chave pública) e do certificado digital.

Mais informações

Atributo	Descrição
Nome da configuração	*com.glide.communications.httpclient.verify_revoked_certi*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	booliano
Valor recomendado	verdadeiro
Valor-padrão	verdadeiro

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Categoria	Comunicação
Risco à segurança	• Pontuação de gravidade: 6,5 • Pontuação do CVSS: média • Detalhes do risco à segurança: não definir *com.glide.communications.httpclient.verify_revoked_cert* com o valor recomendado de "verdadeiro" fará com que a revogação do certificado não seja verificada durante o handshake da TLS.
Dependências e pré-requisitos	Nenhum(a)
Impacto funcional	Esta propriedade deve ser definida como verdadeira para garantir que estamos iniciando uma sessão de TLS (Transport Layer Security, segurança da camada de transporte) com um endpoint autêntico. Se esta propriedade for definida como falsa, não verificaremos se o certificado, o que poderia comprometer a segurança da instância.

Configuração

A categoria Configuração garante que as aplicações tenham um ambiente de build seguro e componentes de biblioteca de terceiros protegidos. Especificamente, garante que um pipeline de build e implantação seja repetível e inclua testes automatizados e evite que problemas de segurança conhecidos sejam implantados. Isso inclui manter as dependências atualizadas e livres de vulnerabilidades conhecidas.

Definição automática de opções de tipo de conteúdo [Removido na Central de segurança 1.3.3]

Configure a propriedade Definir automaticamente opções de tipo de conteúdo na sua instância para evitar ataques de confusão de MIME.

Use esta propriedade para controlar o cabeçalho HTTP de resposta X-Content-Type-Options. O cabeçalho HTTP de resposta X-Content-Type-Options é usado pelo servidor para indicar que os tipos MIME anunciados nos cabeçalhos de tipo de conteúdo devem ser seguidos. Se esta propriedade for definida como falso, será possível que um invasor conduza ataques de confusão de MIME; se definido como verdadeiro, este cabeçalho impedirá o navegador de interpretar arquivos como qualquer coisa, exceto o tipo de conteúdo nos cabeçalhos HTTP.

⚠ **Aviso:** O valor desta propriedade é uma substituição sem banco de dados. Não pode ser alterado ou substituído.

Mais informações

Atributo	Descrição
Nome da configuração	*glide.security.header.auto_set_x_content_type_options*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	booliano

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Valor recomendado	verdadeiro
Valor-padrão	falso
Categoria	Configuração
Risco à segurança	• Pontuação de gravidade: 7,3 • Pontuação de CVSS: alta • Detalhes do risco de segurança: definir esta propriedade como **falso** pode possibilitar que um invasor conduza ataques de confusão de MIME.
Dependências e pré-requisitos	Nenhum
Referências	Adicionar uma propriedade do sistema

Valor do cabeçalho HTTP de controle de cache [Atualizado na Central de segurança 1.3]

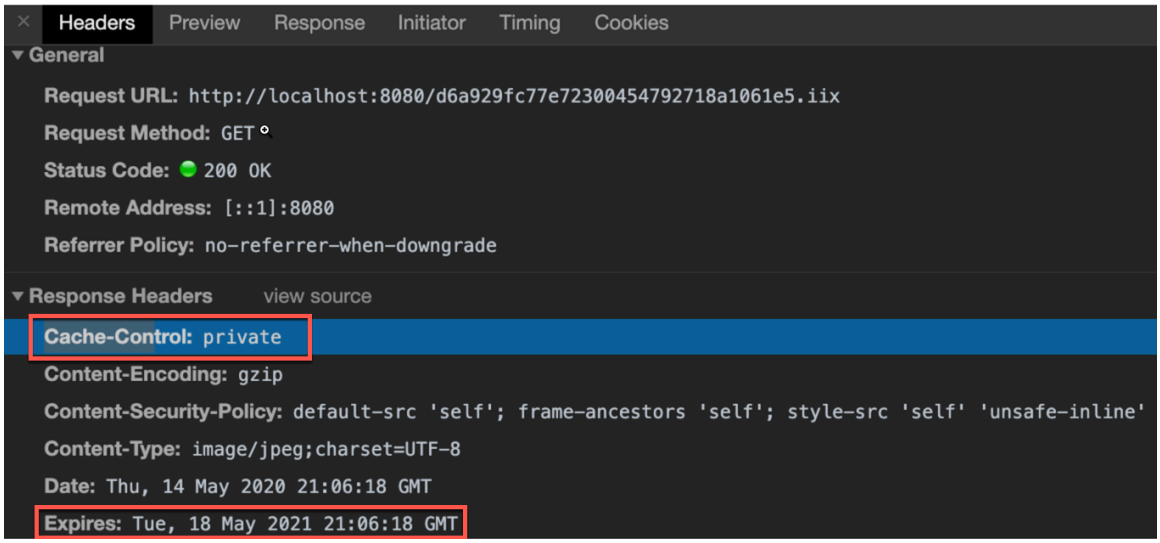
Use a propriedade *glide.http.cache_control* para definir o valor padrão de cache-control nos cabeçalhos de resposta HTTP que Now Platform envia ao solicitar dados de conteúdo estático para uma página. Exemplos de conteúdo estático incluem imagens, CSS e JavaScript renderizados de dentro para uma página.

A propriedade *glide.http.cache_control* define o valor de controle de cache padrão nos cabeçalhos de resposta HTTP como **privado** ou **público**. O padrão é **privado**.

valor	Descrição
privado	O conteúdo estático pode ser armazenado em cache no nível do navegador (cliente), mas não no nível do servidor proxy.
público	O conteúdo estático pode ser armazenado em cache no nível do navegador (cliente) e também no nível do servidor proxy.

O valor de Expires nos cabeçalhos de resposta HTTP controla quando o conteúdo estático expira e tem um valor padrão de 369 dias. Para substituir manualmente o valor padrão, use a propriedade *glide.http.expire.days*.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Nota: Você pode usar a propriedade *glide.http.cache* para habilitar ou desabilitar a configuração dos valores Cache-Control e Expires nos cabeçalhos de resposta HTTP. O padrão é **verdadeiro**, o que permite que você defina:

- Valor padrão de Cache-Control usando a propriedade *glide.http.cache_control*.
- Valor padrão de Expires usando a propriedade *glide.http.expire.days*.

Mais informações

Atributo	Descrição
Nome da propriedade	*glide.http.cache_control*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Categoria	Configuração
Finalidade	Configurar o valor do cabeçalho de resposta HTTP do Cache-Control para conteúdo estático.
Valor recomendado	privado
Valor padrão	privado
Classificação de risco de segurança	4,3
Impacto funcional	(Médio) Define o valor de Cache-Control padrão em um cabeçalho de resposta HTTP.
Risco à segurança	(Alto) Se você definir esta propriedade como **pública**, as instâncias com CDN/proxies poderão armazenar em cache o conteúdo estático e renderizar sem autenticação. • **privado** é uma configuração mais apropriada para instâncias com configuração de CDN/proxy. • Se uma instância não tiver uma configuração de CDN/proxy, qualquer um dos valores deve servir.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Desabilitar depuração do servidor de bate-papo

Habilite ou desabilite os logs do sistema de sua instância configurando esta propriedade.

Use a propriedade *glide.cs.debug* para gerenciar como sua instância lida com logs do sistema. Se a propriedade estiver definida com o valor recomendado de **falso**, os logs do sistema não serão habilitados. Se ela estiver definida como **verdadeira**, os logs do sistema serão habilitados. Defina a propriedade como **verdadeira** somente quando quiser solucionar problemas e desative-a quando terminar. A habilitação de logs do sistema pode fazer com que sejam geradas mensagens em excesso, o que pode sobrecarregar os logs do sistema. As mensagens de log podem expor inadvertidamente informações confidenciais.

Mais informações

Atributo	Descrição
Nome da configuração	*glide.cs.debug*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	booliano
Valor recomendado	falso
Valor-padrão	falso
Categoria	Configuração
Risco à segurança	• Pontuação de gravidade: 2,3 • Pontuação de CVSS: baixa • Detalhes do risco à segurança: a habilitação de logs do sistema pode fazer com que sejam geradas mensagens em excesso, o que pode sobrecarregar o sistema com mensagens de log que inadvertidamente expõem informações confidenciais.
Dependências e pré-requisitos	Nenhum

Desabilitar depuração de elementos de formulário bloqueados

Aqui está a descrição de *glide.security.explain.write.locks*.

Defina *glide.security.explain.write.locks* com o valor recomendado de **falso** para impedir a exibição de explicação de elementos de formulário bloqueados. Defina o valor **verdadeiro** para exibir a explicação de elementos de formulário bloqueados.

Mais informações

Atributo	Descrição
Nome da propriedade	*glide.security.explain.write.locks*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Categoria	Configuração
Finalidade	Os limites exibem o comportamento do SecurityDebugger sem dependência de outras propriedades.
Valor recomendado	falso
Valor-padrão	falso
Tipo de configuração	Booliano
Risco à segurança	(Baixo) Impedirá a exibição da explicação em elementos de formulário bloqueados. Isso torna a aplicação um pouco mais segura, já que menos informações são fornecidas pelo depurador de segurança.
Classificação de risco de segurança	3,5

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Desabilitar depuração do Multi-SSO

A propriedade *glide.authenticate.multisso.debug* controla o registro em log de depuração para Multi-SSO.

Mais informações

Atributo	Descrição
Nome da propriedade	*glide.authenticate.multisso.debug*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Categoria	Configuração
Finalidade	Desabilita depuração Multi-SSO.
Valor recomendado	falso
Valor-padrão	falso
Tipo de configuração	Booliano
Risco à segurança	(Alto) Defina a propriedade com o valor recomendado "Falso", caso contrário, a depuração do MultiSSO será habilitada, o que poderá levar a um vazamento não intencional de informações confidenciais.
Classificação de risco de segurança	4,0
Referências	Propriedades, tabelas e scripts de SSO de vários provedores

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Proibir clonagem de destino [Novo na Central de segurança 1.3]

Configure a propriedade *glide.db.clone.allow_clone_target* para impedir que sua instância seja usada como um destino do clone.

Se *glide.db.clone.allow_clone_target* não estiver definido com o valor recomendado de "falso", a instância poderá ser usada como um destino do clone, ou um registro que especifica o URL da instância e as credenciais usadas para clonagem. Um clone do sistema ocorre quando tudo em um banco de dados é copiado de uma instância para outra. Este é um risco de segurança porque o banco de dados da instância pode ser substituído no processo de clonagem, levando à perda e à falta de integridade de dados. Como solução, certifique-se de que *glide.db.clone.allow_clone_target* esteja definido como "falso".

Mais informações

Atributo	Descrição
Nome da configuração	*glide.db.clone.allow_clone_target*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	booliano
Valor recomendado	falso
Valor padrão	verdadeiro
Categoria	Configuração
Risco à segurança	• Pontuação de gravidade: 5,9 • Pontuação do CVSS: média • Detalhes do risco à segurança: não definir esta propriedade com o valor recomendado de "falso" permite que a instância seja usada como um destino do clone. Este é um risco de segurança porque o banco de dados da instância pode ser substituído no processo de clonagem.
Dependências e pré-requisitos	Nenhum
Referências	• Clone do sistema • Criar um destino de clone
Impacto funcional	Esta propriedade oferece uma proteção adicional que impede que uma instância de produção seja clonada. O valor padrão é "falso" para instâncias de produção e "verdadeiro" para instâncias de produto em fase de desenvolvimento, como desenvolvimento ou CQ. Para permitir que uma instância seja usada como destino do clone, defina esta propriedade como verdadeira.

Desabilitar exibição de rastreamento de pilha da falha de SOAP

Gerencie como os rastreamentos de pilha são exibidos em sua instância.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Use a propriedade *glide.soapfault.display_stack_trace* para gerenciar os rastreamentos de pilha na sua instância. Se esta propriedade for definida como **falsa**, informações confidenciais poderão acabar vazando. Se for definida como **verdadeiro**, nenhum rastreamento de pilha será exibido.

Mais informações

Atributo	Descrição
Nome da configuração	*glide.soapfault.display_stack_trace*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	booliano
Valor recomendado	falso
Valor-padrão	falso
Categoria	Configuração
Risco à segurança	• Pontuação de gravidade: 4,3 • Pontuação do CVSS: média • Detalhes do risco de segurança: definir esta propriedade como **falso** pode expor informações confidenciais por meio do rastreamento de pilha.
Dependências e pré-requisitos	Nenhum

Restringir o acesso ao monitoramento de desempenho

Use a propriedade *glide.security.diag_txns_acl* para controlar o acesso a stats.do, threads.do e replication.do a partir de uma conexão não autenticada.

Quando você define esta propriedade como **verdadeira**, a propriedade *glide.security.diag_txns_acl* só permite o acesso ao seguinte pela conta do administrador:

- https://<instancename>.servicenow.com/stats.do
- https://<instancename>.servicenow.com/threads.do
- https://<instancename>.servicenow.com/replication.do
- https://<instancename>.servicenow.com/thread_pool_stats.do

Sem habilitar esta configuração, ainda é possível acessar esses recursos de uma conexão não autenticada.

Mais informações

Atributo	Descrição
Nome da propriedade	*glide.security.diag_txns_acl*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Categoria	Configuração

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Finalidade	Restringir o acesso às páginas de configuração somente à conta do administrador
Valor recomendado	verdadeiro
Valor-padrão	verdadeiro
Classificação de risco de segurança	5,3
Impacto funcional	(Baixo) Esta correção impõe que somente a conta do administrador obtenha acesso aos dados confidenciais da aplicação para fins de registro em log e solução de problemas.
Risco à segurança	(Moderado) Dados confidenciais, como detalhes do servidor, threads e processos executados no servidor, nunca devem estar visíveis ou acessíveis ao usuário final sem os privilégios apropriados.

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Como ativar a versão atualizada do plug-in Multi-SSO [Atualizado na Central de segurança 1.3 e 1.5]

Verifique se você está usando a v2 do plug-in Multi-SSO e se ele está definido como verdadeiro para reduzir as vulnerabilidades de segurança.

Se o plug-in Multi-SSO estiver habilitado em sua instância, a versão deverá ser v2 e o valor deverá ser definido como **verdadeiro**. As versões anteriores ao Multi-SSO v2, incluindo SAML 1.1 e SAML 2.0, não seguem os padrões de segurança porque usam versões da biblioteca OpenSAML com CVEs (common vulnerabilities and exposures, vulnerabilidades e exposições comuns) conhecidas. Se as CVEs conhecidas forem ameaças de segurança em bibliotecas OpenSAML desatualizadas, isso poderá permitir que um agente mal-intencionado falsifique mensagens e ignore a autenticação por meio de ataques de encapsulamento de assinatura XML, passando-se por entidades ou permitindo que invasores intermediários obtenham acesso não autorizado a uma instância.

Mais informações

Atributo	Descrição
Nome da configuração	*glide.authenticate.multissov2_feature.enabled*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	booliano
Valor recomendado	verdadeiro
Valor-padrão	verdadeiro
Categoria	Configuração
Risco à segurança	• Pontuação de gravidade: 5 • Pontuação do CVSS: média

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
	• Detalhes do risco à segurança: definir o valor da propriedade como **falso** significa que você está usando versões anteriores do Multi-SSO v2, que utiliza bibliotecas OpenSAML com vulnerabilidades de segurança. Isso pode permitir que agentes mal-intencionados falsifiquem mensagens.
Dependências e pré-requisitos	Nenhum
Referências	https://support.servicenow.com/kb?id=kb_article_view&sysparm_article=KB0756504

Impor política de referenciador seguro [Novo na Central de segurança 1.3]

Use a propriedade *com.glide.security.referrerpolicy* para garantir que o cabeçalho HTTP Referrer-Policy envie o nível apropriado de dados para cada página do ServiceNow®, o que evita vazamentos de dados.

Quando a propriedade *com.glide.security.referrerpolicy* é definida como padrão, ela garante que o cabeçalho HTTP Referrer-Policy seja gerenciado com o nível apropriado de informações enviadas, especificamente adaptadas para a página de solicitação específica do Now Platform®. Isso evita vazamentos de dados não autorizados que podem ser acessados de outras partes do URL completo, como o caminho e a cadeia de caracteres de consulta.

Mais informações

Atributo	Descrição
Nome da configuração	*com.glide.security.referrerpolicy*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	cadeia de caracteres
Valor recomendado	padrão
Valor padrão	padrão
Categoria	Configuração
Risco à segurança	• Pontuação de gravidade: 4,3 • Pontuação do CVSS: média • Detalhes do risco à segurança: certifique-se de que a propriedade *com.glide.security.referrerpolicy* esteja definida como padrão para evitar vazamentos de dados não autorizados.
Dependências e pré-requisitos	Nenhum
Referências	Referrer-Policy
Impacto funcional	Controla a quantidade de informações enviada por meio do cabeçalho "referenciador" quando uma solicitação é enviada por uma página:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
	• default: a instância cuidará dos cabeçalhos do referenciador • same-origin: envia um URL de referenciador completo na instância e no mesmo domínio, e nenhum referenciador para fora da origem • origin: envia somente a origem como um referenciador dentro e fora da origem • origin-when-cross-origin: envia um URL de referenciador completo na instância e no mesmo domínio, e apenas a origem fora da origem

Implementação do cabeçalho de segurança x-frame-options: SAMEORIGIN [Atualizado na Central de segurança 1.3]

Use a propriedade *glide.set_x_frame_options* para definir o cabeçalho de resposta X-Frame-Options como SAMEORIGIN para todas as páginas de IU.

Use o cabeçalho de resposta HTTP X-Frame-Options para indicar se o navegador deve ter permissão para renderizar uma página em um `<frame>` ou `<iframe>`. Os sites podem usar esta função para evitar ataques de clickjacking, garantindo que seu conteúdo não seja incorporado a outros sites. Um invasor poderia incorporar sua página na página dele e tornar os elementos da sua página maliciosos. O usuário final pode achar que a página é real já que se parece com a sua página. O usuário final pode clicar nos elementos normalmente e acabar executando o scripts ou elementos maliciosos.

Mais informações

Atributo	Descrição
Nome da propriedade	*glide.set_x_frame_options*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Categoria	Configuração
Finalidade	Atenuar os ataques de ClickJacking.
Valor recomendado	verdadeiro
Valor-padrão	verdadeiro
Classificação de risco de segurança	7,1
Impacto funcional	(Baixo) Esta correção impõe a restrição para renderizar uma aplicação da Now Platform em um aplicativo de terceiros na forma de um iFrame. Se você tiver essa integração, o aplicativo não será renderizado no aplicativo personalizado de terceiros.
Risco à segurança	(Médio) A política Same Origin permite que você restrinja um domínio de recuperar um script ou um recurso de outros domínios. Todos os navegadores modernos oferecem suporte a esta funcionalidade.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
	A política valida a conexão com base no protocolo, na porta e no host. CORS (Cross Origin Request, Solicitação de origem cruzada) é uma modificação da política Same Origin que permite o acesso a recursos/scripts de outro domínio quando declarado explicitamente como uma parte do valor do cabeçalho. • Nesse caso, o cabeçalho X-Frame-Options controla se a aplicação da Now Platform pode ser renderizado no site de terceiros. • Ele reduz a exposição confidencial, pois o valor da propriedade, quando definido como **SAMEORIGIN**, não permite que a renderização aconteça.
Referências	Propriedades do sistema disponíveis Configurar iFrames

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Exigir acesso de gravação à página Adicionar item do Catálogo de serviços [Novo na Central de segurança 1.3]

Use a propriedade *glide.sc.request.add_item_write_access* para impedir que operações não autorizadas sejam realizadas em itens do catálogo.

Mais informações

Atributo	Descrição
Nome da configuração	*glide.sc.request.add_item_write_access*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	booliano
Valor recomendado	verdadeiro
Valor-padrão	falso
Categoria	Configuração
Risco à segurança	• Pontuação de gravidade: 4,3 • Pontuação do CVSS: média • Detalhes do risco à segurança: quando a propriedade *glide.sc.request.add_item_write_access* não está definida como "falsa", qualquer usuário conectado pode acessar a página de IU "Adicionar item do catálogo". Isso pode resultar na execução

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
	de operações não autorizadas em itens do catálogo. Para corrigir este risco de segurança, defina esta propriedade como "verdadeira".
Dependências e pré-requisitos	Nenhum(a)
Impacto funcional	Quando a propriedade for verdadeira, o usuário deve ter acesso de gravação ao registro no contexto da página de IU.

Definir opções do Xframe para impedir a incorporação de sites de terceiros [Atualizado na Central de segurança 1.3]

Configure esta propriedade para impedir que o conteúdo de uma aplicação web seja incorporado a um site de terceiros.

Se essa propriedade não estiver definida com o valor recomendado de **DENY** ou **SAMEORIGIN**, o conteúdo de uma aplicação web poderá ser incorporado a um site de terceiros usando um URI **ALLOW-FROM**, permitindo que sites de terceiros não confiáveis habilitem ataques como click-jacking.

Mais informações

Atributo	Descrição
Nome da configuração	*com.glide.cs.embed.xframe_options*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	cadeia de caracteres
Valor recomendado	sameorigin
Valor padrão	sameorigin
Categoria	Configuração
Risco à segurança	• Pontuação de gravidade: 3,1 • Pontuação de CVSS: baixa • Detalhes do risco à segurança: não definir essa propriedade com o valor recomendado pode permitir que o conteúdo de uma aplicação web seja incorporado a um site de terceiros, possibilitando ataques como click-jacking.
Dependências e pré-requisitos	Nenhum

Proteção de dados

A categoria de proteção de dados aborda os elementos de CIA (Confidentiality, Integrity and Availability, Confidencialidade, integridade e disponibilidade) de dados.

Os componentes da CIA são:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Confidencialidade: os dados são protegidos contra acesso não autorizado em trânsito e em repouso.
- Integridade: os dados são protegidos contra criação, exclusão ou mudança não autorizada.
- Disponibilidade: os dados estão acessíveis quando necessário.

Remover Lembrar-me

Use a propriedade *glide.ui.forgetme* para remover a caixa de seleção **Lembrar-me** da página de login para impedir que as informações de login sejam armazenadas em cache.

Mais informações

Atributo	Descrição
Nome da propriedade	*glide.ui.forgetme*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Categoria	Proteção de dados
Finalidade	Garantir que nenhuma informação de autenticação seja armazenada em cache.
Classificação de risco de segurança	3,5
Valor recomendado	verdadeiro
Valor-padrão	verdadeiro
Impacto funcional	(Baixo) Esta correção mudaria a experiência do usuário, desconectando-o automaticamente da instância quando a sessão expirar. A expiração da sessão dependeria exclusivamente do valor definido na propriedade do sistema, conforme detalhado em Gerenciamento de sessões de usuário.
Risco à segurança	(Baixo) Quando você marca a caixa de seleção **Lembrar-me** no login, um cookie extra é armazenado no computador do usuário. • Sua finalidade é restabelecer automaticamente a sessão para as visitas subsequentes do usuário conectado. • Isso representa um risco de segurança, pois permite que a sessão do usuário esteja ativa até que ele faça logout intencionalmente. A probabilidade de um ataque para este cenário aumenta quando o usuário final deixa o navegador sem supervisão ou se ele for comprometido por um ataque diferente.
Referências	Remover a caixa de seleção Lembrar-me

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exigir limpeza da área de transferência ao colocar a aplicação para celular em segundo plano [Novo na Central de segurança 1.3]

A propriedade *glide.sg.clear_pasteboard_when_backgrounded* controla se o texto copiado do aplicativo para celular da ServiceNow é mantido na ferramenta de recorte e na área de transferência depois que o app está em segundo plano.

Mais informações

Atributo	Descrição
Nome da configuração	*glide.sg.clear_pasteboard_when_backgrounded*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	booliano
Valor recomendado	verdadeiro
Valor-padrão	falso
Categoria	Proteção de dados
Risco à segurança	• Pontuação de gravidade: 3,5 • Pontuação de CVSS: baixa • Detalhes do risco à segurança: se esta propriedade não estiver definida com o valor recomendado de "verdadeiro", as informações confidenciais poderão ser divulgadas na área de transferência do Android ou do iOS, onde poderão ser expostas a outras aplicações no dispositivo.
Dependências e pré-requisitos	Nenhum(a)
Impacto funcional	Esta propriedade limpa a área de transferência copiar/colar quando o app da ServiceNow entra em segundo plano.

Como restringir atualizações de casos de RH nos e-mails pessoais [Novo na Central de segurança 1.3 e atualizado na 1.5]

Use a propriedade *sn_hr_core.restrict_guest_email* para controlar se um usuário pode responder a um caso de RH pelo seu e-mail pessoal.

Quando a propriedade *sn_hr_core.restrict_guest_email* não está definida como verdadeira, um usuário pode enviar um e-mail de uma conta pessoal fazendo referência ao caso de RH a ser incluído nas anotações de trabalho. Isso pode resultar em pequenos problemas de confidencialidade ou integridade se o e-mail pessoal for comprometido ou se comunicar de forma insegura. Um administrador pode querer impedir que os usuários respondam a casos de RH de seu e-mail pessoal, já que ele não pode ter certeza de que o usuário acessará a conta de e-mail pessoal.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mais informações

Atributo	Descrição
Nome da configuração	*sn_hr_core.restrict_guest_email*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	booliano
Valor recomendado	verdadeiro
Valor-padrão	falso
Categoria	Proteção de dados
Risco à segurança	• Pontuação de gravidade: 3,5 • Pontuação de CVSS: baixa • Detalhes do risco à segurança: não ter essa propriedade definida como verdadeira pode resultar em pequenos problemas de confidencialidade ou integridade se o e-mail pessoal for comprometido ou se comunicar de forma insegura.
Dependências e pré-requisitos	Nenhum(a)
Impacto funcional	Esta propriedade controla se uma resposta enviada de um endereço de e-mail pessoal atualizará ou não um caso de RH. Se definida como verdadeira, qualquer resposta proveniente de e-mail pessoal será adicionada às anotações do caso. Se falsa, o caso e as anotações não serão atualizados.

Restringir parâmetros OAuth no corpo de POST [Novo na Central de segurança 1.3]

A propriedade *glide.oauth.allow.parameters.in.post.body.only* controla a aceitação de tokens de acesso da autenticação OAuth de entrada. Os tokens de acesso são confidenciais e só devem ser aceitos quando localizados no corpo de uma solicitação POST.

Mais informações

Atributo	Descrição
Nome da configuração	*glide.oauth.allow.parameters.in.post.body.only*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	booliano
Valor recomendado	verdadeiro
Valor-padrão	verdadeiro
Categoria	Proteção de dados

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Risco à segurança	• Pontuação de gravidade: 7,4 • Pontuação de CVSS: alta • Detalhes do risco à segurança: se *glide.oauth.allow.parameters.in.post.body.only* não estiver definido com o valor recomendado de verdadeiro, os tokens de acesso poderão estar presentes no parâmetro da solicitação GET, que poderia permanecer nos logs de infraestrutura do cliente e resultar em controle da conta se esses logs forem vazados.
Dependências e pré-requisitos	Nenhum
Referências	• OAuth 2.0 • Gerenciar tokens OAuth
Impacto funcional	Garante que o processador oauth_token.do aceite somente parâmetros de corpo POST como entrada para todos os tipos de concessão suportados.

Manipulação de erros e registro em log

A categoria de manipulação de erros e registro em log trata da qualidade e do detalhamento das informações registradas em log para as partes interessadas.

Isso inclui garantir que os logs e as mensagens de erro não coletem informações confidenciais, protejam corretamente os dados de acordo com a classificação e tenham uma vida útil apropriada. Além disso, esta categoria está relacionada à manipulação de erros apropriada e à não divulgação de erros confidenciais para os usuários finais, como rastreamentos de pilha detalhados para exceções não tratadas com implicações de segurança.

Desabilitar agente de log para usuários de baixo privilégio na área restrita de script

Gerenciar a capacidade do sistema Glide de registrar scripts que estão sendo executados no ambiente de área restrita.

Use a propriedade *glide.security.sandbox_no_logging* para controlar a capacidade do sistema Glide de registrar scripts que estão sendo executados no ambiente de área restrita. Se *glide.security.sandbox_no_logging* estiver definido como **falso**, o registro em log estará disponível para usuários com menos privilégios que utilizam scripts na área restrita. Esta é uma possível vulnerabilidade de segurança porque usuários com poucos privilégios podem injetar logs, permitindo que um agente mal-intencionado ofusque um ataque. Configure a propriedade como **verdadeira** para impedir que usuários com menos privilégios que utilizam um script em área restrita tenham a funcionalidade de registro em log.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mais informações

Atributo	Descrição
Nome da configuração	*glide.security.sandbox_no_logging*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	booliano
Valor recomendado	verdadeiro
Valor-padrão	verdadeiro
Categoria	Manipulação de erros e registro em log
Risco à segurança	• Pontuação de gravidade: 2,2 • Pontuação de CVSS: baixa • Detalhes do risco à segurança: definir esta propriedade como **falsa** habilita o registro em log para usuários com menos privilégios, o que pode permitir que um agente mal-intencionado ofusque um ataque.
Dependências e pré-requisitos	Nenhum

Desabilitar depuração do cookie de segurança

Gerencie as mensagens de log relacionadas a cookies em sua instância.

Use a propriedade *glide.secure_cookie.debug* para gerenciar suas mensagens de log relacionadas a cookies. Se esta propriedade for definida como **falsa**, nenhuma mensagem de log será exibida. Se estiver definida como **verdadeira**, as mensagens nas classes `SecureUserCookie` e `Cookie` serão registradas em log. Isso pode levar à exposição de informações confidenciais em sua instância.

Mais informações

Atributo	Descrição
Nome da configuração	*glide.secure_cookie.debug*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	booliano
Valor recomendado	falso
Valor-padrão	falso
Categoria	Manipulação de erros e registro em log

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Risco à segurança	• Pontuação de gravidade: 4,2 • Pontuação do CVSS: média • Detalhes do risco à segurança: configurar essa propriedade como **verdadeira** pode levar à exposição de informações confidenciais.
Dependências e pré-requisitos	Nenhum

Desativação de mensagens de erro de SQL [Atualizado na Central de segurança 1.3]

Utilize a propriedade *glide.db.loguser* para desabilitar a renderização de mensagens de erro de SQL em um navegador.

Mais informações

Atributo	Descrição
Nome da propriedade	*glide.db.loguser*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Categoria	Manipulação de erros e registro em log
Finalidade	Desabilitar a exibição de mensagens de erro de SQL no navegador.
Tipo	booliano
Valor recomendado	falso
Valor padrão	verdadeiro
Classificação de risco de segurança	3,1
Impacto funcional	(Baixo) Esta correção desabilita a renderização de mensagens de erro de SQL. Não há impacto em nenhuma funcionalidade.
Risco à segurança	(Médio) Nenhuma informação confidencial do SQL que possa ajudar um invasor deve aparecer como parte de uma mensagem de erro em uma página da Web.

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Habilitar o log de auditoria de MID [Novo na Central de segurança 1.3 e atualizado na 1.5]

O registro em log de auditoria de comando do MID Server registra detalhes como nome do comando, hash do comando, nome da credencial usada e status de execução.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Depois de habilitados, os logs de auditoria podem ser visualizados por usuários com a função agent_security_admin na tabela ecc_agent_command_audit_log ou no caminho **Mid Server** > **Logs de auditoria de comando**.

Defina *mid.log.command_audit.enable* como verdadeiro na tabela ecc_agent_property para ativar a auditoria para comandos executados pelo MID Server.

Mais informações

Atributo	Descrição
Nome da configuração	*mid.log.command_audit.enable*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	booliano
Valor recomendado	verdadeiro
Valor-padrão	falso
Categoria	Manipulação de erros e registro em log
Risco à segurança	• Pontuação de gravidade: 2,2 • Pontuação de CVSS: baixa • Detalhes do risco à segurança: em caso de uma investigação de segurança, as equipes de resposta do incidente podem usar esta tabela para auditar os comandos executados no MID Server. Sem este log, pode não haver detalhes suficientes para responder a situações como uso não autorizado de conta.
Dependências e pré-requisitos	Nenhum

Habilitar o plug-in de tabelas protegidas [Novo na Central de segurança 1.3]

Use a propriedade *com.glide.security.protected_table.enabled* para impedir que usuários com privilégios mais altos adulterem tabelas de log.

Quando a propriedade *com.glide.security.protected_table.enabled* for definida como **verdadeira**, o plug-in de tabelas protegidas será usado para impedir que usuários com privilégios mais altos em uma instância adulterem tabelas de log. As seguintes tabelas de log têm proteções especiais quando essa propriedade é definida como **verdadeira**:

- syslog (Nenhuma substituição de banco de dados)
- syslog_transaction
- sys_outbound_http_log
- sysevent
- sys_audit
- sys_push_notification
- protected_table_configuration (Nenhuma substituição de banco de dados)

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A integridade dos logs é importante para que o administrador do cliente determine atividades mal-intencionadas em uma instância.

Mais informações

Atributo	Descrição
Nome da configuração	*com.glide.security.protected_table.enabled*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	booliano
Valor recomendado	verdadeiro
Valor-padrão	falso
Categoria	Manipulação de erros e registro em log
Risco à segurança	• Pontuação de gravidade: 4,5 • Pontuação do CVSS: média • Detalhes do risco à segurança: não definir *com.glide.security.protected_table.enabled* com o valor recomendado de "verdadeiro" permite que usuários com privilégios mais altos em uma instância adulterem tabelas de log.
Dependências e pré-requisitos	Nenhum
Referências	Logs do sistema

Registrar todos os campos de solicitação http de saída [Removido na Central de Segurança v1.3.2]

Configure a propriedade *glide.outbound_http.security.log.allow.all.fields* como falsa para impedir que campos HTTP de saída confidenciais sejam registrados em texto sem formatação.

Se esta propriedade não estiver definida com o valor recomendado de **falso**, campos HTTP de saída confidenciais poderão ser registrados em texto sem formatação. Isso pode reduzir a postura de segurança da rede da sua empresa porque as solicitações de saída com dados e credenciais confidenciais podem ser registradas em texto sem formatação não criptografado e, assim, podem ser visualizadas por usuários com menos privilégios.

Mais informações

Atributo	Descrição
Nome da configuração	*glide.outbound_http.security.log.allow.all.fields*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	inteiro
Valor recomendado	30
Valor-padrão	30

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Categoria	Manipulação de erros e registro em log
Risco à segurança	• Pontuação de gravidade: 6,8 • Pontuação do CVSS: média • Detalhes do risco à segurança: não definir esta propriedade como **falsa** aumenta a chance de campos de saída confidenciais serem registrados em texto sem formatação, o que é um risco à segurança.
Dependências e pré-requisitos	Nenhum

Registros de sanitização de HTML

Configure a propriedade *glide.html_sanitize.discarded_log.enable* para determinar se os eventos de sanitização de HTML serão registrados na sua instância.

Se esta propriedade não estiver definida com o valor recomendado de **verdadeiro**, os eventos de sanitização de HTML não serão registrados na tabela *sys_log*. A falta de registro em log pode afetar negativamente os recursos de detecção e investigação de segurança automatizados da instância.

Mais informações

Atributo	Descrição
Nome da configuração	*glide.html_sanitize.discarded_log.enable*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	booliano
Valor recomendado	verdadeiro
Valor-padrão	verdadeiro
Categoria	Manipulação de erros e registro em log
Risco à segurança	• Pontuação de gravidade: 2.4 • Pontuação de CVSS: baixa • Detalhes do risco de segurança: se esta propriedade não estiver definida com o valor recomendado de **verdadeiro**, os eventos de sanitização de HTML não serão registrados na tabela *sys_log*, o que pode afetar os recursos automatizados de detecção e investigação de segurança.
Dependências e pré-requisitos	Nenhum
Referências	Habilitar o limpador de HTML

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Registrar eventos de auditoria de sessão [Novo na Central de segurança 1.3]

Defina a propriedade *glide.authenticate.session_access.log_audit_event* como **verdadeira** para que os eventos de auditoria de sessão sejam criados na tabela *sys_session_access_audit*.

As informações de registro em log sobre o acesso à sessão ajudará na análise de ataques de segurança cibernética. As informações registradas em log incluem usuário, ID de sessão (não confidencial), endereço IP, funções e políticas.

Nota: A propriedade do sistema *glide.authenticate.session_access.log_audit_event* é específica para o acesso com abordagem zero trust. Para obter mais informações, consulte Zero Trust Access.

Mais informações

Atributo	Descrição
Nome da configuração	*glide.authenticate.session_access.log_audit_event*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	booliano
Valor recomendado	verdadeiro
Valor-padrão	verdadeiro
Categoria	Manipulação de erros e registro em log
Risco à segurança	• Pontuação de gravidade: 6,3 • Pontuação do CVSS: média • Detalhes do risco de segurança: não configurar esta propriedade com o valor recomendado de verdadeiro impede que os eventos sejam registrados. Isso pode impedir que você identifique agentes mal-intencionados no caso de um ataque cibernético.
Dependências e pré-requisitos	Nenhum

Registrar representação de usuário

Configure *glide.sys.log_impersonation* para controlar se os eventos de representação do usuário são registrados em log em sua instância.

Se essa propriedade não estiver definida com o valor recomendado de **verdadeiro**, os eventos de representação do usuário não serão mais registrados em log. A falta de registro em log pode afetar negativamente os recursos automatizados de detecção e investigação de segurança da sua instância.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mais informações

Atributo	Descrição
Nome da configuração	*glide.sys.log_impersonation*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	booliano
Valor recomendado	verdadeiro
Valor-padrão	verdadeiro
Categoria	Manipulação de erros e registro em log
Risco à segurança	• Pontuação de gravidade: 6,4 • Pontuação do CVSS: média • Detalhes do risco à segurança: se essa propriedade não estiver definida como **verdadeira**, os eventos de representação do usuário não serão mais registrados, o que pode afetar os recursos de detecção e investigação de segurança da sua instância.
Dependências e pré-requisitos	Nenhum
Referências	Representação de usuários

Desativar mensagens de erro SQL detalhadas do processador de importação

Configure esta propriedade para controlar se as mensagens de erro SQL detalhadas são exibidas.

Se a propriedade estiver definida como **falsa**, será exibida uma mensagem de erro SQL detalhada, que pode vazar informações confidenciais. Para evitar isso, defina a propriedade como **verdadeira** para exibir uma mensagem genérica.

Mais informações

Atributo	Descrição
Nome da configuração	*glide.import.error_message.generic*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	booliano
Valor recomendado	verdadeiro
Valor-padrão	verdadeiro
Categoria	Manipulação de erros e registro em log
Risco à segurança	• Pontuação de gravidade: 3,1 • Pontuação de CVSS: baixa

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
	• Detalhes do risco à segurança: definir a propriedade como **falsa** habilita mensagens SQL detalhadas, o que pode resultar no vazamento de informações.
Dependências e pré-requisitos	Nenhum

Arquivo e recursos

A categoria de arquivos e recursos garante que as aplicações manipulem dados de arquivos não confiáveis com segurança e armazenem dados não confiáveis de fontes não confiáveis com permissões limitadas em um local apropriado.

Isso inclui controles, tais como evitar a negação de serviço por meio de tipos de arquivo grandes ou inesperados, validar o tipo de arquivo e impedir a travessia de caminho.

Proibir o download de arquivos infectados

Gerencie esta propriedade para controlar se os rastreamentos de pilha são exibidos na sua instância.

Quando a propriedade *com.glide.snap.infected_download_allowed* é definida como verdadeira, os usuários podem baixar anexos não verificados caso o serviço de antivírus esteja inativo ou inacessível. Essa situação pode expor os usuários ao risco de baixar um arquivo mal-intencionado e, consequentemente, ao risco de invasão da área de trabalho deles, especialmente se não houver outra proteção de endpoint instalada no dispositivo.

Mais informações

Atributo	Descrição
Nome da configuração	*com.glide.snap.infected_download_allowed*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	booliano
Valor recomendado	falso
Valor-padrão	falso
Categoria	Arquivo e recursos
Risco à segurança	• Pontuação de gravidade: 6,7 • Pontuação do CVSS: média • Detalhes do risco de segurança: não definir esta propriedade com o valor recomendado de falso pode expor sua instância ao download de arquivos mal-intencionados.
Dependências e pré-requisitos	Nenhum

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Ativar pontuação e filtragem de spam de e-mail [Atualizado na Central de segurança 1.3]

Instale o plug-in Email Filter (*com.glide.email_filter*) para instalar a filtragem de e-mail na instância. Esta filtragem identifica cabeçalhos existentes, o que permite que você decida o que fazer com o e-mail com base no cabeçalho associado.

Cada mensagem enviada por meio de servidores de e-mail da Now Platform é avaliada quanto à probabilidade de ser spam.

Nota: Se uma instância usar um servidor de e-mail privado, este tópico não será aplicável. Para mais informações, consulte Pontuação e filtragem de spam de e-mail.

Pré-requisitos

Antes de definir esta propriedade:

Defina a propriedade *glide.email.read.active* como verdadeira. Para saber mais, consulte Habilitar usando seu próprio servidor POP3.

Mais informações

Atributo	Descrição
Nome do Plug-in	*com.glide.email_filter*
Tipo de configuração	Definição do sistema > Plug-ins
Categoria	Arquivo e recursos
Finalidade	Aplicar a filtragem para evitar o envio de e-mails de spam.
Valor recomendado	Ativo
Valor padrão	Nenhum. Este é um plug-in, não uma propriedade do Glide. Portanto, não há valor padrão.
Classificação de risco de segurança	8,1
Impacto funcional	(Baixo) O e-mail nunca é filtrado, bloqueado ou colocado em quarentena da instância como parte da pontuação de spam. Ele é apenas pontuado e enviado para a instância. Toda a filtragem é feita na instância com o plug-in Filtros de e-mail.
Risco à segurança	(Moderado) Filtros de e-mail permite que os administradores usem um construtor de condição ou script condicional para especificar quando ignorar e-mails mal-intencionados de entrada de remetentes conhecidos/desconhecidos.
Referências	Filtros de e-mail https://support.servicenow.com/kb_view.do?sysparm_article=KB0549426

Para saber mais sobre como ativar um plug-in, consulte Ativar um plug-in.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Habilitar a varredura antivírus

A propriedade *com.glide.snap.enable_scan* ativa a funcionalidade de varredura antivírus.

Defina *com.glide.snap.enable_scan* com o valor recomendado de **verdadeiro** para habilitar a varredura antivírus.

Aviso: Esta é uma propriedade tipo porto seguro, o que significa que o valor não pode ser alterado após ser mudado. A reversão não é possível.

Mais informações

Atributo	Descrição
Nome da propriedade	*com.glide.snap.enable_scan*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Categoria	Arquivo e recursos
Finalidade	Para habilitar ou desabilitar a varredura antivírus na instância específica.
Valor recomendado	verdadeiro
Valor-padrão	verdadeiro
Tipo de dados	booliano
Risco à segurança	(Alto) A varredura antivírus ajudar a proteger sua instância contra infecções de vírus que podem ser introduzidas por anexos de arquivo aos registros do sistema, como incidentes, problemas e histórias.
Classificação de risco de segurança	7.7

Como restringir tipos de arquivos para download em conteúdo estático [Atualizado na Central de segurança 1.3]

Use a propriedade *glide.ui.strict_customer_uploaded_static_content* para habilitar restrições nos tipos de arquivo que podem ser baixados quando forem carregados usando a funcionalidade Carregar arquivo.

Você usa esta propriedade com a propriedade *glide.ui.strict_customer_uploaded_content_types*, que cria uma lista delimitada por vírgulas de tipos de arquivo restritos para download. Para saber mais, consulte Tipos de arquivo para download.

Aviso: O valor desta propriedade é uma substituição sem banco de dados. Não pode ser alterado ou substituído.

Mais informações

Atributo	Descrição
Nome da propriedade	*glide.ui.strict_customer_uploaded_static_content*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Categoria	Arquivo e recursos
Finalidade	Garantir que os tipos de arquivo seguros sejam baixados da aplicação.
Valor recomendado	verdadeiro
Valor-padrão	verdadeiro
Classificação de risco de segurança	3,1
Impacto funcional	(Baixo) Esta correção impõe restrição de downloads de arquivo com base nos valores especificados na propriedade *glide.ui.strict_customer_uploaded_content_types*. Para saber mais, consulte Tipos de arquivo para download.
Risco à segurança	(Baixo) As restrições de download de arquivo devem ser aplicadas a todas as fontes de entrada de usuário não confiáveis.

Como limitar o tamanho de anexos em fluxos de treinamento e previsão dos endpoints do GraphQL [Novo na Central de segurança 1.3 e atualizado na 1.5]

A propriedade *glide.platform_ml_di.max_attachment_size_graphql* controla o limite de tamanho máximo permitido para retornar anexos em endpoints de GraphQL de fluxos de treinamento e previsão.

Mais informações

Atributo	Descrição
Nome da configuração	*glide.platform_ml_di.max_attachment_size_graphql*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	inteiro
Valor recomendado	5.242.880
Valor-padrão	5.242.880
Categoria	Arquivo e recursos
Risco à segurança	• Pontuação de gravidade: 4,3 • Pontuação do CVSS: média • Detalhes do risco à segurança: se essa propriedade não estiver definida com o valor recomendado de 5.242.880 ou menos, o retorno de arquivos grandes poderá causar uma DoS (denial of service, negação de serviço).
Dependências e pré-requisitos	Nenhum

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Como limitar o tamanho de anexos em fluxos de treinamento e previsão [Novo na Central de segurança 1.3 e atualizado na 1.5]

A propriedade *glide.platform_ml_di.max_attachment_size* controla o limite de tamanho máximo permitido para retornar anexos em fluxos de treinamento e previsão.

Mais informações

Atributo	Descrição
Nome da configuração	*glide.platform_ml_di.max_attachment_size*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	inteiro
Valor recomendado	4.000.000
Valor-padrão	4.000.000
Categoria	Arquivo e recursos
Risco à segurança	• Pontuação de gravidade: 4,3 • Pontuação do CVSS: média • Detalhes do risco à segurança: se *glide.platform_ml_di.max_attachment_size* não estiver definido com o valor recomendado de 4.000.000 ou menos, o retorno de arquivos grandes poderá causar uma DoS (denial of service, negação de serviço).
Dependências e pré-requisitos	Nenhum

Como limitar o tamanho do corpo da resposta HTTP [Novo na Central de segurança 1.3 e atualizado na 1.5]

Configure as propriedades *glide.http.response.get_body.limit.enabled* e *glide.http.response.get_body.limit* para proteger sua instância contra *OutOfMemoryExceptions*.

As propriedades *glide.http.response.get_body.limit* e *glide.http.response.get_body.limit.enabled* foram introduzidas para habilitar a nova funcionalidade que impede a geração de *OutOfMemoryExceptions* como resultado de uma resposta de solicitação muito longa. *OutOfMemoryExceptions* podem causar ataques de DoS (denial of service, negação de serviço), bem como outros problemas que podem ajudar os invasores a comprometer uma instância.

Para proteger sua instância contra essas vulnerabilidades de segurança, certifique-se de que *glide.http.response.get_body.limit.enabled* esteja definido como verdadeiro e que *glide.http.response.get_body.limit* não tenha mais de 524.288.000 megabytes (500 MB).

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mais informações

Atributo	Descrição
Nome da configuração	*glide.http.response.get_body.limit.enabled* e *glide.http.response.get_body.limit*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	booliano
Valor recomendado	verdadeiro
Valor-padrão	verdadeiro
Categoria	Arquivo e recursos
Risco à segurança	• Pontuação de gravidade: 6,4 • Pontuação do CVSS: média • Detalhes do risco à segurança: não definir essas propriedades com os valores recomendados pode tornar sua instância vulnerável a *OutOfMemoryExceptions* e a ataques de negação de serviço.
Dependências e pré-requisitos	Nenhum(a)
Impacto funcional	Esta propriedade reduz as chances de *OutOfMemoryException* quando um cliente carrega acidentalmente um arquivo grande na memória.

Limite máximo de anexos no e-mail

Configure o número de anexos de e-mail de entrada em sua instância.

As propriedades e *glide.email.inbound.max_attachment_count* controlam o número máximo de anexos de entrada no e-mail da sua instância. Se esta propriedade não estiver definida com o valor recomendado de **30** ou menos, os e-mails de entrada podem fazer com que sua instância perca desempenho.

Mais informações

Atributo	Descrição
Nome da configuração	*glide.email.inbound.max_attachment_count*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	inteiro
Valor recomendado	30
Valor-padrão	30
Categoria	Arquivo e recursos

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Risco à segurança	• Pontuação de gravidade: 5,3 • Pontuação do CVSS: média • Detalhes do risco de segurança: definir o valor da propriedade como maior que 30 pode levar a problemas de perda de desempenho.
Dependências e pré-requisitos	Nenhum
Referências	Propriedades do e-mail

Como minimizar o tamanho permitido do anexo [Atualizado na Central de segurança 1.3]

Configure a propriedade *com.glide.attachment.max_size* para controlar o tamanho máximo permitido para um anexo carregado.

Esta propriedade controla o tamanho máximo de um anexo para carregamento. Se esta propriedade não estiver definida com o valor recomendado de **1024** ou menos, a plataforma poderá aceitar arquivos grandes que podem preencher o armazenamento e levar a um ataque de negação de serviço (DoS).

Nota: O tamanho real de um anexo é calculado multiplicando 1024 x 1024 pelo valor da propriedade. Se o valor da propriedade for **1024**, o tamanho máximo permitido para o anexo será de 1 GB.

Mais informações

Atributo	Descrição
Nome da configuração	*com.glide.attachment.max_size*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	inteiro
Valor recomendado	1024
Valor-padrão	4096
Categoria	Arquivo e recursos
Risco à segurança	• Pontuação de gravidade: 6,5 • Pontuação do CVSS: média • Detalhes do risco de segurança: se esta propriedade não estiver definida como **1024** ou menos, a plataforma poderá aceitar arquivos grandes que podem levar a ataques DoS.
Dependências e pré-requisitos	Nenhum
Referências	Propriedades de limite de anexos

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Validar tipo de arquivo MIME no SOAP Web Service AttachmentCreator [Novo na Central de segurança 1.3]

A propriedade *glide.attachment.enforce_security_validation* determina se os arquivos MIME (Multipurpose Internet Mail Extensions, extensões multifunção para mensagens de internet) passam por validação.

Se *glide.attachment.enforce_security_validation* não estiver definido com o valor recomendado de **verdadeiro**, não haverá validação de arquivos MIME, permitindo que arquivos mal-intencionados sejam carregados com extensões de arquivo incorretas. Quando esta propriedade é definida como **verdadeira**, os arquivos são carregados com a extensão de tipo de arquivo correta.

Mais informações

Atributo	Descrição
Nome da configuração	*glide.attachment.enforce_security_validation*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	Booliano
Valor recomendado	verdadeiro
Valor-padrão	verdadeiro
Categoria	Arquivo e recursos
Risco à segurança	• Pontuação de gravidade: 7,5 • Pontuação de CVSS: alta • Detalhes do risco à segurança: se a propriedade estiver definida como falsa, não haverá validação de arquivos MIME durante os uploads. Isso pode permitir que arquivos mal-intencionados sejam disfarçados, alterando sua extensão.
Dependências e pré-requisitos	Nenhum
Referências	https://developer.mozilla.org/en-US/docs/Web/HTTP/Basics_of_HTTP/MIME_types/Common_types
Impacto funcional	Defina esta configuração de proteção como verdadeira para executar as validações de tipo mime e de extensão de arquivo em anexos de arquivo carregados. Nenhuma validação será executada se esta propriedade estiver definida como falsa. Esta propriedade é definida como verdadeira por padrão.

Código mal-intencionado

A categoria Código mal-intencionado garante que sejam feitos os melhores esforços para confirmar que seu código está livre de vulnerabilidades e funcionalidades indesejadas.

Isso inclui garantir o tratamento seguro e adequado de atividades mal-intencionadas, impedir ataques baseados em tempo, bloquear comunicações de saída para destinos não confiáveis e barrar a inclusão de qualquer código não autorizado ou controlado pelo

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

invasor. Essa categoria inclui bibliotecas de auditoria ou de terceiros da base de código da aplicação.

Bloquear dispositivos móveis com raiz ou jailbreak

Proteja sua instância, impedindo o acesso não autorizado de dispositivos com jailbreak.

Use a propriedade *glide.sg.allow_rooted_jailbroken_device* para proteger sua instância contra acesso não autorizado de dispositivos com jailbreak. Se um usuário tentar se autenticar em uma instância usando um aplicativo para celular enquanto esta propriedade estiver definida como **falsa**, ele receberá o seguinte alerta: `Este dispositivo parece estar com jailbreak e não pode ser usado para acessar esta instância. Entre em contato com o administrador da ServiceNow.` O app permanece congelado enquanto a mensagem de alerta é exibida, e a única maneira de descartar essa mensagem é selecionar **Sair**. Se esta propriedade for definida como **verdadeira**, os usuários serão autenticados em uma instância usando um dispositivo com jailbreak.

Mais informações

Atributo	Descrição
Nome da configuração	*glide.sg.allow_rooted_jailbroken_device*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	booliano
Valor recomendado	falso
Valor-padrão	falso
Categoria	Código mal-intencionado
Risco à segurança	• Pontuação de gravidade: 4,5 • Pontuação do CVSS: média • Detalhes do risco à segurança: a falta de segurança em dispositivos com jailbreak os torna grandes alvos para agentes mal-intencionados. Ter entidades não autorizadas acessando dados corporativos pode prejudicar a postura de segurança de uma rede corporativa.
Dependências e pré-requisitos	Nenhum
Referências	Controle de acesso

Ativação da assinatura de código para dados e scripts de configuração de aplicações [Removido na Central de segurança 1.3]

Gerencie a Assinatura de código para scripts e dados de configuração de aplicação em sua instância.

A assinatura de código pode ajudar a melhorar a segurança validando dados e scripts de configuração de aplicação confidenciais antes de serem usados. A assinatura de código cria assinaturas digitais para que os dados que posteriormente serão verificados confirmem a autenticidade e a integridade dos dados. Esta verificação evita que dados ou scripts mal-intencionados sejam usados na instância, o que pode levar ao comprometimento total da instância.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Use a propriedade *com.snc.kmf.signature.validation.flag* para gerenciar a Assinatura de código para scripts e dados de configuração de aplicação. Quando essa propriedade é definida como **verdadeira**, a Assinatura de código é habilitada para scripts e dados de configuração de aplicação.

Aviso: Esta é uma propriedade tipo porto seguro, o que significa que o valor não pode ser alterado após ser mudado. A reversão não é possível.

Mais informações

Atributo	Descrição
Nome da configuração	*com.snc.kmf.signature.validation.flag*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	booliano
Valor recomendado	verdadeiro
Valor-padrão	falso
Categoria	Código mal-intencionado
Risco à segurança	• Pontuação de gravidade: 6 • Pontuação do CVSS: média • Detalhes do risco à segurança: definir esta propriedade como **verdadeira** habilita a Assinatura de código, o que ajuda a aumentar a segurança validando scripts e dados confidenciais de configuração da aplicação.
Dependências e pré-requisitos	Nenhum

Gestão de sessões

Esta categoria analisa a segurança do estado da aplicação para um usuário. As sessões devem ser exclusivas para cada indivíduo, não podendo ser adivinhadas ou compartilhadas e devem ser invalidadas após períodos de inatividade ou quando não forem necessárias. Isso inclui fatores como atributos de cookie para sessões baseadas em cookie, geração de token de sessão e armazenamento e requisitos para reautenticação federada.

Como minimizar a duração do tempo limite absoluto da sessão [Atualizado na Central de segurança 1.3]

Use a propriedade *glide.ui.user_cookie.max_life_span_in_days* para definir uma duração máxima para os cookies de usuários criados quando os usuários fazem login com a caixa de seleção **Lembrar-me** selecionada. Quando o cookie expirear, os usuários que tiverem selecionado a caixa de seleção **Lembrar-me** serão forçados a se reautenticar na instância.

Ela habilita a validade do cookie de usuário durante dias específicos a partir de quando o cookie foi publicado pela primeira vez. O valor padrão é 30 dias e o limite máximo é de 365 dias.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Para impor um tempo máximo de sesssão para sessões de usuário ativas, consulte Gerenciamento de sessões de usuário.

Mais informações

Atributo	Descrição
Nome da propriedade	*glide.ui.user_cookie.max_life_span_in_days*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Categoria	Gestão de sessões
Finalidade	Para forçar os usuários que selecionaram a caixa de seleção **Lembrar-me** a se reautenticar após dias específicos.
Valor recomendado	Menor ou igual a 30
Valor padrão	30 dias
Impacto funcional	(Médio) Esta propriedade impõe um novo login obrigatório, evitando qualquer tipo de rotação de cookie após um determinado intervalo de tempo.
Classificação de risco de segurança	4,2
Risco à Segurança	(Médio) Os cookies do usuário ativos por um período indefinido de tempo são um risco à segurança e devem expirar em uma configuração baseada em tempo.
Referências	Propriedades do sistema disponíveis Lembrar minhas informações

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Definir funções de exceção de tempo limite de sessão ativa [Novo na Central de segurança 1.3]

A propriedade *glide.active.session.timeout.exception.roles* controla as funções que estão isentas de um tempo limite da sessão ativa.

O tempo limite da sessão ativa impede que uma sessão sequestrada seja usada indefinidamente sem a necessidade de reinserir as informações de autenticação. Para corrigir esse risco de segurança, certifique-se de que a propriedade *glide.active.session.timeout.exception.roles* esteja definida como **edge_encryption, mid_server**.

Mais informações

Atributo	Descrição
Nome da configuração	*glide.active.session.timeout.exception.roles*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Tipo de dados	cadeia de caracteres
Valor recomendado	edge_encryption, mid_server
Valor-padrão	edge_encryption, mid_server
Categoria	Gestão de sessões
Risco à segurança	• Pontuação de gravidade: 7,1 • Pontuação de CVSS: alta • Detalhes do risco à segurança: considere somente uma exceção de tempo limite da sessão ativa para funções internas da conta de integração. Se uma função receber uma exceção para o tempo limite da sessão, e essa função for atribuída a um usuário que é vítima de um ataque de sequestro de sessão, o invasor poderá continuar autenticando essa sessão indefinidamente. Isso pode aumentar o impacto de um incidente de segurança, permitindo que um invasor tenha mais tempo para usar uma conta sequestrada.
Dependências e pré-requisitos	Nenhum

Habilitar CookieDoUsuário versão 3.1

Gerencie a versão do CookieDoUsuário que está habilitada em sua instância para proteger o armazenamento da chave secreta no código de origem.

O CookieDoUsuário v3 é gerado somente quando a propriedade *glide.ui.secure.cookies.use_kmf* está desabilitada. O CookieDoUsuário v3 não é seguro porque a chave secreta para HMAC (hash-based message authentication codes, códigos de autenticação de mensagem baseados em hash) é armazenada no código de origem, que é idêntico para todos os clientes. Um agente mal-intencionado pode usar uma chave secreta para tentar sequestrar sessões do usuário. Para corrigir esta ameaça à segurança, certifique-se de que a propriedade *glide.ui.secure.cookies.use_kmf* que utiliza o CookieDoUsuário v3.1 esteja definida como **verdadeira**. A chave secreta é guardada em um armazenamento seguro, como KMF.

Mais informações

Atributo	Descrição
Nome da configuração	*glide.ui.secure.cookies.use_kmf*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	booliano
Valor recomendado	verdadeiro
Valor-padrão	falso
Categoria	Gestão de sessões

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Risco à segurança	• Pontuação de gravidade: 7,1 • Pontuação de CVSS: alta • Detalhes do risco de segurança: definir isto como **falso** é uma vulnerabilidade de segurança porque a chave secreta para HMAC (hash-based message authentication codes, códigos de autenticação de mensagem baseados em hash) está sendo armazenada no código de origem.
Dependências e pré-requisitos	Nenhum

Impor redefinição de senha em solicitações de API

Gerencie como a funcionalidade de redefinição de senha opera em sua instância.

Quando um usuário recebe a mensagem **A senha precisa ser redefinida**, ele deve inserir uma nova senha na próxima tentativa de autenticação. Esta propriedade controla se a redefinição de senha é obrigatória antes de fazer chamadas de API. Se esta propriedade não estiver definida com o valor recomendado de **verdadeira**, as contas de usuário marcadas com a mensagem **A senha precisa ser redefinida** ainda poderão executar operações consultando a API da tabela por meio da autenticação básica. Esta vulnerabilidade de segurança pode permitir o vazamento de informações se uma conta inativa for comprometida.

Mais informações

Atributo	Descrição
Nome da configuração	*glide.authenticate.api.user.reset_password.mandatory*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	booliano
Valor recomendado	verdadeiro
Valor-padrão	falso
Categoria	Gestão de sessões
Risco à segurança	• Pontuação de gravidade: 8,1 • Pontuação de CVSS: alta • Detalhes do risco à segurança: definir esta propriedade como **falsa** pode levar ao vazamento de informações se uma conta inativa for comprometida.
Dependências e pré-requisitos	Nenhum

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Ativar sinalizador de cookie somente HTTP [Atualizado na Central de segurança 1.3]

Use a propriedade *glide.cookies.http_only* para habilitar o atributo HTTPOnly para cookies confidenciais.

Use o atributo HTTPOnly para impedir ataques, como script entre sites, porque ele não permite o acesso ao cookie usando um script do lado do cliente, como JavaScript. Ele não elimina os riscos de script entre sites, mas elimina alguns vetores de exploração.

Aviso: Esta é uma propriedade tipo porto seguro, o que significa que o valor não pode ser alterado após ser mudado. A reversão não é possível.

Mais informações

Atributo	Descrição
Nome da propriedade	*glide.cookies.http_only*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Categoria	Gestão de sessões
Finalidade	Reduzir o risco de um script do lado do cliente acessar o cookie protegido.
Valor recomendado	verdadeiro
Valor-padrão	verdadeiro
Classificação de risco de segurança	8
Impacto funcional	(Baixo) Esta correção adiciona um sinalizador HTTPOnly extra nos cookies da sessão, protegendo-os contra roubos. • Se você tiver uma funcionalidade personalizada que requer JavaScript para acessar o cookie do usuário, essa funcionalidade será interrompida. Não será o caso em circunstâncias normais. • A Now Platform lida com a gestão de sessão e não deve haver um motivo para um script personalizado acessar os cookies do usuário.
Risco à segurança	(Moderado) Os cookies de sessão na aplicação autenticam um usuário final e fornecem permissões de acesso implícitas na aplicação. Isso significa que há uma necessidade de protegê-los contra roubos ou exportação. Sinalizadores HTTP somente protegem os cookies de sessão de injeções de JavaScript ou vulnerabilidades de script entre sites que os roubam.
Referências	Propriedades do sistema disponíveis

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Minimizar a quantidade de sessões interativas simultâneas [Atualizado na Central de segurança 1.3]

Use esta propriedade com o plug-in Limitar sessões simultâneas para controlar o número de sessões ativas que podem ser abertas por um usuário.

Use esta propriedade **Número máximo de sessões interativas simultâneas para autenticação do Glide** com o plug-in **Limitar sessões simultâneas** (*com.glide.limit.concurrent.sessions*) para controlar o número de sessões ativas abertas por um usuário. O valor recomendado é **1**, o que reduz o número de sessões abertas (um número maior aumenta a probabilidade de que a sessão seja sequestrada).

Mais informações

Atributo	Descrição
Nome da configuração	*glide.authenticate.max.concurrent.interactive.sessions*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	inteiro
Valor recomendado	1
Valor padrão	1
Categoria	Gestão de sessões
Risco à segurança	• Pontuação de gravidade: 3,7 • Pontuação de CVSS: baixa • Detalhes do risco à segurança: definir o valor padrão da propriedade com um valor superior a 1 aumenta a chance de sequestro de sessão.
Dependências e pré-requisitos	O plug-in **Concurrent Interactive Sessions** (*com.glide.limit.concurrent.sessions*) deve estar ativo.
Referências	Limitar sessões simultâneas

Limitar sessões simultâneas em todos os nós [Atualizado na Central de segurança 1.3]

Use a propriedade *glide.authenticate.limit.concurrent.sessions.across.all.nodes* com o plug-in Limitar sessões simultâneas para gerenciar o número de sessões rastreadas em todos os nós.

Quando o plug-in Limitar sessões simultâneas está ativo, o número de sessões abertas pode ser limitado por usuário. Quando este plug-in estiver ativo, certifique-se de que a propriedade (**Limitar sessões simultâneas para autenticação do Glide em todos os nós**) esteja definida como **verdadeira**, para que o número de sessões abertas seja rastreado em todos os nós, em vez de em um único nó da aplicação. Se esta propriedade for definida como **falsa**, várias sessões poderão ser abertas em vários nós, o que aumenta as chances de sequestro de sessão.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mais informações

Atributo	Descrição
Nome da configuração	*glide.authenticate.limit.concurrent.sessions.across.all.*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	booliano
Valor recomendado	verdadeiro
Valor-padrão	verdadeiro
Categoria	Gestão de sessões
Risco à segurança	• Pontuação de gravidade: 3,7 • Pontuação de CVSS: baixa • Detalhes do risco à segurança: quando o plug-in **Limitar sessões simultâneas** é usado, definir esta propriedade como **falsa** permite que várias sessões em vários nós sejam abertas, o que aumenta a chance de uma vulnerabilidade de segurança, como sequestro de sessão.
Dependências e pré-requisitos	Nenhum
Referências	Limitar sessões simultâneas

Plug-in Limitar sessões simultâneas

Configure o plug-in com.glide.limit.concurrent.sessions para reduzir a chance de sequestro de sessão em sua instância.

Este plug-in permite que um administrador limite o número de sessões ativas por usuário e/ou função. É recomendável que este plug-in esteja habilitado e configurado para reduzir a possibilidade de sequestro de sessão. Se este plug-in estiver habilitado e configurado, haverá um limite para o número de sessões abertas que podem ser sequestradas.

Mais informações

Atributo	Descrição
Nome da configuração	*com.glide.limit.concurrent.sessions*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	plug-in
Valor recomendado	com.glide.limit.concurrent.sessions habilitado e configurado
Valor padrão	com.glide.limit.concurrent.sessions habilitado e configurado
Categoria	Gestão de sessões

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Risco à segurança	• Pontuação de gravidade: 3,7 • Pontuação de CVSS: baixa • Detalhes do risco à segurança: se este plug-in não estiver ativo, haverá uma chance maior de sequestro de sessão.
Dependências e pré-requisitos	Nenhum

Limitar a duração da sessão ativa do convidado [Novo na Central de segurança 1.3]

Use a propriedade *glide.guest.active.session.life_span* para controlar a duração das sessões HTTP ativas de um convidado.

A propriedade *glide.guest.active.session.life_span* impõe uma vida útil máxima nas sessões HTTP de convidado ativas, independentemente da inatividade da sessão ou da quantidade de tempo que um usuário está inativo antes que a sessão expire e seja encerrada. O valor configurado está em minutos. O valor zero desabilitará o tempo limite das sessões ativas. Um valor maior poderia permitir que um invasor permanecesse em uma sessão invadida por mais tempo, aumentando a possibilidade de um incidente de segurança. Esta propriedade é limitada a usuários convidados, que têm acesso de privilégios baixos a uma instância.

Para corrigir esta vulnerabilidade de segurança, defina a *glide.guest.active.session.life_span* com um valor maior que 0 e menor ou igual a 720.

Mais informações

Atributo	Descrição
Nome da configuração	*glide.guest.active.session.life_span*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	inteiro
Valor recomendado	1-720 (minutos)
Valor padrão	0
Categoria	Gestão de sessões
Risco à segurança	• Pontuação de gravidade: 4,2 • Pontuação do CVSS: média • Detalhes do risco à segurança: definir a duração máxima com um valor alto oferece a um agente mal-intencionado mais tempo em uma instância caso ele roube uma sessão.
Dependências e pré-requisitos	Nenhum(a)
Impacto funcional	Esta configuração impõe vida útil máxima em sessões HTTP de convidado ativas, independentemente

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
	do tempo limite inativo. O valor configurado está em minutos. O valor zero desabilitará o tempo limite das sessões ativas. A duração máxima deve ser maior do que o tempo limite de inatividade *glide.guest.session_timeout* (o padrão é 30 minutos).

Como limitar as sessões interativas simultâneas [Atualizado na Central de segurança 1.3]

Gerencie o número de sessões interativas em sua instância.

Use a propriedade *glide.authenticate.limit.concurrent.interactive.sessions* para gerenciar o número de sessões interativas em uma instância. Esta propriedade deve ser usada com o plug-in Limitar sessões simultâneas (com.glide.limit.concurrent.sessions). Quando o plug-in está ativo, e a propriedade está definida como **falsa**, um usuário pode ter qualquer número de sessões interativas simultâneas em uma instância. Um número maior de sessões abertas significa uma possibilidade maior de sequestro de sessão.

Mais informações

Atributo	Descrição
Nome da configuração	*glide.authenticate.limit.concurrent.interactive.sessions*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	booliano
Valor recomendado	verdadeiro
Valor-padrão	falso
Categoria	Gestão de sessões
Risco à segurança	• Pontuação de gravidade: 3,7 • Pontuação de CVSS: baixa • Detalhes do risco à segurança: quando o plug-in está ativo, e a propriedade está definida como **falsa**, um usuário pode ter qualquer número de sessões interativas simultâneas, o que aumenta a possibilidade de sequestro de sessão.
Dependências e pré-requisitos	Nenhum
Referências	Como limitar as sessões interativas simultâneas [Atualizado na Central de segurança 1.3]

Limitar a duração da sessão ativa de integrações [Novo na Central de segurança 1.3]

A propriedade *glide.integrations.active.session.life_span* impõe a duração máxima das sessões HTTP ativas do convidado, independentemente do tempo limite de inatividade. O valor configurado está em minutos. O valor zero desabilitará o tempo limite das sessões ativas.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mais informações

Atributo	Descrição
Nome da configuração	*glide.integrations.active.session.life_span*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	inteiro
Valor recomendado	0 a 720
Valor padrão	0
Categoria	Gestão de sessões
Risco à segurança	• Pontuação de gravidade: 4,2 • Pontuação do CVSS: média • Detalhes do risco à segurança: uma duração máxima maior pode permitir que um invasor persista em uma sessão roubada por mais tempo, aumentando o escopo de um incidente de segurança. Esta propriedade é limitada a integrações que têm acesso de baixo privilégio a uma instância. Defina a propriedade do Glide, *glide.integrations.active.session.life_span*, com um valor de "0" e menor ou igual a "720".
Dependências e pré-requisitos	Nenhum

Limitar o intervalo do token de atualização móvel de acesso à sessão baseada em política [Novo na Central de Segurança 1.5]

Use a propriedade *glide.authenticate.session_access.mobile.refresh_token_interval* para controlar o período que deve decorrer antes que um usuário de dispositivo móvel precise se autenticar novamente.

Um usuário precisará se autenticar novamente somente se o administrador tiver configurado os atributos do provedor de identidade na política da sessão (os atributos podem variar a cada login) e o usuário se autenticar usando o SSO (Single Sign-on). O valor padrão representa o tempo em segundos que um usuário tem antes de ser autenticado novamente. Um valor padrão maior fornece a um agente mal-intencionado mais tempo de acesso no caso de um sequestro de sessão.

Mais informações

Atributo	Descrição
Nome da configuração	*glide.authenticate.session_access.mobile.refresh_token_i*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	inteiro
Valor recomendado	1800 (segundos)

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Valor padrão	1800 (segundos)
Categoria	Gestão de sessões
Risco à segurança	• Pontuação de gravidade: 4,3 • Pontuação do CVSS: média • Detalhes do risco à segurança: se a política de ZTA estiver habilitada na instância, os usuários que usarem o SSO durante o login em dispositivo móvel serão forçados a fazer logout e login novamente depois que o valor padrão de 1800 segundos (30 minutos) terminar. Se um valor maior for usado, os usuários terão que esperar esse tempo passar.
Dependências e pré-requisitos	Acesso à sessão baseada em política com abordagem zero trust
Impacto funcional	Esta configuração controla o tempo em segundos após o login em que os usuários precisam sair dos dispositivos móveis se estiverem usando o Single Sign-on para se autenticar e o administrador tiver configurado os atributos do provedor de identidade na política de acesso à sessão.

Limitar a duração da sessão ativa da IU [Novo na Central de segurança 1.3]

A propriedade *glide.ui.active.session.life_span* impõe a duração máxima das sessões HTTP ativas autenticadas, independentemente do tempo limite de inatividade.

O valor configurado está em minutos. O valor zero desabilitará o tempo limite das sessões ativas.

Mais informações

Atributo	Descrição
Nome da configuração	*glide.ui.active.session.life_span*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	inteiro
Valor recomendado	1-720
Valor padrão	0
Categoria	Gestão de sessões
Risco à segurança	• Pontuação de gravidade: 4,2 • Pontuação do CVSS: média • Detalhes do risco à segurança: uma duração máxima maior pode permitir que um invasor

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
	persista em uma sessão invadida por mais tempo, aumentando o escopo de um incidente de segurança.
Dependências e pré-requisitos	Nenhum(a)
Impacto funcional	Impõe a duração máxima das sessões HTTP ativas autenticadas, independentemente do tempo limite de inatividade. O valor configurado está em minutos. O valor zero desabilitará o tempo limite das sessões ativas. A duração máxima deve ser maior do que o tempo limite de inatividade glide.ui.session_timeout (o padrão é 30 minutos).

Invalidação proativa de sessões inativas [Novo na Central de segurança 1.3]

A propriedade *glide.active.session.timeout.invalidate.session* controla se uma sessão expirada é invalidada proativamente antes do servidor do Tomcat.

Quando *glide.active.session.timeout.invalidate.session* não está definida como **verdadeira**, pode haver um pequeno intervalo de tempo em que uma sessão expirada não é invalidada (60 segundos ou mais, dependendo do tamanho da fila). Se uma sessão for sequestrada, o invasor poderá usá-la durante esse pequeno período de tempo. Para corrigir este risco de segurança, defina *glide.active.session.timeout.invalidate.session* como **verdadeiro**.

Mais informações

Atributo	Descrição
Nome da configuração	*glide.active.session.timeout.invalidate.session*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	booliano
Valor recomendado	verdadeiro
Valor-padrão	falso
Categoria	Gestão de sessões
Risco à segurança	• Pontuação de gravidade: 4,6 • Pontuação do CVSS: média • Detalhes do risco à segurança: não definir essa propriedade com o valor recomendado de "verdadeiro" pode fazer com que uma sessão expirada seja invalidada. Isso aumenta as chances de um agente mal-intencionado sequestrar uma sessão.
Dependências e pré-requisitos	Nenhum

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Rotação de identificadores de sessão HTTP

Use a propriedade *glide.ui.rotate_sessions* para habilitar a rotação dos identificadores de sessão HTTP para reduzir vulnerabilidades de segurança.

Se o ID de sessão de um usuário não autenticado não mudar após a autenticação, uma aplicação da Web estará vulnerável a um ataque de fixação de sessão. Um usuário mal-intencionado pode iniciar uma sessão não autenticada e fornecer o ID de sessão associado à vítima. Depois que a vítima é autenticada, o usuário mal-intencionado agora compartilha essa sessão autenticada.

Mais informações

Atributo	Descrição
Nome da propriedade	*glide.ui.rotate_sessions*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Categoria	Gestão de sessões
Finalidade	Obter uma autenticação de sessão mais segura.
Valor recomendado	verdadeiro
Valor-padrão	verdadeiro
Classificação de risco de segurança	8,8
Impacto funcional	(Médio) Esta correção modifica o SessionID quando o usuário navega de uma página não autenticada para páginas autenticadas. • Se você estiver usando um proxy ou codificando o SessionID quando um usuário fizer login pela primeira vez, ou para qualquer finalidade, poderá haver um possível impacto na funcionalidade. • Se você estiver usando o plug-in SAML 2.0 para autenticação de Single Sign-on, ele poderá interferir no compartilhamento de informações da sessão entre a instância e o Provedor de identidade. Nesse caso, você pode definir esta propriedade como falsa.
Risco à segurança	(Moderado) SessionID é usado para processar e autenticar o usuário da instância, mantendo o estado da sessão no navegador. Portanto, SessionID é considerado como dados confidenciais e deve ser seguro por padrão. A Rotação de sessão é um controle de segurança que impõe a alteração de sessionID sempre que o usuário navega de páginas não autenticadas para autenticar páginas.
Referências	Autenticação com SAML

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Minimizar a quantidade de sessões interativas simultâneas [Atualizado na Central de segurança 1.3]

Use esta propriedade com o plug-in Limitar sessões simultâneas para controlar o número de sessões ativas que podem ser abertas por um usuário.

Use esta propriedade **Número máximo de sessões interativas simultâneas para autenticação do Glide** com o plug-in **Limitar sessões simultâneas** (*com.glide.limit.concurrent.sessions*) para controlar o número de sessões ativas abertas por um usuário. O valor recomendado é **1**, o que reduz o número de sessões abertas (um número maior aumenta a probabilidade de que a sessão seja sequestrada).

Mais informações

Atributo	Descrição
Nome da configuração	*glide.authenticate.max.concurrent.interactive.sessions*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	inteiro
Valor recomendado	1
Valor padrão	1
Categoria	Gestão de sessões
Risco à segurança	• Pontuação de gravidade: 3,7 • Pontuação de CVSS: baixa • Detalhes do risco à segurança: definir o valor padrão da propriedade com um valor superior a 1 aumenta a chance de sequestro de sessão.
Dependências e pré-requisitos	O plug-in **Concurrent Interactive Sessions** (*com.glide.limit.concurrent.sessions*) deve estar ativo.
Referências	Limitar sessões simultâneas

Como minimizar a duração do tempo limite da atividade da sessão [Atualizado na Central de segurança 1.3]

Use a propriedade *glide.ui.session_timeout* para designar, em minutos, o valor do tempo limite da atividade.

Existem vários impactos funcionais na definição desta propriedade:

- Quanto mais longo for o tempo limite da sessão especificada, maior será a quantidade de memória utilizada durante uma sessão de processamento. O sistema de base usa uma duração de tempo limite padrão do Apache Tomcat de 30 minutos.
- A Now Platform ainda desconecta os usuários com Lembrar-me. Após 30 minutos de inatividade na aplicação, a plataforma desconecta o usuário automaticamente, a menos que a caixa de seleção **Lembrar-me** na página de login esteja marcada. A diferença é que eles não fazem login novamente para continuar.
- Se houver medidores ou conteúdo nas páginas iniciais dos usuários que sejam atualizados automaticamente, esse tempo limite poderá nunca ser atingido.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mais informações

Atributo	Descrição
Nome da propriedade	*glide.ui.session_timeout*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Categoria	Gestão de sessões
Finalidade	Impor o tempo limite da sessão.
Valor recomendado	Tempo limite especificado pelo usuário em minutos. 60 minutos é o valor recomendado, mas esse valor pode variar dependendo da funcionalidade e do requisito de segurança. Não defina este valor como mais de um dia.
Classificação de risco de segurança	7,5
Impacto funcional	(Médio) Esta correção impõe a expiração oportuna da conta do usuário. Nenhum impacto na funcionalidade, no entanto, a experiência do usuário é alterada.
Risco à segurança	(Alto) As sessões do usuário ativas por um período indefinido de tempo são um risco à segurança e devem expirar em uma configuração baseada em tempo.
Referências	Gerenciar sessões do usuário

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Como minimizar a duração do tempo limite da janela da sessão [Atualizado na Central de segurança 1.3]

Use a propriedade *glide.ui.user_cookie.life_span_in_days* para definir o período de expiração do cookie Lembrar-me. O valor padrão é 15 dias e o limite máximo é de 30 dias.

Mais informações

Atributo	Descrição
Nome da propriedade	*glide.ui.user_cookie.life_span_in_days*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Categoria	Gestão de sessões
Finalidade	Habilitar a expiração padrão do cookie **lembrar-me**.
Tipo de dados	Inteiro
Valor recomendado	15
Valor padrão	15
Classificação de risco de segurança	4,9

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Impacto funcional	(Médio) Esta propriedade é habilitada pelo usuário final quando o usuário final marca a caixa de seleção **Lembrar-me** na página de login e faz login na Now Platform.
Risco à segurança	(Moderado) Os cookies do usuário ativos por um período indefinido de tempo são um risco à segurança e devem expirar em uma configuração baseada em tempo.
Referências	Propriedades do sistema disponíveis Lembrar minhas informações

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Criptografia armazenada

Esta categoria enfoca a criptografia de dados armazenados. Ela engloba vários aspectos importantes, como empregar algoritmos e módulos criptográficos estabelecidos, garantir a geração apropriada de valores pseudoaleatórios, implementar criptografia com base na classificação de dados e armazenar e isolar com segurança o material da chave.

Habilitar criptografador KMF do glide [Removido na Central de Segurança 1.3.2]

Gerencie os criptografadores usados para campos Password2 em sua instância.

Use a propriedade *glide.kmf.encrypter.enabled* para definir o criptografador da KMF como o criptografador padrão para os campos Password2. Essa propriedade garante que padrões de criptografia fortes e compatíveis sejam usados em vez de um criptografador legado. Para garantir que o criptografador da KMF seja usado em vez do criptografador legado, defina esta propriedade como **verdadeira**.

Mais informações

Atributo	Descrição
Nome da configuração	*glide.kmf.encrypter.enabled*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	booliano
Valor recomendado	verdadeiro
Valor-padrão	falso
Categoria	Criptografia armazenada
Risco à segurança	• Pontuação de gravidade: 4,9 • Pontuação do CVSS: média

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
	• Detalhes do risco à segurança: definir esta propriedade como **verdadeira** garante que o criptografador da KMF seja usado em vez do criptografador legado.
Referências	Criptografia Password2 com o KMF (Key Management Framework, Estrutura de gestão de chaves)

Validação, limpeza e codificação

Validação, limpeza e codificação de entrada de endereços para evitar vulnerabilidades como Script entre sites (XSS), injeção de SQL e outros ataques.

Este controle garante que a validação de entrada e a codificação de saída estejam em vigor e configuradas corretamente, como codificação ou escape de dados de saída. Esta categoria também inclui verificações de itens como desserialização de objetos, área restrita quando necessário e validação positiva por meio de listas de permissões.

Restringir o acesso à API com script GlideSystemUserSession [Atualizado na Central de segurança 1.3]

A API passível de script GlideSystemUserSessionSandbox cliente chamável expõe os métodos addErrorMessageNoSanitization e addInfoMessageNoSanitization de GlideSystemUserSession para a área restrita do javascript. Isso permite que todos os usuários chamem este método por meio de script.

Quando definido como **verdadeiro**, uma sessão de usuário em área restrita tem permissão para chamar informações ou mensagens de erro sem limpeza. Um aviso será registrado quando a mensagem for chamada. Quando definido como **falso**, a chamada não é permitida.

⚠ **Aviso:** Esta é uma propriedade tipo porto seguro, o que significa que o valor não pode ser alterado após ser mudado. A reversão não é possível.

Mais informações

Atributo	Descrição
Nome da propriedade	*glide.sandbox.usersession.allow_unsanitized_messages*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Categoria	Controle de acesso
Finalidade	Esta propriedade restringirá a chamada de mensagens informativas ou de erro em uma sessão de usuário em área restrita.
Tipo	booliano
Valor recomendado	falso
Valor padrão	verdadeiro
Classificação de risco de segurança	8,1

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Impacto funcional	(Alto) Definir a propriedade com o valor falso resultará em nenhuma criação de mensagem ou registro em log caso essas funções sejam chamadas.
Risco à segurança	(Alto) Sem a limpeza apropriada, o conteúdo potencialmente perigoso pode ser acessado e a função de erro não limpa fica disponível para o script.
Referências	Controle de Acesso

Desabilitar marcadores JavaScript no HTML incorporado [Atualizado na Central de segurança 1.3]

Use a propriedade *glide.ui.security.codetag.allow_script* para desabilitar o suporte para incorporação de código HTML JavaScript criado usando o marcador [code].

A Now Platform atenua muitos ataques de injeção e entre sites implementando técnicas de escape e codificação. Como resultado, os usuários não podem escrever e enviar entradas no formato HTML para campos de diário. No entanto, os campos de diário podem renderizar texto entre marcadores de código como HTML. Certifique-se de que *glide.ui.security.codetag.allow_script* exista na tabela sys_properties e esteja definido como falso.

- No entanto, há um risco de segurança associado. Se definida como **verdadeira**, usuários mal-intencionados podem gravar código HTML JavaScript prejudicial que pode ser executado em um navegador do cliente diferente após a renderização de campos de diário.
- Defina esta propriedade como **falsa** para que os administradores possam impedir que os campos de diário renderizem o código HTML JavaScript, desabilitando o suporte para o marcador `[code]`.

⚠ **Aviso:** Esta é uma propriedade tipo porto seguro, o que significa que o valor não pode ser alterado após ser mudado. A reversão não é possível.

Mais informações

Atributo	Descrição
Nome da propriedade	*glide.ui.security.codetag.allow_script*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Categoria	Validação, limpeza e codificação
Finalidade	Protege contra scripts entre sites e execução de scripts mal-intencionados
Valor recomendado	falso
Valor-padrão	falso
Classificação de risco de segurança	8,8
Impacto funcional	(Médio) Esta correção impõe o escape de JavaScript na IU e renderiza os resultados codificados para o usuário. Ela pode ter um impacto na funcionalidade

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
	com base na interação do usuário da instância com os dados resultantes.
Risco à segurança	(Alto) A validação de entrada deve ocorrer na aplicação para defesa contra ataques de script entre sites. Esses ataques permitem que scripts externos sejam executados na sessão do usuário no contexto do navegador logado. Os invasores podem usá-los para roubar informações da sessão e dados confidenciais.
Referências	Restringir o marcador CODE nos campos de diário Renderizar entradas do campo de diário como HTML Configurações de Alta Segurança

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Habilitar o gerenciador de segurança Java protegido [Novo na Central de segurança 1.3]

A propriedade *glide.security.manager* contém o nome da classe Java do gerenciador de segurança Java atual.

Aviso: Esta é uma propriedade tipo porto seguro, o que significa que o valor não pode ser alterado após ser mudado. A reversão não é possível.

Mais informações

Atributo	Descrição
Nome da configuração	*glide.security.manager*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	cadeia de caracteres
Valor recomendado	*com.glide.sys.security.ContextualSecurityManager*
Valor-padrão	*com.glide.sys.security.ContextualSecurityManager*
Categoria	Validação, limpeza e codificação
Risco à segurança	• Pontuação de gravidade: 7,2 • Pontuação de CVSS: alta • Detalhes do risco à segurança: se *glide.security.manager* não estiver definido com o valor recomendado de *com.glide.sys.security.ContextualSecurityManager*, é possível que a instância esteja usando um gerenciador de segurança Java obsoleto que não tem as políticas de proteção esperadas. Sem

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
	essa proteção, é possível que um agente mal-intencionado com acesso à execução de script realize a execução remota de código na instância.
Dependências e pré-requisitos	Nenhum

Impor a limpeza de HTML [Atualizado na Central de segurança 1.3]

Use a propriedade *com.glide.security.check_unsanitized_html* para impor o comportamento de limpeza dos campos translated_html globalmente para atribuições de campo.

HTML é um dos tipos que podem ser atribuídos aos campos de dicionário. A atribuição de campos HTML a qualquer tipo de campo fornece a funcionalidade para formatar conteúdo usando marcadores HTML (por exemplo, `<p>`, `<a href>`, `<b>`, `<font>`, `<img>`). Para evitar atividades mal-intencionadas, determinados marcadores HTML podem ser desabilitados usando uma lista de bloqueios. Esta propriedade impedirá que marcadores não permitidos sejam usados em campos translated_html em sua instância.

- Defina esta propriedade para **impor** o comportamento de limpeza dos campos translated_html.
- Defina a propriedade como **desabilitada** para desativar a limpeza de HTML para permitir marcadores de HTML bloqueados em campos translated_html.

⚠ **Aviso:** Esta é uma propriedade tipo porto seguro, o que significa que o valor não pode ser alterado após ser mudado. A reversão não é possível.

Mais informações

Atributo	Descrição
Nome da propriedade	*com.glide.security.check_unsanitized_html*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Categoria	Validação, limpeza e codificação
Finalidade	Impedir o uso de marcadores HTML não seguros para proteger contra ataques, como script entre sites.
Tipo	Cadeia de caracteres
Valor recomendado	impor
Valor-padrão	impor
Classificação de risco de segurança	7,3
Impacto funcional	(Médio) Esta correção impõe que a limpeza de HTML ocorra na IU e renderiza os campos html traduzidos para o usuário. Isso pode afetar a legibilidade e a formatação.
Risco à segurança	(Alto) A validação de entrada deve ocorrer na aplicação para defesa contra ataques de script entre sites. Esses ataques permitem que scripts externos sejam executados nas sessões do usuário no contexto

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
	do navegador conectado. Os invasores podem usá-los para roubar informações da sessão e dados confidenciais.
Referências	Limpador de HTML

Como impor a área restrita de scripts gerados pelo cliente [Atualizado na Central de segurança 1.3]

Use a propriedade *glide.script.use.sandbox* para habilitar a área restrita de script.

Há dois casos na Now Platform que permitem ao cliente enviar scripts ao servidor para avaliação:

Filtros ou consultas

É válido enviar um filtro para o servidor, como `assigned_to=JavaScript:getMyGroups ()`.

API do sistema

A chamada de API permite que o cliente execute scripts arbitrários no servidor e receba uma resposta.

Se você habilitar a área restrita de script, o script que está sendo avaliado em qualquer um desses dois pontos de entrada será executado em uma área restrita com direitos reduzidos, com as seguintes características:

- Somente as regras de negócios marcadas como cliente chamável estão disponíveis na área restrita.
- Somente as inclusões de script marcadas como cliente chamável estão disponíveis na área restrita.
- Certas chamadas de API (em grande parte, mas não inteiramente, limitadas àquelas que lidam com acesso direto ao banco de dados não são permitidas.
- Você não pode inserir, atualizar ou excluir dados de dentro da área restrita. Por exemplo, todas as chamadas para `current.update ()` serão ignoradas. Se você executar a Now Platform sem habilitar a área restrita de script, nenhuma dessas restrições se aplicará.

⚠ **Aviso:** Esta é uma propriedade tipo porto seguro, o que significa que o valor não pode ser alterado após ser mudado. A reversão não é possível.

Mais informações

Atributo	Descrição
Nome da propriedade	*glide.script.use.sandbox*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Categoria	Validação, limpeza e codificação
Finalidade	Impor a validação das consultas JavaScript do lado do cliente que são iniciadas na plataforma
Valor recomendado	verdadeiro
Valor-padrão	verdadeiro

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Classificação de risco de segurança	9,8
Impacto funcional	(Crítico) Esta correção impõe a validação das consultas JavaScript do lado do cliente que são iniciadas na contra a Now Platform Há um possível impacto se o cliente tiver personalizações que incluem consultas JavaScript codificadas para executar operações CRUD.
Risco à segurança	(Crítico) A Now Platform fornece uma ampla variedade de recursos e funcionalidades por meio de consultas JavaScript. No entanto, sem a autorização e a validação apropriadas, é possível que um invasor execute operações não autorizadas na plataforma.
Referências	Configurar propriedade da área restrita de script *glide.script.use.sandbox* pertence à mesma família de propriedades que protegem e restringem a execução de scripts originados no cliente: • *glide.script.allow.ajaxevaluate*: Consulte Habilitar AJAXEvaluate. • *glide.script.secure.ajaxglideerecord*: Consulte Habilitar a verificação de ACL de AJAXGlideRecord.

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Como converter imagens de e-mails recebidos em anexos [Atualizado na Central de segurança 1.3 e removido na 1.5]

Use a propriedade *glide.email.inbound.convert_html_inline_attachment_references* para especificar se o e-mail de entrada deve ser convertido em HTML para que as imagens do e-mail apareçam na visualização do corpo do HTML.

O seguinte acontece quando a propriedade do sistema *glide.email.inbound.convert_html_inline_attachment_reference* é definida como falsa:

- Na Now Platform, links de cid quebrados (ID de conteúdo) aparecem no lugar das imagens recebidas. O formato no qual a imagem do e-mail aparece depende da configuração da propriedade no momento em que o e-mail é recebido, e não da configuração da propriedade atual.
- O conteúdo "mal-intencionado" recebido no anexo não é mencionado no HTML do e-mail. O próprio anexo é armazenado na tabela sys_attachment.
- O processamento de e-mail de entrada não atualizará os dados HTML do e-mail para refletir o local armazenado do anexo na tabela sys_attachment. Isso resulta no seguinte:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Imagens em linha não aparecem na exibição de e-mail no formatador de atividades.

  Nota: Para resolver esse problema com o formatador de atividades, primeiro verifique se não há problemas de segurança. Em seguida, defina a propriedade do sistema *glide.email.inbound.convert_html_inline_attachment_reference* como **verdadeira** para permitir que os e-mails futuros recebidos contenham o URL HTML necessário para fazer referência à imagem. Alterar a propriedade não atualiza os e-mails já recebidos. O novo valor afeta somente os e-mails de entrada recebidos após a mudança da propriedade.

- Imagens em linha não aparecem quando o e-mail é exibido na visualização HTML do e-mail.
- Ao anexar email.body_htm em ações de entrada entre marcadores de código, as imagens estão ausentes.

Pré-requisitos

Antes de definir essa propriedade, defina a propriedade *glide.email.read.active* como verdadeira. Para saber mais, consulte Habilitar usando seu próprio servidor POP3.

Mais informações

Atributo	Descrição
Nome da propriedade	*glide.email.inbound.convert_html_inline_attachment_refere*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Categoria	Validação, limpeza e codificação
Finalidade	Restringir a renderização de imagem na visualização do corpo HTML.
Valor recomendado	falso
Classificação de risco de segurança	5,4
Impacto funcional	(Médio) Depois que esta propriedade é configurada, o usuário não pode ver a visualização da imagem no corpo do e-mail.
Risco à segurança	(Médio) Se a propriedade não estiver habilitada, um invasor poderá enviar imagem mal-intencionada contendo malware.
Referências	Propriedades do e-mail Configuração de entrada de e-mails

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Desabilitar AJAXEvaluate

Use *glide.script.allow.ajaxevaluate* para proteger a API do sistema contra vulnerabilidades de execução de script do cliente por meio de chamadas AJAX.

A elevação para a função security_admin é necessária para editar a propriedade.

Aviso: Esta é uma propriedade tipo porto seguro, o que significa que o valor não pode ser alterado após ser mudado. A reversão não é possível.

Mais informações

Atributo	Descrição
Nome da propriedade	*glide.script.allow.ajaxevaluate*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Categoria	Validação, limpeza e codificação
Finalidade	Impedir que um usuário execute scripts como um privilégio de administrador.
Valor recomendado	falso
Valor-padrão	falso
Tipo de configuração	Booliano
Impacto funcional	(Médio) Esta correção força o processador AJAXEvaluate a ser desligado. Isso pode afetar a funcionalidade se você estiver usando explicitamente o processador de avaliação AJAX como parte de qualquer script personalizado.
Risco à segurança	(Alto) O processador AjaxEvaluator executa Scripts de cliente na área restrita. No entanto, há várias propriedades adicionais que podem permitir que o escopo das atividades na área restrita seja expandido ou totalmente desativado.
Classificação de risco de segurança	7,3
Referências	Esta propriedade pertence à mesma família de propriedades que protegem e restringem a execução de scripts originados no cliente: • *glide.script.use.sandbox*: Consulte Área restrita de scripts gerados pelo cliente • *glide.script.allow.ajaxevaluate*: Consulte Habilitar AJAXEvaluate.

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Como desativar a expansão de entidade no Analisador de fluxo de XMLDocument2 [Atualizado na Central de segurança 1.5]

Se as personalizações não exigirem expansão de entidade, use a propriedade *glide.stax.allow_entity_resolution* para desabilitar completamente a expansão de entidade externa. O XML conclui a análise, mas não inclui entidades internas ou externas.

- Se você definir esta propriedade como **verdadeira**, todas as entidades externas tentarão resolver ou expandir as entidades de assunto, sujeitas à configuração da propriedade *glide.stax.whitelist_enabled*.
- Se você definir essa propriedade como **falsa**, todas as resoluções e expansões da entidade serão bloqueadas. Para saber mais, consulte validação de entidade XMLdoc2 com lista de permissões.

Pré-requisitos

Antes de definir esta propriedade:

- Defina as propriedades *glide.xml.entity.whitelist.enabled* e *glide.stax.whitelist_enabled* como verdadeiras. Para saber mais, consulte Validação de entidade XMLdoc/XMLUtil com lista de permissões e Validação de entidade XMLdoc2 com lista de permissões.
- Defina uma lista de FQDN delimitada por vírgulas na propriedade *glide.xml.entity.whitelist*, que são os únicos URLs que podem ser acessados usando o a propriedade de processamento de entidade de XML. Para saber mais, consulte Processamento de entidade externa de XML - lista de permissões.

⚠ **Aviso:** Esta é uma propriedade tipo porto seguro, o que significa que o valor não pode ser alterado após ser mudado. A reversão não é possível.

Mais informações

Atributo	Descrição
Nome da propriedade	*glide.stax.allow_entity_resolution*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Categoria	Autenticação
Finalidade	Este controle de correção deve ser habilitado para defesa contra um ataque de expansão de entidade XML/Billion laughs.
Valor recomendado	falso
Valor padrão	verdadeiro
Impacto funcional	(Baixo) Se a personalização estiver usando expansão de entidade, então, a Now Platform pode bloquear o processamento adicional.
Risco à segurança	(Crítico) Um invasor pode usar esta vulnerabilidade para expandir os dados de forma exponencial, consumindo rapidamente todos os recursos do sistema.
Solução alternativa	Se a personalização exigir expansão da entidade, defina esta propriedade como verdadeira e siga as

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
	etapas documentadas na Validação da entidade XMLdoc2 com lista de permissões.

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Para obter mais informações sobre os recursos OWASp, consulte OWASp.

Desabilitar URL do conteúdo externo

Gerencie como os metadados de link externo são usados em sua instância com o Bate-papo do Connect.

Use a propriedade *glide.ui.url.external.content* para gerenciar metadados de link externo em sua instância. Se a propriedade estiver definida com o valor recomendado **falsa**, nenhum metadado de link externo será renderizado. Se definida como **verdadeira**, Bate-papo do Connect recuperará metadados de link externo de fontes como o YouTube ou artigos de notícias para renderizar mensagens mais ricas. Isso pode resultar em ataques de SSRF (Server Side Request Forgery, falsificação de solicitações do lado do servidor).

Mais informações

Atributo	Descrição
Nome da configuração	*glide.ui.url.external.content*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	booliano
Valor recomendado	falso
Valor padrão	verdadeiro
Categoria	Validação, limpeza e codificação
Risco à segurança	• Pontuação de gravidade: 8,1 • Pontuação de CVSS: alta • Detalhes do risco à segurança: definir esta propriedade como **verdadeira** pode expor sua instância a ataques de SSRF.
Dependências e pré-requisitos	Nenhum
Referências	Bate-papo do Connect

Como definir tipos MIME para download restritos [Atualizado na Central de segurança 1.3]

A propriedade *glide.ui.attachment.download_mime_types* forçará a lista especificada de tipos de arquivos perigosos a ser baixada para o cliente e não exibida em linha no navegador.

Se o tipo MIME de um arquivo estiver presente em *glide.ui.attachment.download_mime_types*, um download será forçado. Por exemplo,

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

baixar texto/html força os arquivos HTML a serem baixados para o cliente como um arquivo, em vez de exibidos em linha no navegador, prevenindo um ataque XSS.

Para exibir uma lista de tipos MIME existentes, digite `/sys_attachment_icon_rule_list.do`. Você pode habilitar qualquer um desses tipos MIME para atender aos requisitos de conformidade de segurança em Now Platform.

Nota: A função security_admin é necessária para editar a propriedade.

Mais informações

Atributo	Descrição
Nome da propriedade	*glide.ui.attachment.download_mime_types*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Categoria	Validação, limpeza e codificação
Finalidade	Manter corretamente a lista de tipos de arquivos perigosos que não podem ser exibidos no navegador impedirá ataques de script entre sites (XSS).
Valor recomendado	Lista de tipos MIME aplicáveis ou o valor recomendado: `text/html,image/svg,image/svg+xml,application/xml`
Valor padrão	Lista de tipos MIME aplicáveis para o valor padrão: `text/html,image/svg,image/svg+xml,application/xml`
Tipo de configuração	Cadeia de caracteres: qualquer valor separado por vírgula de tipos mime de aplicação.
Impacto funcional	(Baixo) Esta correção impõe a realização das verificações de validação antes de executar uma ação ao clicar em um anexo em uma aplicação da Now Platform. Não há nenhum impacto potencial, mas a experiência do usuário é alterada.
Risco à segurança	(Moderado) Os invasores podem abusar dos tipos MIME e colocar conteúdo de script não intencional no anexo do lado da vítima para capturar informações confidenciais. A capacidade de ter XSS pode levar ao fácil alcance da escalação de privilégios para funções superiores, como administrador, onde mais movimento lateral pode ser realizado. No contexto atual, preencha a propriedade com uma lista de tipos MIME de anexo separados por vírgula que não devem ser renderizados em linha no navegador.
Classificação de risco de segurança	6,3

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Propriedades relacionadas	• *glide.ui.attachment.force_download_all_mime_types* • *glide.ui.attachment.tables_ignore_force_download*
Referências	Forçar o download de tipos MIME.

Como desabilitar o código HTML integrado [Atualizado na Central de segurança 1.3]

Use a propriedade *glide.ui.security.allow_codetag* para desabilitar o suporte para incorporação de código HTML criado usando o marcador [code].

A Now Platform atenua muitos ataques de injeção e entre sites implementando técnicas de escape e codificação. Como resultado, os usuários não podem escrever/enviar entradas no formato HTML para campos de diário. Mas os campos de diário podem renderizar texto entre tags de código como HTML.

- No entanto, há um risco de segurança associado. Se definido como `verdadeiro`, usuários mal-intencionados podem gravar código HTML JS prejudicial que pode ser executado em um navegador do cliente diferente após a renderização de campos de diário.
- Defina esta propriedade como `falsa` para que os administradores possam impedir que os campos de diário renderizem o código HTML, desabilitando o suporte para o marcador `[code]`.

Mais informações

Atributo	Descrição
Nome da propriedade	glide.ui.security.allow_codetag
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Categoria	Validação, limpeza e codificação
Configurar na Central de segurança da instância	Sim
Finalidade	Proteger contra scripts entre sites e execução de scripts mal-intencionados
Valor recomendado	falso
Valor padrão	verdadeiro
Classificação de risco de segurança	4,2
Impacto funcional	(Médio) Esta correção impõe a codificação HTML na IU e renderiza os resultados codificados para o usuário. Esta propriedade é definida como `verdadeira` por padrão. Nesse estado, sua instância exibe HTML renderizado em formulários e campos de diário. Se esta propriedade estiver definida como `falsa`, o HTML não será renderizado corretamente e as tags HTML poderão aparecer nos campos de diário em

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
	formulários. Ela pode ter um impacto adverso na funcionalidade e nas interações do usuário com os dados resultantes.
Risco à segurança	(Médio) A validação de entrada deve ocorrer na aplicação para defesa contra ataques de script entre sites. Esses ataques permitem que scripts externos sejam executados na sessão de um usuário no contexto do navegador logado. Os invasores podem usá-los para roubar informações da sessão e dados confidenciais.

Como habilitar o Sanitizer de HTML no Virtual Agent [Atualizado na Central de segurança 1.3]

Use a propriedade *com.glide.cs.html.sanitizer.enabled* para habilitar o HTMLSanitizerService.

Mais informações

Aviso: Esta é uma propriedade tipo porto seguro, o que significa que o valor não pode ser alterado após ser mudado. A reversão não é possível.

Atributo	Descrição
Nome da propriedade	*com.glide.cs.html.sanitizer.enabled*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Categoria	Validação, limpeza e codificação
Finalidade	Prevenir ataques de script entre sites e injeção de HTML à aplicação.
Valor recomendado	verdadeiro
Valor-padrão	verdadeiro
Classificação de risco de segurança	8
Impacto funcional	(Alto) Esta correção impõe o mecanismo de codificação de saída HTML antes que os dados do usuário sejam renderizados de volta para o usuário. Se o cliente tiver alguma personalização que envolva a renderização do atributo HTML ou dos dados de conteúdo, haverá um impacto na funcionalidade.
Risco à segurança	(Alto) A entrada do usuário deve ser tratada com segurança quando os dados são armazenados e processados na aplicação. Isso reduz os ataques de script entre sites do lado do cliente, codificando os dados de saída.

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Habilitar proteção de interpolação do JS Jelly

Use a propriedade *glide.ui.jelly.js_interpolation.protect* para garantir que qualquer JavaScript prestes a ser executado em uma página do Jelly esteja protegido contra injeção com a ajuda da interpolação do Jelly.

Quando você define a propriedade como **verdadeira**, uma aplicação passa por uma árvore de scripts Jelly (aninhada). Ela envolve expressões Jelly potencialmente perigosas com um filtro que:

- Escapa dos resultados por segurança, ou
- Se a segurança não puder ser garantida, gera uma SecurityException porque a expressão que seria avaliada representa um possível problema de segurança.

⚠ **Aviso:** Esta é uma propriedade tipo porto seguro, o que significa que o valor não pode ser alterado após ser mudado. A reversão não é possível.

Mais informações

Atributo	Descrição
Nome da propriedade	*glide.ui.jelly.js_interpolation.protect*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Categoria	Validação, limpeza e codificação
Finalidade	Atenuar os ataques de execução de código mal-intencionado que podem ocorrer usando o Jelly Injection.
Valor recomendado	verdadeiro
Valor-padrão	falso
Classificação de risco de segurança	9
Impacto funcional	(Alto) Esta propriedade faz uma melhor estimativa se uma expressão está entre aspas. Ela pode citar incorretamente uma expressão legítima. Nesse caso, pode ser necessário marcar manualmente uma expressão como segura.
Risco à segurança	(Moderado) A injeção de JEXL é uma forma de injeção de entrada exclusiva da Now Platform que pode levar à falsificação de solicitação entre sites e à execução de código. Desativar completamente a proteção pode abrir muitas vulnerabilidades de segurança P1.
Solução alternativa	Para marcar manualmente uma expressão como segura, adicione o prefixo SAFE à expressão do Jelly: `${SAFE:sysparm_input};` Adicionar SAFE às cegas a cada expressão é a maneira incorreta de abordar o problema, pois pode abrir uma vulnerabilidade de segurança.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
	• Somente adicione SAFE a uma expressão se você puder garantir que a expressão não contém a entrada do cliente. • Caso contiver, um cliente mal-intencionado pode causar avaliação de JavaScript privilegiado.
Referências	Marcadores Jelly Configurações de Alta Segurança

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Habilitar proteção de interpolação do JS Jelly para expressões aninhadas

Gerencie a proteção de interpolação na sua instância.

Use a propriedade *glide.ui.jelly.js_interpolation.protect_nested_expressions* para gerenciar a proteção de interpolação. A proteção de interpolação garante que, quando as expressões do Jelly forem usadas em JavaScript, elas sejam consideradas seguras por se enquadrarem em determinadas categorias ou por serem marcadas como SAFE na própria expressão. Sem essa mitigação habilitada, um agente mal-intencionado pode enviar um parâmetro GET para uma página do Jelly e fazer com que o conteúdo desse parâmetro seja avaliado como JavaScript do lado do servidor com privilégios de administrador. Se esta propriedade não estiver definida com o valor recomendado de **verdadeiro**, expressões mal-intencionadas do Jelly interpoladas em JavaScript serão permitidas, e um usuário poderá executar o código usando um modelo do Jelly.

Aviso: Esta é uma propriedade tipo porto seguro, o que significa que o valor não pode ser alterado após ser mudado. A reversão não é possível.

Mais informações

Atributo	Descrição
Nome da configuração	*glide.ui.jelly.js_interpolation.protect_nested_expressio*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	booliano
Valor recomendado	verdadeiro
Valor-padrão	falso
Categoria	Validação, limpeza e codificação
Risco à segurança	• Pontuação de gravidade: 9 • Pontuação de CVSS: Crítica • Detalhes do risco à segurança: se a propriedade estiver definida como **falsa**, expressões mal-intencionadas do Jelly serão permitidas.
Dependências e pré-requisitos	Nenhum

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Impor links relativos

Use a propriedade *glide.cms.catalog_uri_relative* para impor links relativos do parâmetro URI em `em/ess/catalog.do`.

- Quando definida como **verdadeira**, somente URLs relativas são permitidas por meio da página `/ess/catalog.do` usando o parâmetro *uri*.
- Quando definida como **falsa**, todas as URLs são permitidas, o que pode permitir vinculação a conteúdo externo não autorizado.

Mais informações

Atributo	Descrição
Nome da propriedade	*glide.cms.catalog_uri_relative*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Categoria	Validação, limpeza e codificação
Finalidade	Restringir as tentativas de vincular conteúdo externo não autorizado.
Valor recomendado	verdadeiro
Valor-padrão	falso
Classificação de risco de segurança	2,6
Impacto funcional	(Baixo) Esta correção impõe a validação na página do Catálogo de forma que somente URLs relativas sejam permitidas. Links existentes para aplicações da Web externos são quebrados.
Risco à segurança	(Alto) URLs absolutos podem representar um risco à segurança quando usados como parte de um parâmetro ou um valor de campo, redirecionando a página de origem para um site controlado por um adversário.

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Impor verificação da lista de permissões de URL

Use a propriedade *glide.security.url.whitelist* para adicionar uma camada extra de validação para garantir que qualquer URL externo introduzido faça parte dos URLs da lista de inclusões.

O redirecionamento aberto ocorre quando uma página da Web vulnerável é redirecionada para uma página não confiável e mal-intencionada que pode comprometer o usuário. Os ataques de redirecionamento aberto vêm com um ataque de phishing porque o link vulnerável modificado é idêntico ao site original, aumentando a probabilidade de sucesso do ataque de phishing.

Esta propriedade é aplicável nos seguintes casos:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- `/logout.do?sysparm_goto_url={External URL}`
- `/cms_login_redirect.do?sysparm_goto_url={External URL}`

Os usuários são direcionados para um site externo confiável após fazerem logout da instância:

- `/logout_redirect.do?sysparm_url={External URL}`
- `/saml_redirector.do?sysparm_uri={External URL}`

Quando o SAML está habilitado, ele invoca um URL de logout do IDP (identity provider, provedor de identidade).

Mais informações

Atributo	Descrição
Nome da propriedade	*glide.security.url.whitelist*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Categoria	Validação, limpeza e codificação
Finalidade	Implementar o redirecionamento de URL seguro durante o login, logout ou outros redirecionamentos. Esta propriedade atenua um dos 10 principais ataques da OWASP, chamados de redirecionamentos e encaminhamentos inválidos.
Tipo	Cadeia de caracteres
Valor padrão	verdadeiro
Valor recomendado	verdadeiro
Valor	Os URLs aprovados da sua organização [Alguns FQDN (Fully Qualified Domain Name, Nome de domínio completo) definidos, por exemplo, http://www.servicenow.com.br]
Classificação de risco de segurança	8,3
Impacto funcional	(Médio) Esta correção impõe validação na página de logout. Isso pode ter um impacto funcional em um usuário de uma instância com uma configuração SSO/SAML.
Risco à segurança	(Alto) O redirecionamento aberto do lado do cliente pode permitir que o invasor redirecione as vítimas/usuários para o site controlado pelo invasor e é visto como um risco à segurança.
Referências	Correções e erros de Multi-SSO (SAML 2.0)

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Escapar fórmulas do Excel [Atualizado na Central de segurança 1.3]

Use a propriedade *glide.export.escape_formulas* para impedir a injeção do Excel, também conhecida como injeção de fórmula.

A injeção do Excel ocorre quando os sites incorporam entradas não confiáveis em arquivos do Excel. Quando você usa um aplicativo de planilha, como o Microsoft Excel ou o LibreOffice Call, para abrir um arquivo, todas as células que começam com +, -, = ou @ são interpretadas como uma fórmula. Quando você define a propriedade *glide.export.escape_formulas* como **verdadeira**, os valores de cadeia de caracteres que começam com +, -, = ou @ são anexados com um único apóstrofo ao exportar para arquivos CSV, XLS ou XLSX.

Mais informações

Atributo	Descrição
Nome da propriedade	*glide.export.escape_formulas*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Categoria	Validação, limpeza e codificação
Finalidade	Evitar a aplicação no Excel ou na injeção de fórmula.
Valor recomendado	verdadeiro
Valor-padrão	falso
Classificação de risco de segurança	6,5
Impacto funcional	(Baixo) Fórmulas mal-intencionadas podem ser usadas para sequestrar o computador do usuário, explorando vulnerabilidades no software de planilha.
Risco à segurança	(Moderado) As fórmulas maliciosas representam um risco mesmo quando a planilha de incorporação não contém informações confidenciais, pois elas podem ser usadas para comprometer o computador do visualizador.
Solução alternativa	Como alternativa, considere remover todos os espaços em branco à direita onde for possível e limitar todos os dados fornecidos pelo cliente a caracteres alfanuméricos.
Referências	Propriedades do sistema disponíveis

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Como fazer escapes de HTML em exibições de lista [Atualizado na Central de segurança 1.3]

Use a propriedade *glide.ui.escape_html_list_field* para forçar escapes de HTML para campos HTML em uma exibição de lista.

HTML é um dos tipos que podem ser atribuídos aos campos de dicionário. A atribuição de campos HTML a qualquer tipo de campo fornece a funcionalidade para formatar conteúdo usando códigos HTML (por exemplo, `<p>`, `<a href>`, `<b>`, `<font>`, `<img>`). Um usuário mal-

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

intencionado pode injetar código HTML no campo de formulário para executar scripts indesejados em diferentes sessões de cliente/usuário.

- Defina esta propriedade como **falsa** para executar um escape de HTML antes que os registros/campos sejam renderizados no navegador quando a tabela aparecer como uma exibição de lista.
- Se estiver definida como **verdadeira** e você selecionar essa coluna em uma exibição de lista ao exibir uma tabela ou lista de registros, esses campos em formato HTML poderão ser exibidos.

⚠ **Aviso:** Esta é uma propriedade tipo porto seguro, o que significa que o valor não pode ser alterado após ser mudado. A reversão não é possível.

Mais informações

Atributo	Descrição
Nome da propriedade	*glide.ui.escape_html_list_field*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Categoria	Validação, limpeza e codificação
Finalidade	Prevenir ataques de script entre sites à aplicação.
Valor recomendado	verdadeiro
Valor-padrão	verdadeiro
Classificação de risco de segurança	8,8
Impacto funcional	(Médio) Esta correção impõe a codificação de HTML na IU no nível de analisador HTML e, então, renderiza os resultados codificados para o usuário. Ela pode ter um impacto na funcionalidade com base na interação do usuário da instância com os dados resultantes.
Risco à segurança	(Alto) A validação de entrada deve ocorrer na aplicação para defesa contra ataques de script entre sites. Esses ataques permitem que scripts externos sejam executados nas sessões do usuário no contexto do navegador conectado. Os invasores podem usá-los para roubar informações da sessão e dados confidenciais.
Referências	Configurações de Alta Segurança

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Escapar do JavaScript

Use a propriedade *glide.html.escape_script* para forçar o escape de marcadores JavaScript (`<script></script>`) em campos HTML nas exibições de lista.

HTML é um dos tipos que podem ser atribuídos aos campos de dicionário. A atribuição de campos HTML a qualquer tipo de campo fornece a funcionalidade para formatar conteúdo

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

usando códigos HTML (por exemplo, `<p>`, `<a href>`, `<b>`, `<font>`, `<img>`). Se você definir *glide.html.escape_script* como **falsa**, os marcadores (`<script></script>`) podem surgir quando você selecionar essa coluna em uma exibição de lista ao exibir uma tabela ou lista de registros.

Um invasor mal-intencionado pode inserir código JavaScript incorporando-o nos marcadores (`<script></script>`). O invasor pode se aproveitar ao injetar um vetor JS sofisticado que pode ser executado quando qualquer usuário abrir o registro da tabela.

Aviso: Esta é uma propriedade tipo porto seguro, o que significa que o valor não pode ser alterado após ser mudado. A reversão não é possível.

Mais informações

Atributo	Descrição
Nome da propriedade	*glide.html.escape_script*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Categoria	Validação, limpeza e codificação
Finalidade	Prevenir ataques de script entre sites contra uma aplicação.
Valor recomendado	verdadeiro
Valor-padrão	verdadeiro
Classificação de risco de segurança	8,8
Impacto funcional	(Médio) Esta correção impõe o escape de JavaScript na IU e renderiza os resultados codificados para o usuário. Ela pode ter um impacto na funcionalidade com base na interação do usuário da instância com os dados resultantes.
Risco à segurança	(Alto) A validação de entrada deve ocorrer na aplicação para defesa contra ataques de script entre sites. Esses ataques permitem que scripts externos sejam executados na sessão do usuário no contexto do navegador logado. Os invasores podem usá-los para roubar informações da sessão e dados confidenciais.
Referências	Propriedades do sistema disponíveis Configurações de Alta Segurança

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Como fazer escape de scripts Jelly [Atualizado na Central de segurança 1.3]

Use a propriedade *glide.ui.escape_all_script* para forçar o escape de todos os scripts injetados no Jelly.

Ela escapa de todas as cadeias de caracteres JS e HTML incluídas em<j:jelly> `...` </j:jelly> antes de serem gravadas no fluxo de saída, evitando que vários problemas de XSS ocorram.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mais informações

Atributo	Descrição
Nome da propriedade	*glide.ui.escape_all_script*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	booliano
Categoria	Validação, limpeza e codificação

Finalidade	Se a propriedade não estiver definida como **verdadeira**, os desenvolvedores precisarão executar várias etapas em cada script Jelly personalizado para evitar problemas de XSS. Essas etapas incluem localizar as variáveis Jelly enviadas para o fluxo de saída para renderizar em páginas da Web e executar o escape em cada um dos seguintes marcadores:
	
	`$â {JS:expression}`
	
	`$â {HTML:expression}`
	
	OU
	
	`$â {JS,HTML:expression}`

Valor recomendado	verdadeiro
Valor-padrão	verdadeiro
Classificação de risco de segurança	7,3
Impacto funcional	(Médio) Esta correção impõe o escape do Jelly no nível do analisador. Ela pode ter um impacto na funcionalidade na interação do usuário da instância com os dados resultantes.
Risco à segurança	(Alto) A validação de entrada deve ocorrer em todas as entradas do usuário inseridas na aplicação. Ao fazer isso, os ataques de injeção contra a plataforma podem ser defendidos e protegidos.
Solução alternativa	A IU pode ser afetada porque alguns dos scripts e marcadores HTML projetados para renderização em uma página da Web podem aparecer quebrados. Esta correção envia a página codificada de saída para o navegador renderizar. Por exemplo, em vez de `'minha cadeia de caracteres aqui'`, ela pode exibir `'<u>minha cadeia de caracteres aqui</u>`, já que o marcador `<u>` teve o escape correto. Nesse caso, para impedir o escape, adicione o prefixo NOESC à expressão do Jelly para impedir o escape de JS. Por exemplo:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
	• Antes: ($[jvar_context_menus]); • Depois: `($[NOESC: jvar_context_menus]);` • Antes: $[jvar_ui_policy_scripts] • Depois: `$[NOESC: jvar_ui_policy_scripts]`
Referências	Configurações de Alta Segurança Marcadores Jelly

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Scripts de escape no bloco de anotações [Atualizado na Central de segurança 1.3]

Saiba como o bloco de anotações afeta a postura de segurança da sua instância e como gerenciá-lo para que scripts mal-intencionados não possam ser executados nele.

O bloco de anotações é uma maneira fácil de definir informações no servidor que você pode acessar no navegador. Um administrador pode criar scripts para qualquer coisa, incluindo registros arbitrários. Se esta propriedade não estiver definida com o valor recomendado de **verdadeira**, será possível executar scripts mal-intencionados, como uma vulnerabilidade de script entre sites.

Mais informações

Atributo	Descrição
Nome da configuração	*glide.ui.escape_scratchpad*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	booliano
Valor recomendado	verdadeiro
Valor-padrão	verdadeiro
Categoria	Validação, limpeza e codificação
Risco à segurança	• Pontuação de gravidade: 6,5 • Pontuação do CVSS: média • Detalhes de risco de segurança: se esta propriedade não estiver definida com o valor recomendado de **verdadeiro**, será possível executar scripts mal-intencionados, como uma vulnerabilidade de script entre sites.
Dependências e pré-requisitos	Nenhum
Referências	Administração do Fluxo de trabalho

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Como fazer escapes de marcação XML [Atualizado na Central de segurança 1.3]

Use a propriedade *glide.ui.escape_text* para forçar o escape de valores XML no nível do analisador antes de transmiti-los ao navegador do cliente.

O script entre sites ocorre quando um invasor injeta JavaScript mal-intencionado em um ponto de entrada. A plataforma/aplicação não consegue escapar do JavaScript malicioso antes de transmiti-lo ao navegador da vítima para execução. O escape neste contexto significa o seguinte:

- **&** --> `&`
- **<** --> `<`
- **>** --> `>`
- **"** --> `"`
- **'** --> `'`
- **/** --> `/`

Exemplo: `<script>alert('XSS Attack');</script>`

Escape: `<script>alert('XSS Attack');</script>`

Certifique-se de que a propriedade *glide.ui.escape_text* exista na tabela sys_properties e esteja definida como verdadeira.

Aviso: Esta é uma propriedade tipo porto seguro, o que significa que o valor não pode ser alterado após ser mudado. A reversão não é possível.

Mais informações

Atributo	Descrição
Nome da propriedade	*glide.ui.escape_text*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Categoria	Validação, limpeza e codificação
Finalidade	O escape de XML garante que os navegadores não analisem o JavaScript mal-intencionado incorporado em dados não confiáveis e o executem como JavaScript. • Um usuário mal-intencionado pode tentar um ataque XSS para sequestrar a sessão de outros usuários ou redirecionar o usuário para um site mal-intencionado. • A NOW Platform contém código para proteger os cookies, mas o escape depende desta propriedade ser definida como **verdadeira**.
Valor recomendado	verdadeiro
Classificação de risco de segurança	8,8

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Impacto funcional	(Médio) Essa correção impõe a codificação XML no nível do analisador XML na interface do usuário. Ele renderiza os resultados codificados para o usuário, o que pode ter um impacto na funcionalidade com base na interação do usuário da instância com os dados resultantes.
Risco à segurança	(Alto) A validação de entrada deve ocorrer na aplicação para defesa contra ataques de script entre sites. Esses ataques permitem que scripts externos sejam executados na sessão do usuário no contexto do navegador logado. Os invasores podem usá-los para roubar informações da sessão e dados confidenciais.

Solução alternativa	Depois de definir esta propriedade como **verdadeira**, a renderização é interrompida nos marcadores HTML na descrição do item do catálogo ou no texto de ajuda da variável do item do catálogo. Você pode não conseguir usar a formatação HTML em alguns campos.
	
	No entanto, se a propriedade *glide.ui.escape_text* for desativada, todas as expressões JEXL serão prefixadas com um codificador de saída:
	
	`${JS:expression}`
	
	`${HTML:expression}`
	
	ou
	
	`${JS,HTML:expression}`

Escapar resposta XML

Gerencie como os escapes XML são tratados em sua instância.

Use esta propriedade para gerenciar se as respostas XML têm escape. Se a propriedade estiver definida com o valor recomendado de **falsa**, as respostas XML não terão escape, o que pode resultar em um ataque de injeção de XML. A injeção de conteúdo XML não intencional em uma mensagem XML pode alterar a lógica pretendida de uma aplicação.

Mais informações

Atributo	Descrição
Nome da configuração	*glide.soaprequest.unescape_xml_response*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	booliano
Valor recomendado	falso
Valor-padrão	falso

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Categoria	Validação, limpeza e codificação
Risco à segurança	• Pontuação de gravidade: 6,4 • Pontuação do CVSS: média • Detalhes do risco à segurança: definir esta propriedade como **falsa** desabilita o escape de XML, o que pode resultar em um ataque de injeção de XML.
Dependências e pré-requisitos	Nenhum

Como habilitar o Sanitizer de HTML [Atualizado na Central de segurança 1.3]

Use a propriedade *glide.html.sanitize_all_fields* para habilitar a inclusão de script HTMLSanitizer, que limpa a entrada de HTML, de acordo com os atributos das listas de exclusões e de inclusões configuradas em um script.

Os tipos de campo disponíveis com dicionário/campos incluem HTML e HTML traduzido. Esses campos de entrada HTML permitem que os usuários gravem entrada no formato HTML, por exemplo:

`<h1>Teste</h1>`), usando os marcadores HTML mais básicos, como `<img>`, `<a href …>`e `<iframe>`.

Isso pode abrir uma porta para que um invasor injete um vetor mal-intencionado com marcadores HTML, como:

```
[<IMG SRC=" &#14; JavaScript:alert('XSS');">] [<IMG
onmouseover="alert('xss')">], [a href="" onclick=alert (/xss/)].
```

Mais informações

Atributo	Descrição
Nome da propriedade	*glide.html.sanitize_all_fields*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Categoria	Validação, limpeza e codificação
Finalidade	Prevenir ataques de script entre sites e injeção de HTML à aplicação
Valor recomendado	verdadeiro
Valor-padrão	verdadeiro
Classificação de risco de segurança	8,8
Impacto funcional	(Alto) Esta correção impõe o mecanismo de codificação de saída HTML antes que os dados do usuário sejam renderizados de volta para o usuário. Se o cliente tiver alguma personalização que envolva a renderização do atributo HTML ou dos dados de conteúdo, haverá um impacto na funcionalidade.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Risco à segurança	(Alto) A entrada do usuário deve ser tratada com segurança quando os dados são armazenados e processados na aplicação. Isso reduz os ataques de script entre sites do lado do cliente ao codificar os dados de saída.
Solução alternativa	Esta propriedade limpa todos os campos HTML no sistema. Se você precisar habilitar a limpeza de HTML em campos individuais, consulte Habilitar a limpeza em campos individuais. Você também pode configurar a lista de inclusões ou de exclusões para limpar marcadores HTML e atributos de acordo com a política da sua organização.
Referências	Habilitar o limpador de HTML Limpador de HTML

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Restrição de pacotes Java permitidos [Atualizado na Central de segurança 1.3]

Configurar essas propriedades protege contra APIs perigosas expostas ao mecanismo de script.

Configure as tabelas do sistema e instale o plug-in recomendado de acordo.

Se a tabela *sys_whitelist_member* e *sys_whitelist_package* não forem valores vazios, APIs perigosas poderão ser expostas ao mecanismo de script. As entradas correspondem ao namespace Java que não foi aprovado pelas equipes de segurança da ServiceNow.

Instale o Packages call removal tool. Consulte Packages call removal tool para obter detalhes.

Entre em contato com Suporte e atendimento ao cliente para editar essas tabelas.

Mais informações

Atributo	Descrição
Tabela, nome do plug-in	Tabelas: • *sys_whitelist_member* • *sys_whitelist_package* Plug-in: com.glide.script.packages_call_removal
Tipo de configuração	Configuração tabular, plug-ins
Categoria	Validação, limpeza e codificação

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Finalidade	Proteger contra APIs perigosas expostas ao mecanismo de script.
Valor recomendado	Vazio
Valor padrão	Nenhum. Essa é uma configuração de tabela e não uma propriedade do Glide; portanto, não há valor padrão.
Tipo de configuração	lista de tabelas, plug-in
Risco à segurança	(Alto) APIs perigosas podem ficar expostas ao mecanismo de script. Essas APIs compatíveis provavelmente introduzirão instabilidade e insegurança na instância.
Classificação de risco de segurança	8,2

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Packages call removal tool

Habilite e execute o plug-in Packages Call Removal Tool (*com.glide.script.packages_call_removal*) e analise se cada uma das mudanças propostas deve ser concluída ou rejeitada.

O Packages Call Removal Tool é um plug-in que:

- Verifica scripts em busca de chamadas de pacote para classes Java da Now Platform.
- Propõe mudanças para substituí-las por nomes GlideScript preferenciais.
- Facilita as mudanças de script.

Nota: Se este registro for um registro do sistema de base, o uso da recomendação da ferramenta fará com que o item seja marcado como customer_update. No entanto, ainda pode ser útil usar essa ferramenta porque ela sinaliza Pacotes, chamadas xxx.

O Packages Call Removal Tool pode relatar algumas chamadas de pacote usadas em `sa_mapping_ext_commands` e `sa_custom_operation`. Essas chamadas de pacote pertencem ao MID Server. Como não há classes, o código é executado no MID Server. Se você encontrar qualquer uma das chamadas de pacote listadas a seguir na seção Erros, marque-as como Rejeitadas (Ignoradas). A ferramenta não relata essa chamada de pacote novamente.

- `Packages.com.snc.sw.util.JSONUtil.toJSONPlain(file_content);`
- `Packages.com.snc.sw.util.JSONUtil.toJSONPlain(file_name);`
- `Packages.com.snc.sw.commands.HttpCallHandler;`
- `Packages.com.snc.sw.dto.ProviderType.SSH`

Mais informações

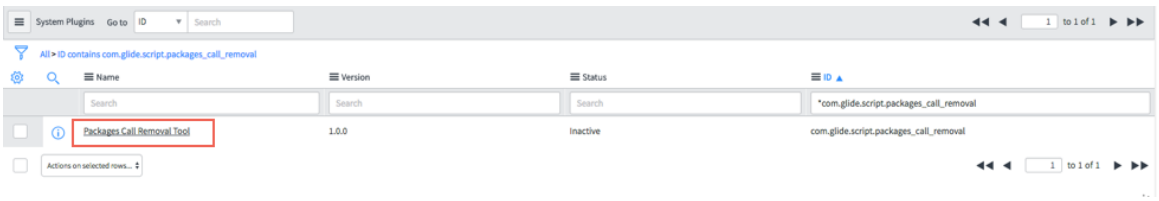
Atributo	Descrição
Nome do Plug-in	com.glide.script.packages_call_removal

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

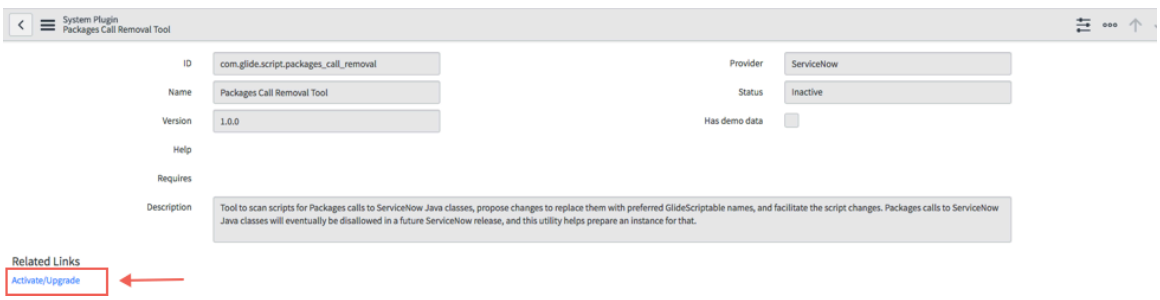
Atributo	Descrição
Tipo de configuração	Definição do sistema > Plug-ins
Finalidade	Remover/substituir chamadas de pacote/membro não autorizadas por nomes Glide aceitáveis (GlideScriptable) que só permitem o acesso autorizado aos dados.
Valor recomendado	Ativo
Impacto funcional	(Baixo) Esta correção substitui as chamadas de pacote por APIs `GlideScriptable` e pode afetar as personalizações que incluem chamadas de pacote. A ferramenta não substitui as chamadas de pacote automaticamente. Em vez disso, ela fornece sugestões que são armazenadas na tabela packages_call_item. Seu administrador pode decidir se aceita ou rejeita a mudança proposta.
Risco à segurança	(Médio) As chamadas de API do lado do cliente que resultam na recuperação de dados ou no acesso a objetos no servidor são consideradas perigosas do ponto de vista da segurança. Elas devem ser validadas para autorização e restrição de acesso a objetos confidenciais.

Etapas para configurar

1. Navegue até **Definição do sistema** > **Plug-ins**.

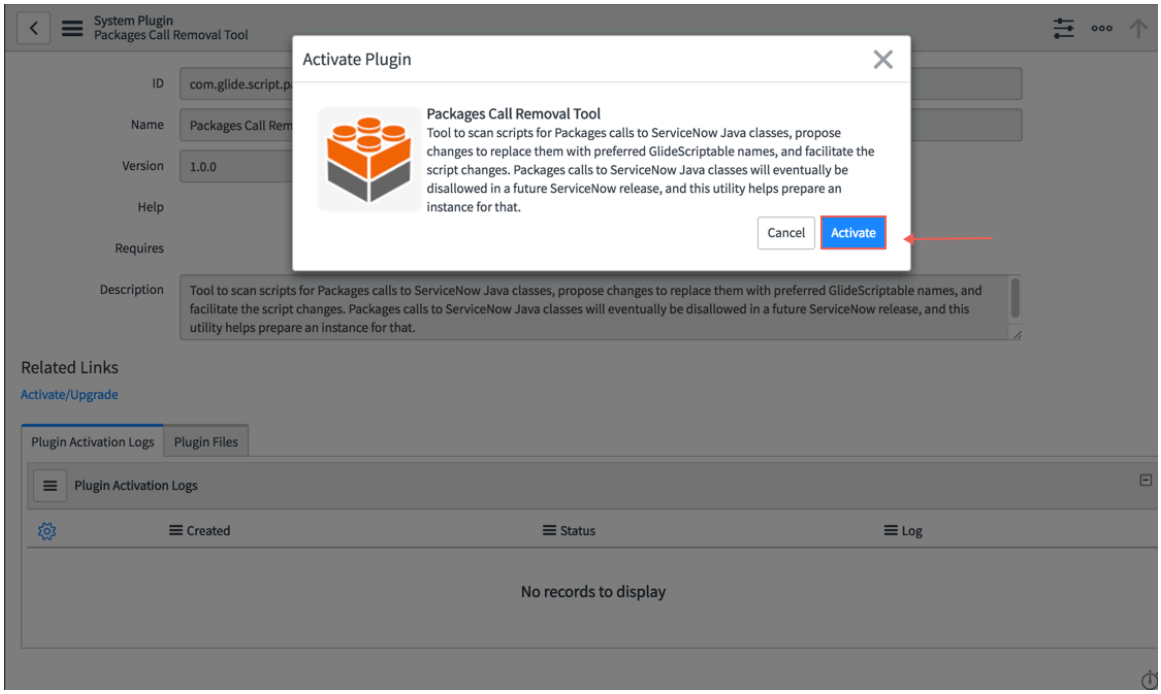


2. Pesquise o plug-in ID = `com.glide.script.packages_call_removal`.



3. Clique em **Ativar/Fazer upgrade** para ativar o plug-in.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Para verificar chamadas de pacote de lista de inclusões e chamadas de membro da lista de inclusões, conclua as ações descritas nas seções Etapas para configurar nos seguintes tópicos:
   - Verificar chamadas de membros da lista de permissões
   - Verificar chamadas de pacotes da lista de permissões

Nome distinto inicial do LDAP não definido [Atualizado na Central de segurança 1.3]

Use esta propriedade para gerenciar o nome distinto de um registro do servidor LDAP.

Esta propriedade controla o nome distinto de um registro do servidor LDAP que é inserido durante a execução de um script de correção OOB (out-of-the-box, pronto para uso). Se definida com o valor recomendado de "" ou em branco, os dados do servidor LDAP poderão ser enumerados por um usuário com privilégios menores.

Mais informações

Atributo	Descrição
Nome da configuração	*glide.ldap.initial.dn*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	cadeia de caracteres
Valor recomendado	em branco
Valor padrão	em branco
Categoria	Validação, limpeza e codificação
Risco à segurança	• Pontuação de gravidade: 2,7 • Pontuação de CVSS: baixa

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
	• Detalhes do risco à segurança: definir o valor da propriedade como '"' ou em branco pode tornar os dados do servidor LDAP acessíveis para um usuário com privilégios menores.
Dependências e pré-requisitos	Nenhum

Como impor a segurança estrita de cookies de sessão [Atualizado na Central de segurança 1.3]

Use a propriedade *glide.ui.secure_cookies* para exigir cookies formatados corretamente

Quando você define a propriedade como verdadeira, sua instância rejeita uma sessão se o cookie associado não estiver no formato esperado.

Aviso: Esta é uma propriedade tipo porto seguro, o que significa que o valor não pode ser alterado após ser mudado. A reversão não é possível.

Mais informações

Atributo	Descrição
Nome da propriedade	*glide.ui.secure_cookies*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Categoria	Validação, limpeza e codificação
Finalidade	Obter uma autenticação de sessão mais segura.
Valor recomendado	verdadeiro
Valor-padrão	verdadeiro
Classificação de risco de segurança	8,8
Impacto funcional	(Baixo) Quando a propriedade é definida como verdadeira, os cookies formatados incorretamente são rejeitados. Quando esse tipo de cookie é rejeitado, o usuário deve fazer login novamente.

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Como minimizar o limite de expansão da entidade [Atualizado na Central de segurança 1.3]

Use a propriedade *glide.xmlutil.max_entity_expansion* para alterar o limite máximo de expansão da entidade para um número menor.

A Now Platform não processa outras expansões de entidade que sejam maiores do que o limite permitido especificado nesta propriedade.

Nota: 500 é o mínimo padrão imposto pela Now Platform, que é considerado um limite seguro.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mais informações

Atributo	Descrição
Nome da propriedade	*glide.xmlutil.max_entity_expansion*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Categoria	Validação, limpeza e codificação
Finalidade	Este controle de correção deve ser habilitado para defesa contra ataques de expansão de entidade XML/Billion laughs.
Valor recomendado	3000
Valor padrão	100.000
Classificação de risco de segurança	5,3
Impacto funcional	(Baixo) Se a personalização estiver usando a expansão de entidade grande, a Now Platform poderá bloquear o processamento posterior.
Risco à segurança	(Moderado) Um invasor pode usar esta vulnerabilidade para expandir os dados de forma exponencial, consumindo rapidamente todos os recursos do sistema.

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Restrição de tipos MIME carregados [Atualizado na Central de segurança 1.3]

Use a propriedade *glide.security.file.mime_type.validation* para ativar a verificação de tipo MIME para uploads. Você pode habilitar (definir a propriedade como **verdadeira**) ou desabilitar (defini-la como **falsa**) a validação do tipo MIME para anexos de arquivo.

Pré-requisitos

Antes de definir esta propriedade, defina a propriedade *glide.attachment.extensions*. Somente as extensões especificadas em *glide.attachment.extensions* são verificadas quanto ao tipo MIME durante o upload. Para saber mais, consulte Restringir extensões de arquivo.

Mais informações

Atributo	Descrição
Nome da propriedade	*glide.security.file.mime_type.validation*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Categoria	Validação, limpeza e codificação
Finalidade	Impor a verificação de tipo MIME/bytes mágicos durante uploads de arquivo.
Valor recomendado	verdadeiro

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Valor-padrão	verdadeiro
Classificação de risco de segurança	5,4
Impacto funcional	(Médio) Esta correção permite a verificação do tipo MIME nos anexos da aplicação. Não há nenhum impacto na funcionalidade, a menos que haja uma intenção mal-intencionada ao carregar os arquivos, já que esta validação está apenas verificando se há falhas de sincronização entre o tipo MIME e os dados.
Risco à segurança	(Médio) Para reduzir vulnerabilidades, como inclusão de arquivo e uploads de arquivo mal-intencionados, a verificação do tipo MIME deve ser habilitada.
Referências	Administrar anexos

Consulte Configurações de proteção de segurança da instância para obter detalhes sobre como configurar propriedades de proteção.

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Restrição de entidades externas XML [Atualizado na Central de segurança 1.3]

Use a propriedade *glide.security.file.mime_type.validation* para ativar a verificação de tipo MIME para uploads. Você pode habilitar (definir a propriedade como **verdadeira**) ou desabilitar (defini-la como **falsa**) a validação do tipo MIME para anexos de arquivo.

Pré-requisitos

Antes de definir esta propriedade, defina a propriedade *glide.attachment.extensions*. Somente as extensões especificadas em *glide.attachment.extensions* são verificadas quanto ao tipo MIME durante o upload.

Aviso: Esta é uma propriedade tipo porto seguro, o que significa que o valor não pode ser alterado após ser mudado. A reversão não é possível.

Mais informações

Atributo	Descrição
Nome da propriedade	*glide.xml.entity.whitelist*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Categoria	Validação, limpeza e codificação
Finalidade	Esse controle de correção deve ser ativado para se defender contra ataques XXE.
Valor recomendado	verdadeiro
Valor-padrão	verdadeiro

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Classificação de risco de segurança	5,4
Impacto funcional	(Baixo) Se a personalização estiver usando uma entidade externa, não a inclusão listada na propriedade *glide.xml.entity.whitelist*, a NOW Platform poderá bloquear o processamento adicional.
Risco à segurança	(Crítico) Um invasor pode usar o DTD para incluir solicitações HTTP arbitrárias que o servidor pode executar. Isso pode levar a outros ataques usando o relacionamento de confiança do servidor com outras entidades.

Exigência de validação da entidade XMLdoc2 com expansão da entidade allowlistDisable [Atualizado na Central de segurança 1.3]

Se as personalizações não exigirem expansão de entidade, use a propriedade *glide.xmlutil.max_entity_expansion* para desabilitar completamente a expansão de entidade externa. O XML conclui a análise, mas não inclui entidades internas ou externas.

- Se você definir esta propriedade como **verdadeira**, todas as entidades externas tentarão resolver ou expandir as entidades de assunto, sujeitas à configuração da propriedade *glide.stax.whitelist_enabled*.
- Se você definir essa propriedade como **falsa**, todas as resoluções e expansões da entidade serão bloqueadas. Para saber mais, consulte Validação de entidade XMLdoc2 com lista de permissões.

Pré-requisitos

Antes de definir esta propriedade:

- Defina as propriedades *glide.xml.entity.whitelist.enabled* e *glide.stax.whitelist_enabled* como verdadeiras. Para aprender mais, consulte Validação de entidade XMLdoc/XMLUtil com lista de permissões e Validação de entidade XMLdoc2 com lista de permissões.
- Defina uma lista de FQDN delimitada por vírgulas na propriedade *glide.xml.entity.whitelist*, que são os únicos URLs que podem ser acessados usando a propriedade de processamento de entidade de XML. Para saber mais, consulte Processamento de entidade externa XML - lista de permissões.

⚠ **Aviso:** Esta é uma propriedade tipo porto seguro, o que significa que o valor não pode ser alterado após ser mudado. A reversão não é possível.

Mais informações

Atributo	Descrição
Nome da propriedade	*glide.stax.whitelist_enabled*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Categoria	Validação, limpeza e codificação

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Finalidade	Este controle de correção deve ser habilitado para defesa contra um ataque de expansão de entidade XML/Billion laughs.
Valor recomendado	verdadeiro
Valor-padrão	falso
Classificação de risco de segurança	9,8
Impacto funcional	(Baixo) Se a personalização estiver usando expansão de entidade, então, a Now Platform pode bloquear o processamento adicional.
Risco à segurança	(Crítico) Um invasor pode usar esta vulnerabilidade para expandir os dados de forma exponencial, consumindo rapidamente todos os recursos do sistema.
Solução alternativa	Se a personalização exigir expansão da entidade, defina esta propriedade como verdadeira e siga as etapas documentadas na Validação de entidade XMLdoc2 com lista de permissões.

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Para obter mais informações sobre os recursos OWASp, consulte OWASp.

Definir uma política de segurança de conteúdo para arquivos SVG [Novo na Central de segurança 1.3]

A propriedade *com.glide.csp.self_script_src_svg* adiciona a diretiva **script-src none** ao cabeçalho Content-Security-Policy HTTP quando Scalable Vetor Graphics (SVGs) são acessados por meio da extensão de arquivo Translation Memory Index (IIX).

A propriedade *com.glide.csp.self_script_src_svg* impede que anexos de arquivo mal-intencionados que armazenam ataques de script entre sites (XSS) sejam executados na instância. Sem esta política, um agente mal-intencionado pode induzir um usuário a executar código JavaScript arbitrário no navegador da web, o que pode levar a vulnerabilidades de segurança, como exfiltração de dados e tomada de controle da sessão.

Mais informações

Atributo	Descrição
Nome da configuração	*com.glide.csp.self_script_src_svg*
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Tipo de dados	booliano
Valor recomendado	verdadeiro
Valor-padrão	verdadeiro
Categoria	Validação, limpeza e codificação

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
Risco à segurança	• Pontuação de gravidade: 7,1 • Pontuação de CVSS: alta • Detalhes do risco à segurança: não definir esta propriedade com o valor recomendado pode fazer com que um usuário execute código JavaScript arbitrário de um agente mal-intencionado.
Dependências e pré-requisitos	Nenhum(a)
Impacto funcional	Esta propriedade impede que arquivos Scalable Vector Graphics (SVG) acessem scripts externos.

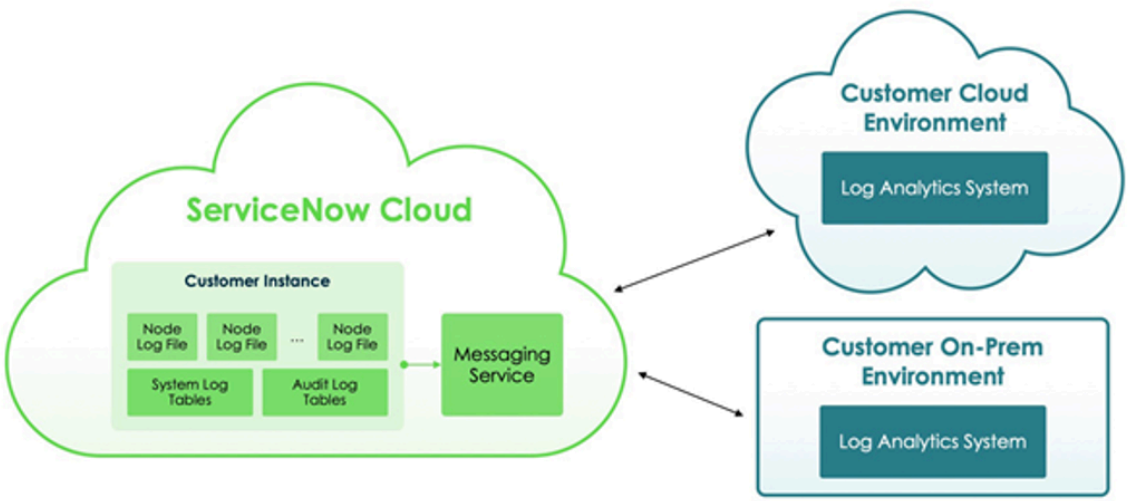
Log de serviço de exportação (LES)

Log de serviço de exportação (LES) permite exportar perfeitamente o sistema da instância e os logs da aplicação para as ferramentas de análise de segurança corporativa. O serviço oferece integração altamente escalonável e praticamente em tempo real com suas ferramentas de análise de fácil manutenção e configuração.

A ferramenta de integração permite que você aproveite suas soluções de análise para executar o seguinte:

- Detectar ameaças à segurança ServiceNow e analisar incidentes de segurança
- Solucionar problemas e otimizar o desempenho do app ServiceNow
- Monitorar e otimizar a experiência do usuário ServiceNow

O LES utiliza um recurso da Now Platform chamado Serviço de envio de mensagens Hermes, que é um serviço de enfileiramento e transmissão de dados multilocatário e de vários clusters que se baseia no Apache Kafka, que permite que sua instância produza e consuma grandes volumes de eventos do Kafka. Apache Kafka é uma plataforma de streaming de dados de código aberto que oferece um ponto único de integração para a troca de dados entre sistemas de negócios da sua organização.



O LES encaminha uma cópia dos eventos de log para Serviço de envio de mensagens Hermes à medida que eles são gerados.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

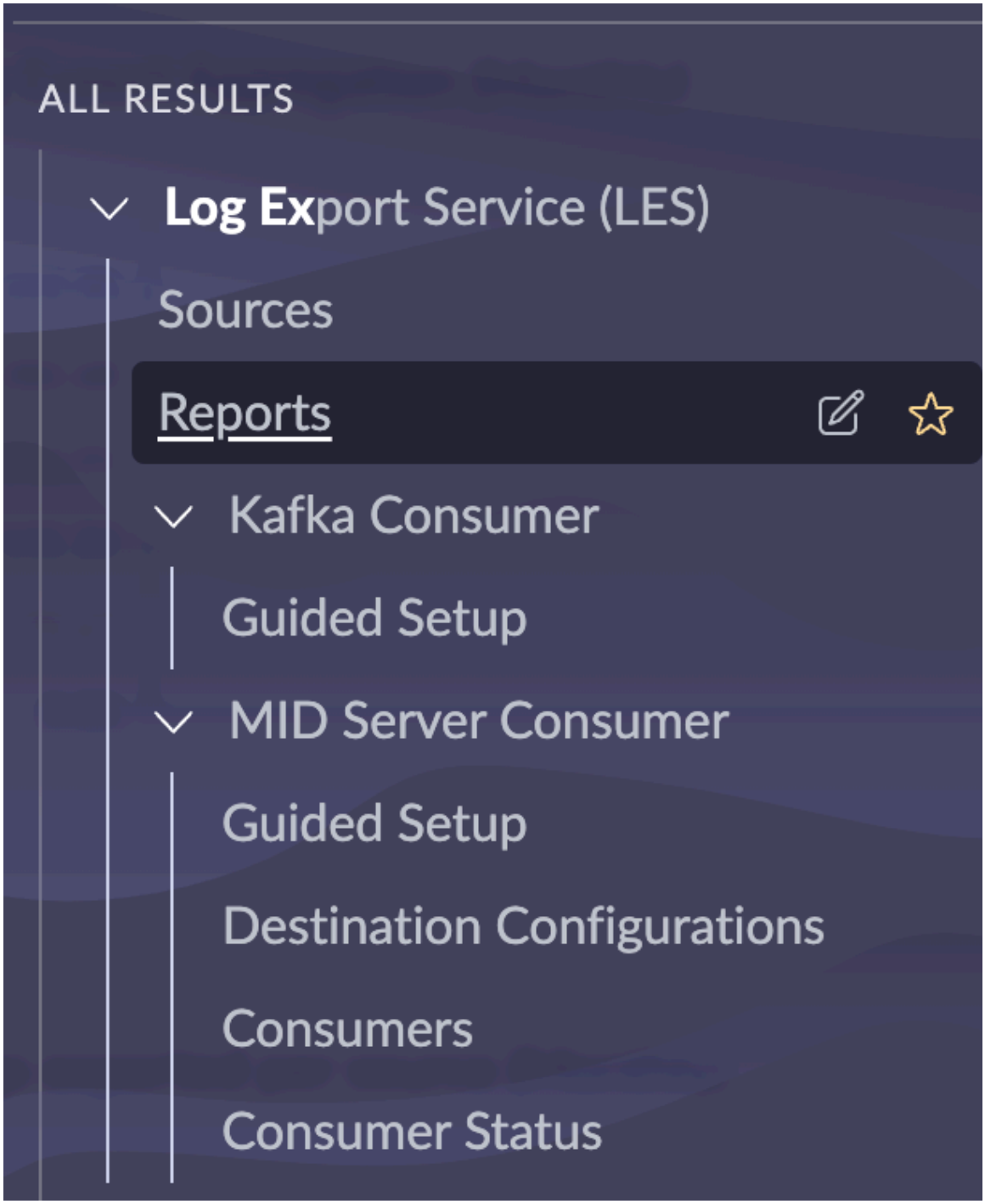
O Serviço de envio de mensagens Hermes é um serviço multilocatário, com vários clusters, de transporte de dados e de enfileiramento criado no Apache Kafka que permite que sua instância produza e consuma grandes volumes de eventos do Kafka. O Serviço de envio de mensagens Hermes é um Recurso da Now Platform disponível como parte de Stream Connect para Apache Kafka, Log de serviço de exportação (LES) e Replicação de dados da instância (IDR).

Os sistemas de análise de log externo, na nuvem ou no local, podem usar e consumir os eventos de log do Serviço de envio de mensagens Hermes. O LES fornece três opções de conectividade para consumir os logs:

- MID Server dedicado: um MID Server dedicado é instalado no local ou na nuvem e se conecta automaticamente a Serviço de envio de mensagens Hermes, extraindo eventos de log continuamente e enviando-os para registrar ferramentas de análise por meio de uma conexão REST.
- Aproveite o conector Kafka da sua solução de análise de log (por exemplo, Splunk): um conector Kafka do produto de análise de log de sua escolha está instalado no local ou na nuvem e conecta-se automaticamente a Serviço de envio de mensagens Hermes, extraindo eventos de log continuamente e enviando-os por push para ferramentas de análise de log.
- Diretamente do seu sistema Kafka: o sistema Kafka se conecta diretamente a Serviço de envio de mensagens Hermes e usa seus comandos de protocolo Kafka nativos e conectividade para extrair eventos de logs dele.

Para configurar e gerenciar o LES, é necessário instalá-lo de ServiceNow Store. A aplicação LES fornece Configurações assistidas para ajudar você a instalar o serviço, páginas para configurar o serviço (origens de log, consumidores e destinos) e relatórios para entender a criação e o consumo de logs.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Nota: Você também pode criar uma nova configuração de fonte. Para obter mais informações, consulte Criar uma configuração de fonte de log.

Funções Log de serviço de exportação

Log de serviço de exportação está instalado com essas funções.

Administrador da aplicação [sn_logstoanalytics.admin]

Para saber mais sobre como gerenciar assinaturas por usuário, consulte Como gerenciar assinaturas por usuário no Gestão de assinaturas e entre em contato com o representante da sua conta.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Esta função é instalada juntamente com a aplicação LES e permite que um usuário não administrador utilize a aplicação.

Contém as funções

Lista de funções contidas na função.

Nenhum.

Grupos

Lista de grupos aos quais esta função está atribuída por padrão.

Nenhum.

Elevado

Se a função é elevada. Funções elevadas não são atribuídas a usuários ou grupos e devem ser usadas por elevação. Para obter detalhes, consulte Elevação para uma função privilegiada.

Nº

Considerações especiais

Nenhum.

Administrador de sistema [admin]

Para saber mais sobre como gerenciar assinaturas por usuário, consulte Como gerenciar assinaturas por usuário no Gestão de assinaturas e entre em contato com o representante da sua conta.

A função de administrador é necessária para a configuração da aplicação de armazenamento LES.

Contém as funções

Lista de funções contidas na função.

- sn_templated_snip.template_snippet_admin
- sn_employee.admin
- taxonomy_admin
- sn_ace.ace_user
- sn_hr_sp.esc_admin

Grupos

Lista de grupos aos quais esta função está atribuída por padrão.

Nenhum.

Elevado

Se a função é elevada. Funções elevadas não são atribuídas a usuários ou grupos e devem ser usadas por elevação. Para obter detalhes, consulte Elevação para uma função privilegiada.

Não.

Considerações especiais

Nenhum.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Origens de log

Log de serviço de exportação (LES) pode exportar origens de log de algumas Tabelas de log do sistema, a Tabela de auditoria e Arquivos de log do nó da aplicação.

A seguir estão as origens de log que podem ser exportadas pelo LES.

- Tabelas de log do sistema
  - Tabela syslog: exibe avisos e erros de processos, registros e eventos não críticos de instância, como uso de memória na máquina do servidor
  - Tabela syslog_transaction: exibe todas as atividades do navegador para uma instância
  - Tabela sys_outbound_http_log: exibe todas as solicitações e respostas para serviços web de saída, como REST e SOAP
- Tabela de auditoria: use a tabela sys_audit para exibir as mudanças de registro feitas nas tabelas escolhidas para serem auditadas
- Arquivos de log do nó da aplicação: use os arquivos de log do host local para exibir os erros do nó da aplicação. Sua instância terá vários nós, e cada nó terá vários arquivos de log.

Consulte Logs do sistema para saber mais sobre o esquema e a finalidade das origens de log acima.

Criar uma configuração de fonte de log

Regule e defina filtros nos logs a serem encaminhados criando uma configuração de fonte de log.

Antes de Iniciar

Função necessária: administrador ou sn_logstoanalytics.admin

Procedimento

1. Navegue até **Todos** > **Serviço de exportação de log**.
   Uma lista de configurações de fonte é exibida.
2. Selecione **Novo** se quiser criar uma nova configuração de fonte.
   Você também pode selecionar uma configuração de fonte existente se quiser modificá-la.
   O formulário fonte é exibido.
3. No formulário, preencha os campos.

Formulário fonte

Campos	Descrição
Tipo de fonte	Tipos de fontes de log ◦ Log de Nó ◦ Tabela Para obter mais informações, consulte Origens de log.
Nível de Log	Um conjunto de níveis de registro em log padrão que podem ser usados para controlar a saída de registro em log. Seguindo a convenção, cada nível

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campos	Descrição
	encaminhará logs de severidade igual ou superior. **Nota:** Este campo fica visível somente quando uma das condições a seguir é atendida. ◦ Quando você seleciona Log de nó como o Tipo de fonte. ◦ Quando você seleciona Tabela como o Tipo de origem e a tabela é syslog
Aceita	Especifica o formato em que os logs são encaminhados para o Hermes. Eles podem ser enviados como JSON ou como texto sem formatação.
Tabela	Seleção de tabela para logs do tipo de tabela. **Nota:** Este campo fica visível somente quando você seleciona Tabela como o Tipo de fonte.
Tipo de Filtro	Condições para encaminhar logs de forma seletiva. **Nota:** Este campo ficará visível somente se você selecionar syslog ou sys_audit como a tabela.

4. Selecione **Enviar** para criar uma nova configuração de fonte.

Como criar vários tópicos na tabela de origem do LES

Consuma mensagens de cada tipo de fonte de forma independente, criando um tópico exclusivo por tipo de fonte.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Adicione a propriedade do sistema sn_logstoanalytics.kafka.multi_topics e a defina como verdadeira.
   Por padrão, ela é definida como falsa.
2. Crie um novo registro de fonte.

   Nota: Quando você cria um novo tipo de fonte, um tópico exclusivo é criado para ele.

   Os nomes dos tópicos têm o tipo de fonte como sufixo. Por exemplo, sn_logstoanalytics.node_log tem node_log como o tipo de fonte.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Opcional: Crie outro tópico para uma fonte diferente, como nas etapas anteriores.

Nota: Se a propriedade sn_logstoanalytics.kafka.multi_topics estiver definido como falsa, a capacidade de criar vários tópicos na tabela de fontes será desativada.

Nota: Esse recurso não é compatível com o consumidor do MID Server (LES v2). Você deve usar seu próprio consumidor (LES v1).

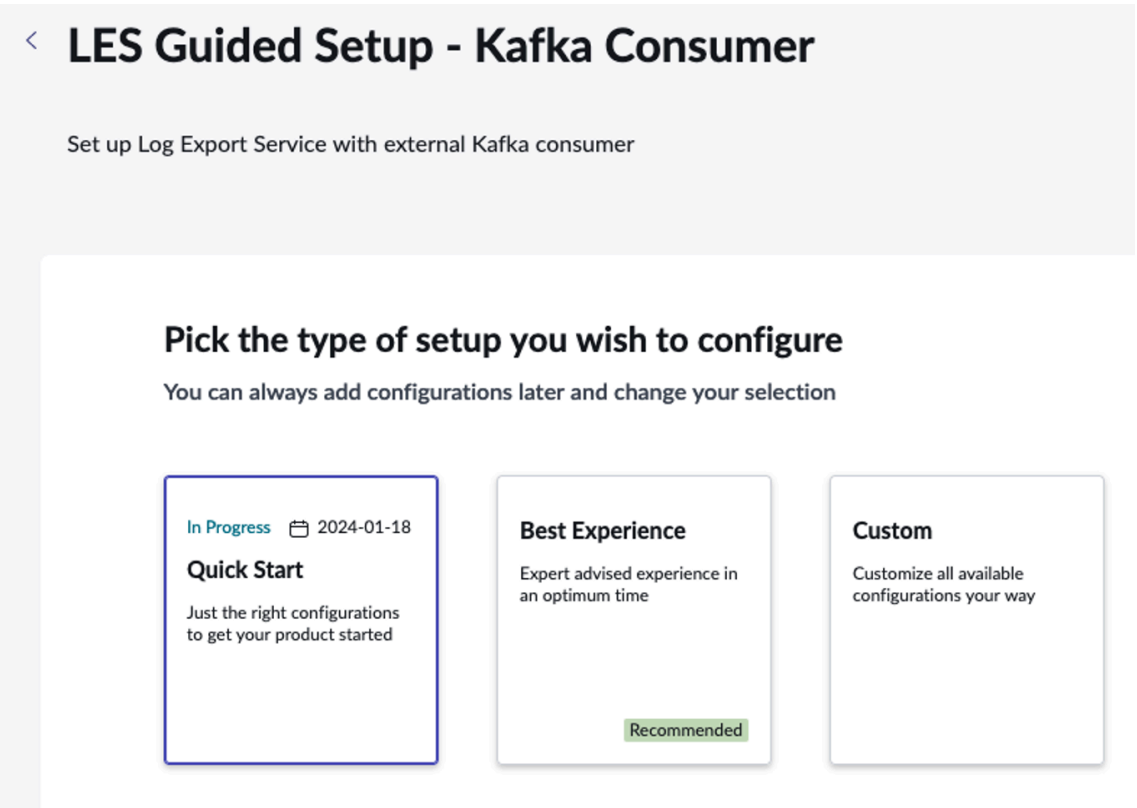
Consumidor do Kafka

Use a configuração assistida para percorrer a configuração inicial do LES. A Configuração assistida ajuda no planejamento da distribuição do produto e na execução da configuração básica para entrar em operação.

A Configuração assistida organiza as atividades de configuração em categorias. Cada categoria fornece informações, como orientações para planejamento, etapas de pré-configuração e links para conteúdos de ajuda úteis. As categorias também fornecem um conjunto de links para as páginas da instância em que realiza a configuração. O processo da Configuração assistida acompanha o que foi feito, para que você possa parar e iniciar novamente de onde parou.

Página inicial da Configuração assistida

A página inicial da Configuração assistida contém os aspectos gerais dos tipos de configuração. Você pode selecionar seu tipo de Configuração assistida e selecionar **Continuar** para abrir as etapas e começar a configuração.



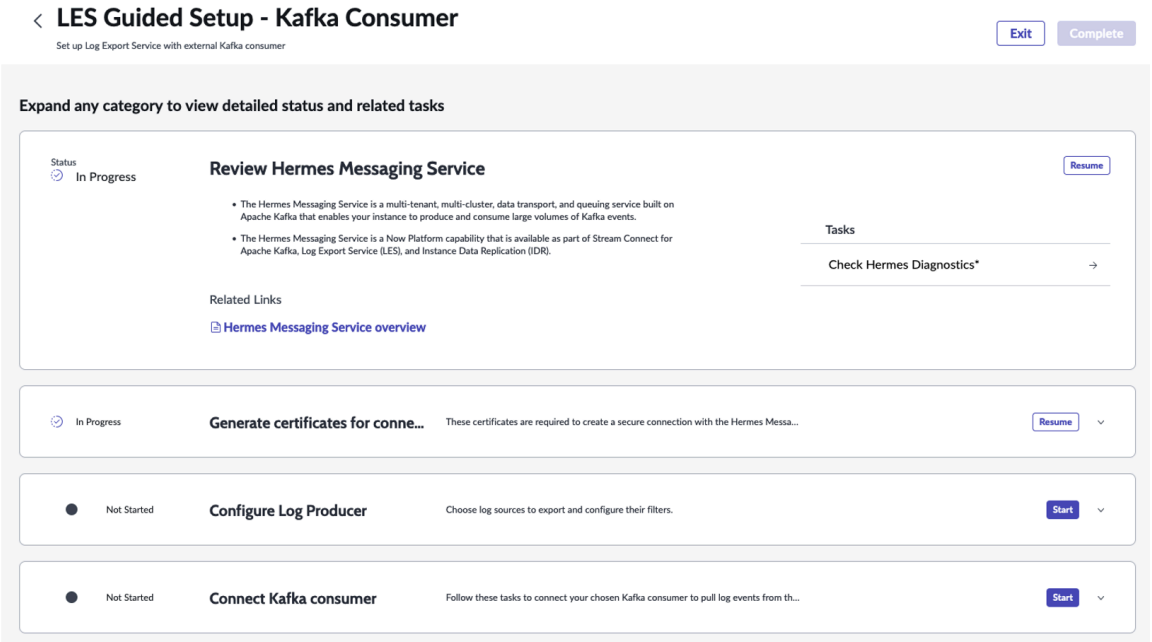
As três configurações dessa página, Início rápido/Melhor experiência/Personalizada oferecem as mesmas tarefas e funcionalidades. Elas são necessárias para coordenar a integração entre a instância da ServiceNow e a ferramenta de análise de log de destino com o respectivo administrador. O administrador de análise de log deve configurar

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a própria ferramenta para se conectar à instância da ServiceNow com segurança. É recomendável compartilhar o documento Configurar uma conexão segura com o Serviço de envio de mensagens Hermes com o administrador de análise de log com antecedência. Mesmo que você tenha marcado uma tarefa como concluída, é possível voltar e marcá-la como "em andamento". Para fazer isso, clique na caixa **Editar** no canto superior direito da categoria. Em seguida, clique na caixa **Editar** da tarefa que você deseja desmarcar. A caixa **Marcar como concluída** não estará mais marcada.

Página de categorias da Configuração assistida

A página de categorias contém uma visão geral e descrições das categorias e tarefas associadas. Clique na seta suspensa para conferir informações sobre a categoria ou clique no botão "Iniciar" para abrir as etapas da Configuração assistida e começar a configuração.



Siga as instruções de configuração para concluir as tarefas de cada categoria.

Configuração assistida para consumidores do Kafka

Implemente as etapas a seguir para obter uma configuração assistida completa para consumidores do Kafka.

Antes de Iniciar

Navegue até **Serviço de exportação de log (LES)** > **Consumidor do Kafka** > **Configuração assistida**. Selecione o tipo de configuração que você quer definir e clique em **Continuar**.

> **Nota:** Durante a instalação da aplicação Log de serviço de exportação, a ServiceNow provisionará a infraestrutura Serviço de envio de mensagens Hermes subjacente. Observe que a conclusão desse processo pode levar algumas horas desde o momento em que você solicita a instalação da aplicação Log de serviço de exportação.

Função necessária: administrador

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Analise o diagnóstico do Serviço de envio de mensagens Hermes.

   É recomendável verificar se o Serviço de envio de mensagens Hermes está instalado e funcionando com a ferramenta de diagnóstico Hermes, que é exibida na tela durante essa etapa. Se você vir um erro de "Página não encontrada" nessa página, o Hermes não está instalado e é necessário entrar em contato com o administrador do sistema.

   - Informações de configuração: as informações de inicialização a seguir são usadas para a conexão ao Serviço de envio de mensagens Hermes. A “Inicialização do produtor” representa a conexão usada para o envio de mensagens para o Hermes, e “Inicialização do consumidor 1 e 2” são usadas para recuperação de mensagens do Hermes.
     - Inicialização do produtor
     - Inicialização do consumidor 1
     - Inicialização do consumidor 2
   - PKI da instância: o componente de infraestrutura de chave pública (PKI) da instância permite que uma instância da ServiceNow atue como um emissor em uma hierarquia de confiança X.509.
   - Conectividade da inicialização: clique em **Executar teste** para confirmar que o cliente externo pode se conectar às portas de instância definidas (produtor e consumidor).
   - Conectividade da instância: clique em **Executar teste** para confirmar que a instância pode enviar e receber mensagens.
   - Exibir tópicos: clique no tópico listado para recuperar o carimbo de data/hora da última mensagem.

   Nota: Você pode acessar o diagnóstico Hermes no futuro para solucionar possíveis problemas de conectividade, retornando a essa etapa da configuração assistida ou navegando até **Todos** > *Serviço de envio de mensagens Hermes* > **Diagnóstico**.

2. Gere certificados para uma conexão segura ao Serviço de envio de mensagens Hermes e extraia eventos de log dele.

   Você vai usar esses certificados ao conectar o sistema externo.

   Configure uma conexão segura ao Serviço de envio de mensagens Hermes. Para obter mais informações, consulte Configurar uma conexão segura com o Serviço de envio de mensagens Hermes. Você vai precisar desses certificados para autenticação e autorização no cliente que extrairá os logs do Hermes.

   Nota: As funções de administrador ou Hermes_admin são necessárias para essa etapa.

3. Configure o produtor de log: escolha as origens de log para exportar e configurar os filtros. Realize as seguintes tarefas para configurar o produtor de log.

   - Configure as origens de log para exportar: crie um registro de origem para cada uma das origens de log que você quer exportar.

     Nota: As funções de administrador ou sn_logstoanalytics.admin são necessárias para concluir essa etapa

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Clique em **Novo** no canto superior direito

b. Selecione um tipo de origem

c. Selecione os filtros adequados para o tipo de origem selecionado

> **Nota:** Os filtros são diferentes dependendo do tipo de origem selecionado

d. Clique em "Atualizar"
Após a criação, será exibido o nome do tópico do Hermes para o qual a origem do log será exportada. Escreva o nome do tópico, porque você vai precisar dele para configurar o sistema do consumidor de log. O campo Ativo controla se aquela origem de log será exportada ou não. Caso encontre erros, volte para a tarefa "Verificar o Diagnóstico do Hermes" e confira o status dele.

- Valide o Produtor de log: depois de criar uma origem da qual produzir logs, você pode ver registros de log implementados no tópico usando o **Serviço de envio de mensagens Hermes** > **Inspetor de tópicos Hermes**.

a. Selecione "Tópicos externos"

b. Clique em "Listar tópicos"

c. Selecione a linha com o tópico da etapa anterior (listado em "Origens")

d. Ajuste a data de início das mensagens, se necessário

e. Clique em **Exibir** para conferir uma mensagem de log que foi exportada para o tópico

4. Conecte o consumidor do Kafka: conecte o consumidor do Kafka escolhido para extrair eventos de log do Hermes de acordo com estas tarefas.

- Identifique o consumidor do Kafka: você tem duas opções baseadas na arquitetura de análise de log.
  - Se você tiver seu próprio sistema Kafka e escolhê-lo para agregação de log, poderá se conectar diretamente ao serviço de envio de mensagens Hermes usando o protocolo Kafka nativo.
  - Se você preferir conectar a ferramenta de análise de log diretamente ao serviço de envio de mensagens Hermes, será preciso implantar um conector do Kafka compatível com o sistema de análise de log (ou seja, Splunk Connect para Kafka).

> **Nota:** Nos dois casos, é preciso trabalhar com o administrador desses sistemas para coordenar a conexão com o serviço de envio de mensagens Hermes.

- Importe os certificados do Hermes para o sistema do consumidor do Kafka: faça login em seu sistema do consumidor do Kafka e verifique se você tem os direitos de administrador apropriados para configurá-lo e conectá-lo a um sistema externo. Importe os certificados gerados na tarefa "Configurar uma conexão segura com o serviço de envio de mensagens Hermes" para o conector ou o servidor do Kafka. Siga as instruções da documentação do consumidor do Kafka escolhido.
- Configure os processos do Kafka: o serviço de envio de mensagens Hermes foi desenvolvido para oferecer alta disponibilidade. Dois processos são necessários para consumir mensagens do Hermes. Dois processos são necessários porque o Hermes usa alguns clusters do Kafka para fins de failover. Se um cluster ficar inativo, os dados serão produzidos para o outro cluster do Kafka do Hermes.

  Em seu sistema de consumidor do Kafka, será preciso criar dois processos de consumidor separados para se conectar aos dois clusters do Kafka do Hermes. Para os dois

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

processos, especifique o mesmo tópico do Kafka do Hermes, mas configure dois endereços de inicialização separados:

- <instance_name>.service-now.com:4100,<instance_name>.service-now.com:4101,<instance_name>.service-now.com:4102,<instance_name>.service-now.com:4103
- <instance_name>.service-now.com:4200,<instance_name>.service-now.com:4201,<instance_name>.service-now.com:4202,<instance_name>.service-now.com:4203

Observações importantes:

- Ao acessar o tópico do Kafka em sistemas externos, anexe "snc.<instance name>." ao tópico para o qual os logs são encaminhados.
- Configure cada consumidor com o mesmo ID de grupo de consumidores do Kafka.
- Instale os arquivos de repositório de chaves e repositório de confiança em um local em que os consumidores possam acessá-los.
- Se os consumidores pedirem, especifique as propriedades dos conversores JSON do Kafka para desabilitar esquemas: “key.converter.schemas.enable=false”, “value.converter.schemas.enable=false”

◦ Verifique se o consumidor do Kafka extrai logs do Hermes: verifique no consumidor do Kakfa escolhido se é possível extrair eventos de log do serviço de envio de mensagens Hermes.

Consumidor do MID Server

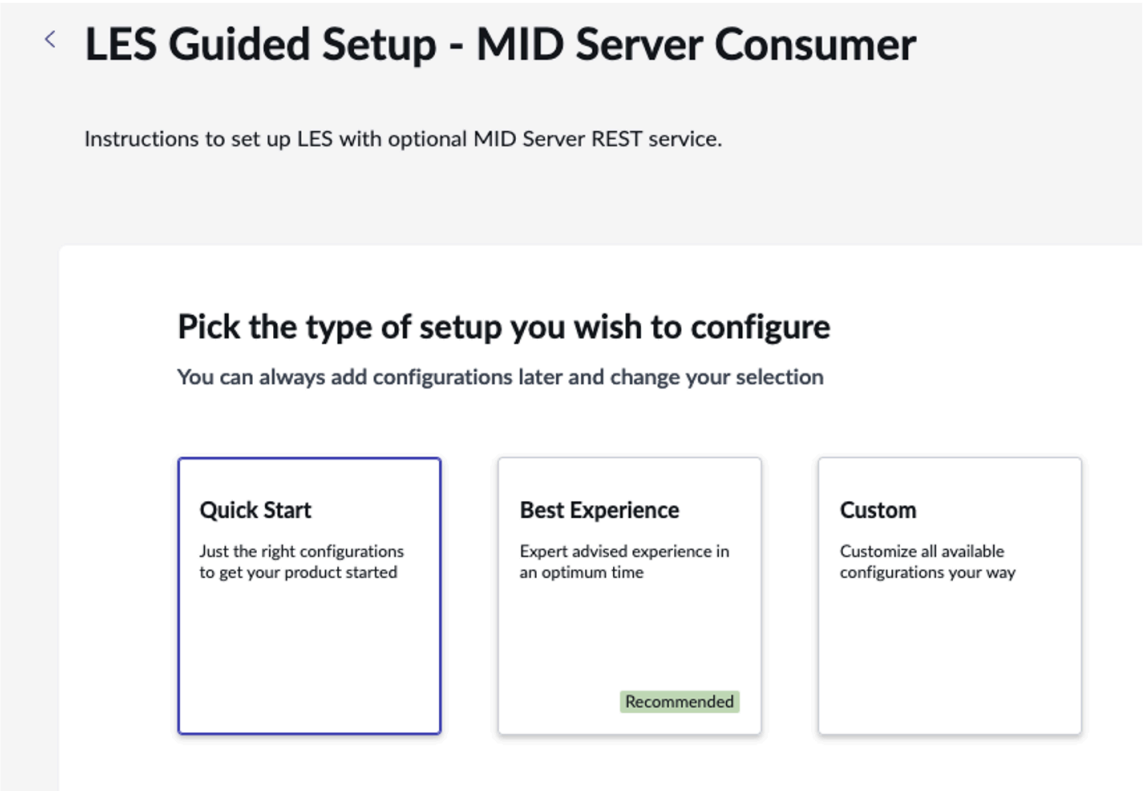
Use a Configuração assistida para percorrer a configuração inicial do LES. A Configuração assistida ajuda no planejamento da distribuição do produto e na execução da configuração básica para entrar em operação.

A Configuração assistida organiza as atividades de configuração em categorias. Cada categoria fornece informações, como orientações para planejamento, etapas de pré-configuração e links para conteúdos de ajuda úteis. As categorias também fornecem um conjunto de links para as páginas da instância em que realiza a configuração. O processo da Configuração assistida acompanha o que foi feito, para que você possa parar e iniciar novamente de onde parou.

Página inicial da Configuração assistida

A página inicial da Configuração assistida contém os aspectos gerais dos tipos de configuração. Você pode selecionar seu tipo de Configuração assistida e selecionar **Continuar** para abrir as etapas e começar a configuração.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

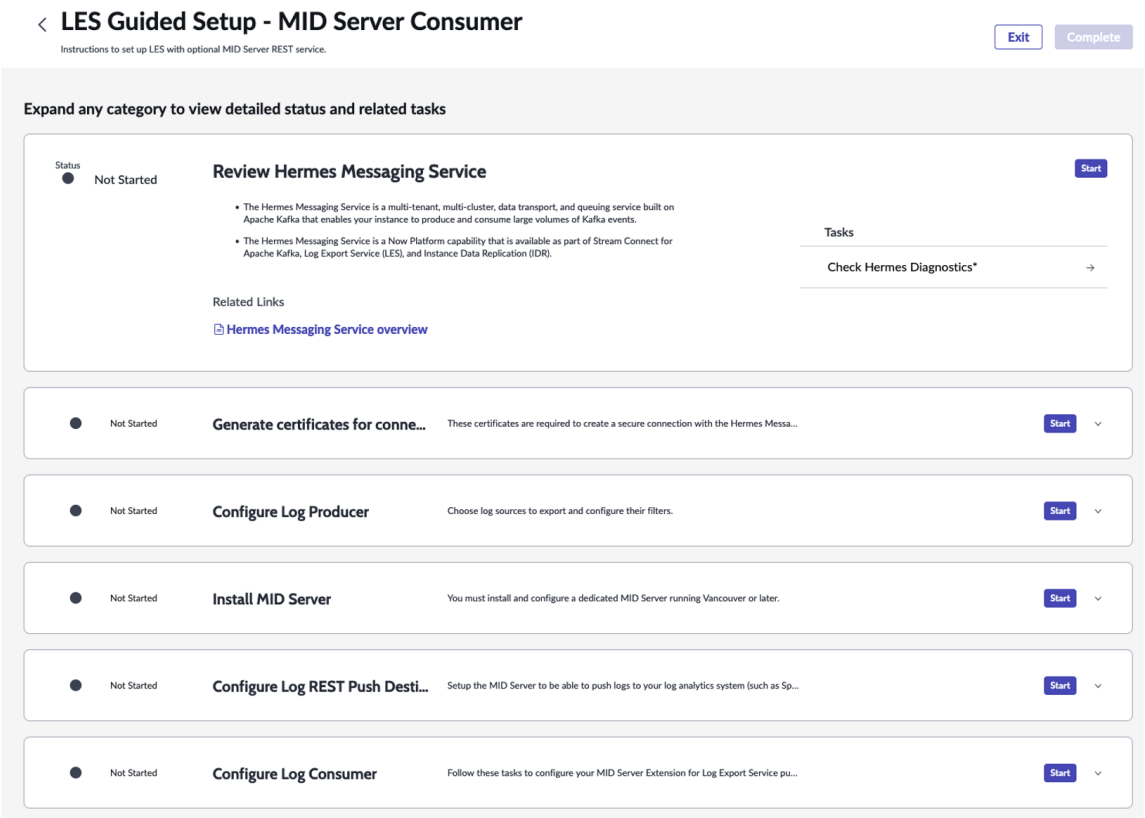


As três configurações dessa página, Início rápido/Melhor experiência/Personalizada, oferecem as mesmas tarefas e funcionalidades. Um MID Server dedicado é necessário para transmitir logs continuamente da instância para o sistema de análise de log. O MID Server precisa de uma configuração única para estabelecer uma conexão segura com o Serviço de envio de mensagens Hermes. Mesmo que você tenha marcado uma tarefa como concluída, é possível voltar e marcá-la como "em andamento". Para fazer isso, primeiro clique na caixa **Editar** no canto superior direito da categoria. Em seguida, clique na caixa **Editar** da tarefa que você quer desmarcar. A caixa **Marcar como concluída** não estará mais marcada.

Página de categorias da Configuração assistida

A página de categorias contém os aspectos gerais e as descrições das categorias e tarefas associadas. Clique na seta suspensa para conferir informações sobre a categoria ou clique no botão **Iniciar** para abrir as etapas da Configuração assistida e começar a configuração.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Siga as instruções de configuração para concluir as tarefas de cada categoria.

Configuração assistida para consumidores do MID Server

Implemente as etapas a seguir para obter uma configuração assistida completa para consumidores do MID Server.

Antes de Iniciar

Navegue até **Serviço de exportação de log (LES)** > **Consumidor do MID Server** > **Configuração assistida**. Selecione o tipo de configuração que você quer definir e clique em **Continuar**.

Nota: Durante a instalação da aplicação Log de serviço de exportação, a ServiceNow provisionará a infraestrutura Serviço de envio de mensagens Hermes subjacente. Observe que a conclusão desse processo pode levar algumas horas desde o momento em que você solicita a instalação da aplicação Log de serviço de exportação.

Função necessária: administrador

Procedimento

1. Analise o diagnóstico do Serviço de envio de mensagens Hermes.

   É recomendável verificar se o Serviço de envio de mensagens Hermes está instalado e funcionando com a ferramenta de diagnóstico Hermes, que é exibida na tela durante essa etapa. Se você vir um erro de "Página não encontrada" nessa página, o Hermes não está instalado e é necessário entrar em contato com o administrador do sistema.

   - Informações de configuração: as informações de inicialização a seguir são usadas para conexão com o Serviço de envio de mensagens Hermes. A "Inicialização do produtor" representa a conexão usada para o envio de mensagens para o Hermes, e

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

"Inicialização do consumidor 1 e 2" são usadas para recuperação de mensagens do Hermes.

- Inicialização do produtor
- Inicialização do consumidor 1
- Inicialização do consumidor 2

◦ PKI da instância: o componente de infraestrutura de chave pública (PKI) da instância permite que uma instância da ServiceNow atue como um emissor em uma hierarquia de confiança X.509.

◦ Conectividade da inicialização: clique em **Executar teste** para confirmar que o cliente externo pode se conectar às portas de instância definidas (produtor e consumidor).

◦ Conectividade da instância: clique em **Executar teste** para confirmar que a instância pode enviar e receber mensagens.

◦ Exibir tópicos: clique no tópico listado para recuperar o carimbo de data/hora da última mensagem.

Nota: Você pode acessar o diagnóstico Hermes no futuro para solucionar possíveis problemas de conectividade, retornando a essa etapa da configuração assistida ou navegando até **Todos** > *Serviço de envio de mensagens Hermes* > **Diagnóstico**.

2. Gere certificados para uma conexão segura com o Serviço de envio de mensagens Hermes e extraia eventos de log dele.

Configure uma conexão segura com o Serviço de envio de mensagens Hermes. Consulte Configurar uma conexão segura com o Serviço de envio de mensagens Hermes para obter mais informações. Você vai precisar desses certificados para autenticação e autorização no cliente que extrairá os logs do Hermes.

Nota: As funções de administrador ou Hermes_admin são necessárias para essa etapa.

3. Configure o produtor de log: escolha as origens de log para exportar e configurar os filtros. Realize as seguintes tarefas para configurar o produtor de log.

◦ Configure as origens de log para exportar: crie um registro de origem para cada uma das origens de log que você quer exportar.

Nota: As funções de administrador ou sn_logstoanalytics.admin são necessárias para concluir essa etapa

a. Clique em **Novo** no canto superior direito

b. Selecione um tipo de origem

c. Selecione os filtros adequados para o tipo de origem selecionado

Nota: Os filtros são diferentes dependendo do tipo de origem selecionado

d. Clique em "Atualizar"
Após a criação, será exibido o nome do tópico do Hermes para o qual a origem do log será exportada. Escreva o nome do tópico, porque você vai precisar dele para configurar o sistema do consumidor de log. O campo "Ativo" controla se a origem de log será exportada ou não. Caso encontre erros, volte para a tarefa "Verificar o Diagnóstico do Hermes" e confira o status dele.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Valide o produtor de log: depois de criar uma origem da qual produzir logs, é possível conferir os registros de log implementados no tópico usando o **Serviço de envio de mensagens Hermes** > **Inspetor de tópicos do Hermes**.
  a. Selecione "Tópicos externos"
  b. Clique em "Listar tópicos"
  c. Selecione a linha com o tópico da etapa anterior (listado em "Origens")
  d. Ajuste a data de início das mensagens, se necessário
  e. Clique em **Exibir** para conferir uma mensagem de log que foi exportada para o tópico

4. Instale o MID Server: instale e configure um MID Server dedicado que execute a versão Vancouver ou posterior.
   Instale o MID Server de acordo com as tarefas a seguir.
   - Instale o MID Server dedicado: o MID Server que o serviço de exportação de log usa deve ser dedicado somente para essa finalidade e não deve executar outros processos. Isso é importante para garantir a entrega oportuna de mensagens de log exportadas para o endpoint REST. Você pode instalar o novo MID Server usando a Use a a configuração assistida do MID Server ou instalando-o manualmente. Para a instalação manual, confira a documentação Configurar conectividade de rede do MID Server e, em seguida, a documentação Instalar o MID Server.
   - Valide o MID Server: valide manualmente o MID Server após instalar, para habilitá-lo a executar tarefas de automação. Para validar o MID Server dedicado ao LES, consulte Validar o MID Server

5. Configure o destino de push de REST do log: configure o MID Server para enviar logs ao sistema de análise de log (como o Splunk).
   Configure o destino de push de REST do log de acordo com as tarefas a seguir.
   - Adicione propriedades do MID: adicione propriedades do MID Server para que ele se conecte ao Hermes. Navegue até **MID Server** >**Propriedades** e defina os valores apropriados para cada propriedade listada abaixo.

Nome	Valor
mid.les.kafka.ssl.truststore.password	<password>
mid.les.kafka.ssl.keystore.password	<password>
mid.les.kafka.ssl.key.password	<password>
mid.les.kafka.ssl.truststore.location	<your_path>/<truststore>.p12
mid.les.kafka.ssl.keystore.location	<your_path>/<keystore>.p12
mid.les.kafka.ssl.truststore.type	PKCS12
mid.les.kafka.ssl.keystore.type	PKCS12
mid.les.kafka.client.id	<instance_name>
mid.les.kafka.group.id	snc.<instance_name> .group1
mid.les.kafka.bootstrap.servers	<instance_name>.servicenow.com:4100,<instance_name>
mid.les.kafka.set2.bootstrap.servers	<instance_name>.servicenow.com:4200,<instance_name>

Siga estas instruções para saber como obter alguns dos valores acima

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- <password> é a senha que você definiu para o armazenamento de chaves e o armazenamento confiável
- <your_path> é o caminho do arquivo para o diretório em que você baixou os arquivos de armazenamento de chaves e de armazenamento confiável. Os certificados precisam estar no servidor em que você está executando o MID
- <instance_name> é o nome da sua instância da ServiceNow. Se você estiver em dúvida, poderá encontrá-lo consultando a tabela sys_properties
- Você pode obter os valores de mid.les.kafka.bootstrap.servers e mid.les.kafka.set2.bootstrap.servers na Página de diagnóstico do Hermes. Navegue até **"Serviço de envio de mensagens Hermes"** > **"Diagnóstico"** e copie as strings em Consumer Bootstrap 1 (Inicialização do consumidor 1) e Consumer Bootstrap 2 (Inicialização do consumidor 2), respectivamente.

◦ Configure um destino: crie um novo registro de configuração de destino, que define o endpoint REST para o qual a extensão vai encaminhar os logs.

Nota: As funções de administrador ou sn_logstoanalytics.admin são necessárias para concluir essa etapa.

a. Navegue até **Serviço de exportação de log (LES)** > **Configurações de destino**

b. Crie um novo registro de configuração

c. Especifique o URL do endpoint pretendido para as origens de log exportadas

d. Pesquise ou crie novas credenciais para conectar ao endpoint. Ao criar credenciais para o endpoint, somente os seguintes tipos de credencial são válidos com o LES: autenticação básica, OAuth e chave de API

e. Pesquise ou crie um novo script de transformação. Enviamos com o script pré-escrito, **SplunkTransform** para Splunk

6. Configure o consumidor de log: configure a extensão do MID Server para o serviço de exportação de log de acordo com estas tarefas.

◦ Configure o contexto do consumidor LES: nesta etapa, você vai atualizar o registro do consumidor LES para executar no MID Server dedicado que você acabou de instalar para o serviço de exportação de log. Navegue até **MID server** > **Extensões** > **Contexto do consumidor LES** e configure os campos a seguir para atualizar o registro do consumidor LES:

- Clique em "Consumidor LES" para abrir o registro de contexto do MID Server
- Selecione o MID Server específico para o campo "Executar em"
- Insira o nome do MID validado na etapa anterior no campo "MID Server"

Clique em **Atualizar** para salvar.

Nota: Enviamos com um contexto pré-criado. Não crie um segundo contexto. Isso pode ter consequências indesejadas.

◦ Configure o consumidor: crie um novo registro de consumidor, que representa o processo que faz parte da extensão do MID Server para o serviço de exportar log. Navegue até **Serviço de exportação de log (LES)** > **Consumidores** e crie um novo registro de configuração especificando o tópico do Hermes para recuperar mensagens de log e o destino para retransmiti-las. Quando você seleciona o módulo **Consumidores**, ele mostra informações sobre o nome do consumidor e a configuração de destino.

a. Crie um novo registro de consumidor

b. Escolha um tópico de origem no menu suspenso

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

c. Escolha a configuração do destino

d. Inicie o consumidor

- Verifique a integração do MID Server: navegue até **Serviço de exportação de log (LES)** > **Status do consumidor** e exiba os campos "Status" e "Detalhes do status" do registro definido. As informações nesses campos relatam o estado atual do processo em execução no MID Server, incluindo quaisquer localizações de erros ao retransmitir mensagens ao endpoint REST. Essa é apenas uma página de exibição de status. Se você quiser criar um novo registro de consumidor, navegue até **Serviço de exportação de log (LES)** > **Consumidores**. Se o status do consumidor indicar o início do processo, você poderá inspecionar o endpoint para exibir os logs que foram retransmitidos para ele. Além disso, é possível exibir os logs no MID Server para ver se há detalhes adicionais sobre a localização de quaisquer erros. Você também pode habilitar o registro em log de depuração no MID Server para obter mais informações, se necessário.

> **Nota:** Se você fizer qualquer mudança em um dos registros do Consumidor, ela aparecerá na página de exibição "Status do consumidor". Se você selecionar o nome de registro de um consumidor na lista "Status do consumidor", será aberto o formulário "Consumidor" para o registro selecionado. Em seguida, será possível atualizar a configuração de nome e de destino do registro selecionado.

Como revisar o relatório de logs

Analise o tamanho de cada log de dados revisando o painel de relatórios de logs.

Antes de Iniciar

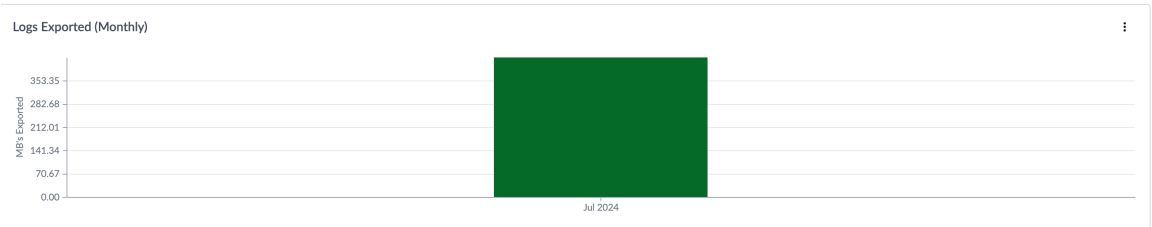
Função necessária: administrador ou sn_logstoanalytics.admin

Procedimento

1. Navegue até **Todos** > **Serviço de exportação de log** > **Relatórios**.

2. Revise os dados de log nos widgets abaixo.

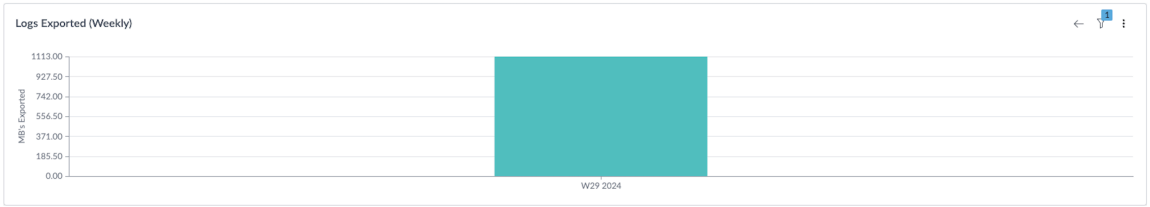
- Logs exportados (mensalmente): mostra os megabytes exportados por mês na exibição inicial. É possível analisar o gráfico mais detalhadamente para exibir os dados de cada semana ou os dados diários. Você pode exibir dados dos últimos 395 dias.



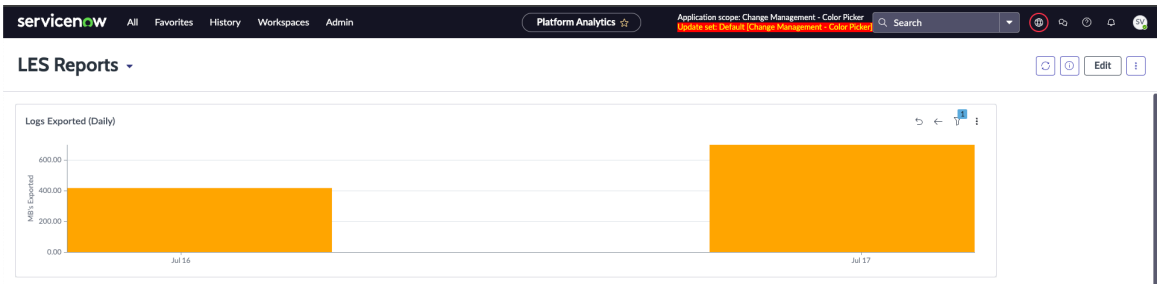
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Clique nas setas no canto superior direito do widget para analisar os dados em mais detalhes. Também é possível retornar aos dados primários.

Semanalmente:

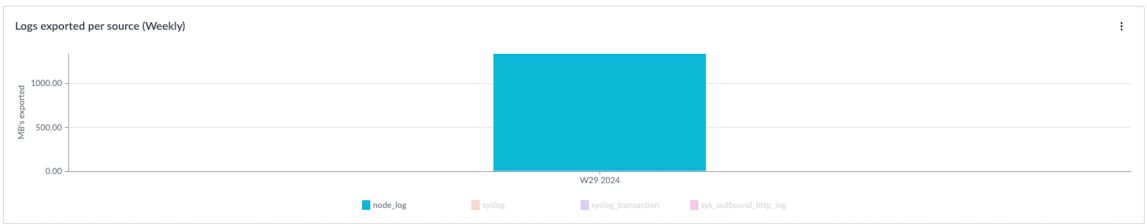


Diariamente:

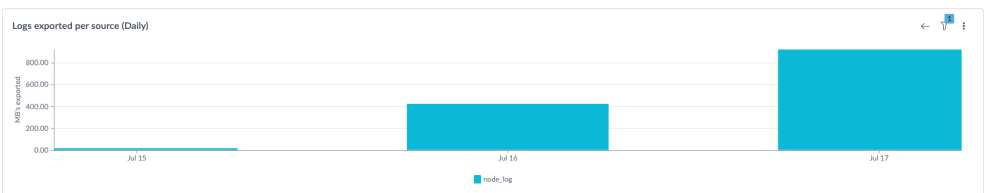


Os dados desse relatório refletem a coleta realizada quatro horas antes.

- Logs exportados por origem (semanalmente): esse widget mostra os tipos de logs que foram exportados semanalmente. Também é possível analisar em mais detalhes para ver os dados de log diários. Você pode exibir os dados dos últimos 32 dias.



Nota: É possível marcar ou desmarcar a origem da qual você deseja exibir os dados. As origens das quais é possível exibir os logs são: node_log, syslog, syslog_transaction e sys_outbound_http_log.

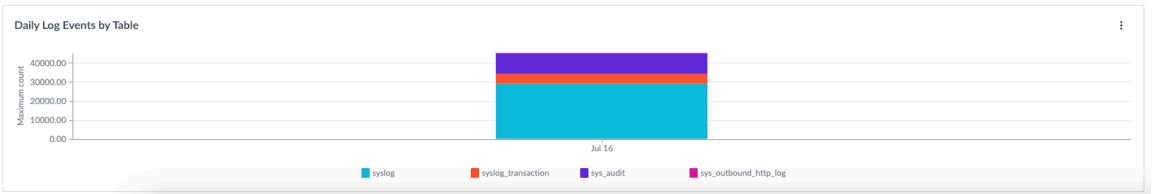


- Log exportado por origem (últimas 24 horas): mostra os dados das últimas 24 horas. O gráfico progride cronologicamente da esquerda para a direita em uma escala de 24 horas; os dados mais antigos (24ª hora) são posicionados à direita e, os dados mais recentes, no lado esquerdo do relatório. É possível marcar ou desmarcar a origem da qual você deseja exibir os dados. As origens das quais é possível exibir os logs são: node_log, syslog, syslog_transaction e sys_outbound_http_log.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Dependendo da hora do dia em que você verifica esses dados, o widget se atualiza dinamicamente para refletir exatamente as últimas 24 horas.

- Eventos de log diários por tabela: mostra os eventos de log gerados por cada tabela de log por dia. É possível marcar ou desmarcar as tabelas das quais você deseja exibir os dados.



Nota: As tabelas das quais é possível exibir os eventos de log são: syslog, syslog_transaction, sys_audit e sys_outbound_http_log.

Logs

O módulo de Logs fornece uma variedade de logs que você pode usar para solucionar problemas e depurar transações e eventos que ocorrem na instância.

Primeiros passos

Logs do sistema

O módulo Logs do Sistema fornece uma variedade de logs que você pode usar para solucionar problemas e depurar transações e eventos que ocorrem na instância.

Registro em log, auditoria e erros

Aplique uma estratégia de registro em log e auditoria para que você possa identificar e agir em atividades suspeitas em tempo hábil.

Logs do sistema

O módulo Logs do Sistema fornece uma variedade de logs que você pode usar para solucionar problemas e depurar transações e eventos que ocorrem na instância.

Acesse os seguintes logs no módulo Logs do Sistema:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Log	Descrição
Transações	Todas as atividades de aplicação de uma instância.
E-mail e envio por push	Todas as notificações por e-mail e mensagens por push enviadas de todas as instâncias do sistema.
Logs de eventos	Todos os eventos do sistema que ocorrem dentro do sistema.
Importar	Atividade de importação de dados na plataforma.
Mudanças na tabela	Mudanças feitas em todas as tabelas do sistema.
Registro em log de serviço web de saída	Todas as solicitações de serviços da Web de saída, como solicitações REST e SOAP.
Imagens da assinatura	Assinaturas eletrônicas para o bloco de assinaturas de RH.
Sistema	Avisos e erros de processos, registros e eventos não críticos de instância, como uso de memória na máquina do servidor.

Use o Navegador de arquivos de log para pesquisar e baixar logs. Você também pode pesquisar logs arquivados no histórico de logs.

Outros logs

Sua instância oferece outros logs além daqueles no módulo Logs do sistema. Por exemplo, o Módulo Diagnóstico do sistema fornece histórico de upgrade e logs de consulta lenta, que você pode usar para obter informações sobre como as consultas estão afetando o desempenho da plataforma. O Tabela de atualizações do cliente registra todas as mudanças feitas no sistema.

Log do Sistema

Exiba avisos e erros de processos, registros e eventos não críticos de instância, como uso de memória na máquina do servidor.

As informações a seguir são rastreadas no log do sistema:

- Fluxos de trabalho
- Configuração
- Sessões de bate-papo
- Transações para cada exibição de cada página no sistema, incluindo tempos de carregamento para rede, servidor e navegador
- E-mail de entrada e saída
- Eventos acionados no sistema
- Importações e integrações
- Avisos do sistema, erros e logs de script
- Informações de atualização para ativações de plug-in, conjuntos de atualizações ou upgrades do sistema

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

As entradas de log aparecem somente para o dia atual. Para exibir outros arquivos de log, use o navegador de arquivos de log. Este log fornece as seguintes informações para todas as ocorrências:

Log do sistema

Campo	Descrição
Criado	Data e hora da atividade de registro em log para a localidade da máquina que executa a instância.
Nível	Tipo de mensagem. Os níveis são Depuração, Erro, Aviso e Informações. • Um aviso é um erro que foi tratado e recuperado. • Um erro é algo que deve ser corrigido.
Mensagem	Mensagem gerada pelo sistema sobre a natureza da ocorrência.
Fonte	Nome do processo ou área afetada pela ocorrência. Por exemplo, a origem da ocorrência pode ser E-MAIL ou Memória.
Pacote de origem	Nome do pacote de aplicações associado à ocorrência. Clique no nome para exibir o registro do Aplicativo da store [sys_store_app] para este pacote.

Registro em log de fluxo de trabalho

- Cada atividade executada, incluindo:
  - Data e hora de início
  - Data e hora de fim
  - Estado, por exemplo, Concluído, Cancelado, Tempo esgotado, Erro
  - Resultado
  - Descrição da falha, se houve um erro
- Histórico de transição, incluindo:
  - Tempo de transição
  - Transição de atividade de
  - Transição de atividade para
  - Qual transição foi acionada
- Log de fluxo de trabalho, incluindo quaisquer declarações de log adicionadas ao fluxo de trabalho

Informações de configuração

- Ação realizada, incluindo inserir, atualizar e excluir
- Categoria de mudança
- Comentários registrados com a mudança
- Nome da mudança
- Diferença XML da mudança
- Conjunto de atualizações ao qual a mudança está associada

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Data e hora da mudança
- Usuário que fez a mudança
- Tabela onde a mudança foi feita
- Nome do objeto que está sendo alterado
- Tipo do objeto que está sendo alterado
- Exibir a mudança feita em, para mudanças em formulários ou listas

Logs de transações

O registro em log de transações registra todas as atividades do navegador para uma instância. Para ajudar na depuração de problemas do sistema, você pode filtrar os logs de transações por escopo da aplicação, limitando as transações que aparecem somente às transações originadas em escopos específicos.

O registro em log de transações fornece as seguintes informações para todas as atividades.

Campo	Descrição
Criado	Data e hora da ação da aplicação para a localidade da máquina que executa a instância.
Tipo	Tipo de transação registrada.
Criado por	Usuário que criou esta atividade.
Aplicação de origem	Escopo da aplicação no qual a transação foi originada. Global será exibido se a transação tiver sido originada no escopo global.
Tempo de resposta	Tempo de resposta de ida e volta para a solicitação da aplicação, em milissegundos.
Tempo da rede	Tempo de latência da resposta da rede após a solicitação da aplicação, em milissegundos.
Comprimento da saída	Tamanho da cadeia de caracteres de saída enviada pela instância à aplicação, em bytes.
Contagem SQL	Número de comandos do SQL Server executados para esta atividade.
Contagem de regra de negócio	Número de regras de negócio executadas para esta atividade.
Tempo de regra do negócio	Tempo decorrido para a execução das regras de negócios para esta atividade.
URL	Aplicação ou módulo conectado pela aplicação do cliente.
ID do sistema	Identificador gerado pelo sistema da instância do cliente que está fazendo a solicitação. Este ID é usado para ambientes de cluster nos quais várias instâncias (nós) se comunicam com o banco de dados.
Endereço IP	Endereço IP do cliente que está fazendo a solicitação.
Compactados em G	Indicação se uma página da Web compactada foi solicitada pela aplicação.
Protocolo	Protocolo HTTP usado pela aplicação para esta instância.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Client transaction timings

O plug-in Client Transaction Timings aprimora os logs do sistema, fornecendo informações adicionais sobre as durações das transações que ocorrem entre o cliente e o servidor.

Você pode rastrear problemas de desempenho até a origem exibindo onde o tempo está sendo consumido e como o tempo foi gasto durante uma transação.

Este plug-in requer que o Indicador de tempo de resposta Indicador de tempo de resposta esteja habilitado e coleta informações dos seguintes navegadores:

- Firefox
- Internet Explorer
- Chrome

Informação de Transações do cliente

A instalação do plug-in adiciona o módulo *Transações do cliente* à aplicação *Logs do sistema*. Ele fornece uma lista de todas as transações registradas entre o cliente e o servidor no último dia:

Informação de Transações do cliente

Campo	Descrição
Criado	Momento em que a transação foi registrada.
Tempo de resposta	Número de ms gastos pelo servidor na execução da transação.
Tempo de regras de negócios	Número de ms gastos por regras de negócios acionadas pela transação.
Tempo do SQL	Número de ms gastos pelo banco de dados SQL.
Tempo de resposta do cliente	(Load_completion_time) - (start_time). Inclui a hora do servidor.
Tempo de rede do cliente	Número de ms gastos pela rede pela qual o cliente está se conectando.
Tempo do navegador	Número de ms gastos pelo navegador na execução da transação.
Tempo do client script	O número de ms gastos na execução de scripts de cliente.
Tempo da Política de IU	Número de ms gastos na execução da política de IU.
Tipo	Tipo de transação: • Formulário • Lista • Outro
Tabela	Nome da tabela exibida. Por exemplo, incident, change_request.
Exibição	Exibir para este formulário/lista.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Informações detalhadas do cliente

Um maior detalhamento dos tempos do cliente para toda a renderização de Formulário (mas não a renderização de lista) também é rastreado. Para ver os detalhes, analise um registro de transação de cliente específico e observe a lista relacionada na base da tela.

Informações detalhadas do cliente

Campo	Descrição
Ordem	Ordem durante o carregamento em que esta operação ocorreu.
Tipo	Tipo de operação.
Nome	Nome descritivo desta operação específica
Duração	Número de ms que esta operação levou para ser concluída.

Logs de push

Consulte o registro em log de push para rastrear o status das notificações por push que estão na fila para enviar do seu sistema.

Para exibir o registro em log de push, navegue até **Logs do sistema** > **Notificações por push**. Os usuários devem ter a função push_admin ou admin para exibir o registro em log de push.

Campos de log de push

Campo	Descrição
Reivindicar	Número de identificação gerado pelo trabalho agendado que envia a notificação por push. Este número é aplicado ao campo **Reivindicar** para garantir consistência em vários trabalhos agendados por push.
Carga	Conteúdo da notificação por push.
Contagem de fila	Número de vezes que o sistema tentou enviar a notificação por push. O status da notificação por push está relacionado à contagem da fila. • Se a contagem da fila for 0 por mais tempo do que o esperado, não há trabalhos agendados que tentarão enviar a notificação por push. • Se a contagem da fila for maior que 0 e o **Tipo** for **bem-sucedido**, você poderá inferir que este é o número de vezes que o sistema tentou enviar a notificação por push antes de finalmente a enviar. • Se a contagem da fila atingir 10, o sistema deixará de tentar enviar a notificação por push. O **Tipo** muda para **falha**.
ID de Solicitação	Número de identificação exclusivo para a notificação por push. Semelhante ao ID da mensagem de um e-mail, o ID da solicitação é usado como um token de correlação para a notificação por push.
Tipo	Status para indicar se a notificação por push foi enviada. A coluna Tipo pode ter estes valores:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campos de log de push

Campo	Descrição
	• **falha**: a mensagem não pôde ser enviada. • **pendente**: a mensagem está na fila para processamento. • **sucesso**: a mensagem foi enviada com sucesso, embora não tenha necessariamente sido recebida pelo dispositivo móvel.

Informações relacionadas

Trabalhos agendados

Logs de e-mail e caixas de correio do sistema

O registro em log de e-mail do sistema registra todos os e-mails que a instância cria ou recebe. As caixas de correio do sistema são exibições filtradas deste log.

Cada e-mail de notificação que a instância cria ou recebe é registrado em um registro de E-mail [sys_email]. Você pode navegar até um log desses registros em **Logs do sistema** > **E-mails**.

As caixas de correio do sistema são exibições filtradas da tabela de e-mails [sys_email]. A instância atribui um registro de e-mail a uma caixa de correio do sistema, dependendo dos valores dos campos **Tipo** e **Estado**. Para obter mais informações, consulte Caixas de correio do sistema.

Os seguintes campos podem ser incluídos no layout do log do sistema e em qualquer uma das caixas de correio do sistema:

Log de e-mail

Campo	Descrição
Caixa de correio	A caixa de correio do sistema que lista este registro de e-mail. A instância define o valor deste campo de acordo com os valores dos campos **Tipo** e **Estado**.
Estado	O estado atual do e-mail (Erro, Ignorado, Processado ou Pronto).
Tipo de recebimento	O tipo de e-mail de entrada (Nenhum, Encaminhar, Novo ou Resposta).
Tipo	O status do e-mail As opções são: • recebido: o servidor recebeu este e-mail. • recebido – ignorado: o servidor recebeu este e-mail, mas ele foi ignorado pela instância para fins de ação de e-mail de entrada. Normalmente, esses e-mails são spam ou respostas automáticas. Consulte o campo Cadeia de caracteres de erro para obter detalhes. • envio – falha: o servidor tentou enviar o e-mail e falhou. Consulte o campo Cadeia de caracteres de erro para obter detalhes. • envio – ignorado: o servidor ignorou o envio deste e-mail. Normalmente, isso é para um e-mail que foi gerado, mas não tinha um endereço de e-mail do destinatário ou é um e-mail duplicado. Consulte o campo Cadeia de caracteres de erro para obter detalhes.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Log de e-mail

Campo	Descrição
	• envio – pronto: o e-mail está pronto para ser enviado, mas não foi enviado pelo servidor de e-mail. Normalmente, um e-mail permanece neste estado por apenas um curto período de tempo. • envio - tradução - pronto: o e-mail é gerado durante a tradução de e-mail e enviado. Normalmente, um e-mail permanece neste estado por apenas um curto período de tempo. • enviado: o e-mail foi enviado pela instância sem erros ou problemas.
Destino	Uma referência de ID de documento para o registro se o e-mail for gerado por uma inserção, atualização ou exclusão de um registro específico.
Usuário	O nome do usuário, do registro do usuário, da instância da qual a notificação por e-mail foi enviada. **Nota:** Este é um campo de cadeia de caracteres.
Tipo de notificação	O tipo de notificação As opções são: • Nenhum • SMS • SMTP
UID	O ID exclusivo do e-mail armazenado no servidor.
Criado	Data e hora da atividade de e-mail para a localidade da máquina que executa a instância.
Excluídos	Para e-mail de entrada, indica se o e-mail foi excluído do servidor de e-mail.
Ponderação	O peso do e-mail, que determina a prioridade de envio em relação a outras notificações na mesma tabela.
Importância	Uma indicação de que o e-mail foi enviado com um nível de importância alterado, como Urgente.
Evento e Notificação de Origem	Para e-mails gerados por notificações, uma lista incorporada que armazena o evento e a notificação que criou o e-mail.
Assunto	O assunto do e-mail Para notificações, você cria o texto do assunto em **Notificação do sistema** > **E-mail** > **Notificações**.
Cadeia de caracteres de erro	A cadeia de caracteres de erro capturada do servidor de e-mail para determinar por que o e-mail não foi enviado. Isso é registrado somente se o e-mail falhar.
Destinatários	Os endereços de e-mail dos destinatários.
Corpo	O corpo do e-mail, exibido na marcação HTML bruta. Use o link relacionado Visualizar corpo do HTML para ver o texto do corpo como HTML renderizado.
Tipo de conteúdo	O tipo de conteúdo de e-mail.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Log de e-mail

Campo	Descrição
Cabeçalhos	Todos os cabeçalhos incorporados ao e-mail.

Logs de eventos

O registro em log de eventos registra todos os eventos do sistema que ocorrem na Now Platform.

Este log fornece as seguintes informações para todos os eventos que ocorrem:

Log de eventos

Campo	Descrição
Criado	Data e hora do evento para a localidade da máquina que executa a instância.
Nome	Nome do evento conforme listado no Registro de eventos.
URI (Identificador uniforme de recursos)	Consulta HTTP que gerou o evento.
Parm1	Valor específico do evento que depende do evento e do destinatário.
Parm2	Valor específico do evento que depende do evento e do destinatário.
Tabela	Tabela de banco de dados usada para este evento.
Processado	Data e hora em que o processamento do evento começou. Essa hora reflete o local da máquina que executa a instância.
Tempo de processamento	Tempo necessário para processar este evento, em milissegundos.
Fila	Nome da fila do processador

Logs de importação

O registro em log de importação exibe informações em formato detalhado sobre qualquer atividade de importação de dados na plataforma.

Para obter uma exibição mais detalhada dos conjuntos para importação que produziram um log específico, consulte **Conjuntos para importação** > **Histórico de transformações**.

Este log fornece as seguintes informações para todas as importações:

Log de Importação

Campo	Descrição
Criado	Data e hora da importação para a localidade da máquina que executa a instância.
Nível	Tipo de mensagem exibida. Para arquivos de importação, o nível é Informações.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Log de Importação

Campo	Descrição
Mensagem	Mensagem gerada pelo sistema sobre o status da importação.
Fonte	Nome da origem externa da importação, como uma integração.

Módulo Diagnóstico do sistema

A aplicação Diagnóstico do sistema fornece logs relacionados à plataforma.

Estes logs estão disponíveis:

Histórico de upgrades

Rastreia cada upgrade para uma instância.

Consultas lentas

Fornece informações sobre como as consultas afetam o desempenho da plataforma. Consulte Usar um log de consulta lenta.

Tabela de atualizações do cliente

As mudanças feitas no sistema são registradas na tabela Atualizações do cliente `[sys_update_xml]` em ordem cronológica. Existem algumas exceções, conforme observado abaixo.

Para navegar até esta tabela, insira `sys_update_xml.list` no filtro de navegação. Para obter informações sobre conjuntos de atualizações, consulte Conjuntos de atualizações do sistema.

As seguintes informações são armazenadas sobre cada atualização:

Tabela de atualizações do cliente

Campo	Descrição
Nome	Um nome que identifica o registro atualizado.
Criado	A data e a hora em que o registro de Atualização do cliente foi criado.
Criado Por	O usuário que realizou a mudança.
Tipo	O tipo de atualização.
Atualizado	A data e a hora em que o registro de Atualização do cliente foi atualizado.
Atualizada Por	O usuário que realizou a atualização.
Atualizações	O número de vezes que o registro foi atualizado.
Nome de destino	O nome do elemento que foi alterado.
Exibição	A exibição do formulário que foi alterada se fosse uma mudança de layout do formulário.
Carga	O conteúdo XML do registro após a mudança.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela de atualizações do cliente

Campo	Descrição
Conjunto de atualizações remoto	Uma referência a esse conjunto de atualizações se a mudança foi realizada por um conjunto de atualizações remoto.
Conjunto de atualizações local	O conjunto de atualizações com o qual a mudança está associada.

Nota: Algumas mudanças de aplicação não são representadas por registros de Atualização do cliente (sys_update_xml) Exemplos:

- Tipos de metadados em que updateSynch = falso
- Mudanças em cascata em tabelas e campos, como mudanças de nome de exibição
- Referências de metadados não resolvidas de outras aplicações (resultando em nenhum "valor de exibição" no elemento)
- Mudanças de sys_id para arquivos de aglutinação
- Mudanças nas ações de fluxo/fluxo que podem gerar sys_documentation
- Registros ua_table_license_config gerados na criação da tabela
- Trabalhos em execução em segundo plano, como processamento de linguagem natural
- Casos em que sys_update_xml é modificado ou removido manualmente

Para saber mais, consulte Confirmar mudanças.

Histórico do log

O sistema usa rotação e extensão de tabela para arquivar logs mais antigos.

Por padrão, o sistema usa a seguinte programação para arquivar logs comuns:

Programação de arquivamento de log comum

Tabela	Programação de arquivamento	Rotações	Tipo
Evento [ecc_event]	Todos os dias	7	Rotação
Fila [ecc_queue]	Todos os dias	7	Rotação
Evento [sysevent]	Todos os dias	7	Rotação
Log [syslog]	Todas as semanas	8	Rotação
Log de transações [syslog_transaction]	Todas as semanas	8	Rotação
E-mail [sys_email]	A cada 30 dias	8	Extensão

Usar o navegador de arquivos de log

A instância fornece o navegador de arquivos de log de utilitários e o download do arquivo de log.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Use **Logs do sistema** > **Utilitários** > **Navegador de arquivos de log de nó** para exibir qualquer entrada de log do sistema. Você pode pesquisar arquivos de log usando os seguintes filtros:

Navegador de arquivos de log

Campo	Descrição
Hora de início	Data e hora iniciais do intervalo que você quer pesquisar para a localidade da máquina que executa a instância.
ID da Sessão	Cadeia de caracteres hexadecimal gerada pelo sistema que identifica a sessão que gerou a entrada de log.
Hora de término	Data e hora finais do intervalo que você quer pesquisar para a localidade da máquina que executa a instância.
Mensagem	Descrição da ocorrência gerada pelo sistema.
Nível	Tipo de mensagem exibida. Os níveis são Depuração, Erro, Aviso e Informações. Um aviso é um erro que foi tratado e recuperado. Um erro é algo que deve ser corrigido.
Nome do thread	Identificador gerado pelo sistema do thread que criou o arquivo de log.
Máximo de linhas	Número máximo de registros retornados para um filtro específico.

A instância cria arquivos compactados de logs do sistema a cada dois dias e limpa os arquivos de log após 21 dias.

Importante: Quando um nó é descontinuado, os arquivos de log do nó são limpos imediatamente, o que significa que eles não são arquivados por mais 21 dias.

Você pode baixar arquivos de log e exibi-los com **Logs do sistema** > **Utilitários** > **Download do arquivo de log do nó**. Selecione um arquivo de log na lista e clique em **Fazer download do log** em *Links relacionados* para abrir ou salvar o arquivo.

Nota: Os arquivos de log estão disponíveis somente para o nó ao qual você está conectado. Para ver o nó conectado no momento, navegue até **Diagnóstico do sistema** > **Estatísticas**.

Use o novo botão **Mostrar logs do sistema** nos formulários Transação e Transação ativa para exibir todas as entradas de log do sistema que foram geradas durante a execução da transação. Uma transação pode ter qualquer número de entradas de log do sistema. As várias entradas de log do sistema para todas as transações dificultam correlacionar uma transação com suas respectivas entradas. A ação de IU **Mostrar registros de log do sistema** ajuda a correlacionar as transações ativas e concluídas com as respectivas entradas, criando um URL para consultar a tabela de logs de sistema. Identificar as entradas corretas do log do sistema para uma transação específica ajuda a depurar e resolver problemas de segurança.

Segurança de registro em log aprimorada

Explore o campo **Atribuição** nas linhas de logs de nó para identificar o script ou o componente que gerou a mensagem de log. As linhas de início da transação incluem o novo campo para identificar o tipo de solicitação feita.

Alcance o seguinte usando as novas melhorias:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Rastreie o originador de origem de cada uma das linhas de log
- Caso as informações do originador não estejam disponíveis, imprima o nome da classe Java e uma atribuição
- No início de cada linha de transação, contém o ID e o tipo de transação

Use o ID da transação de cada linha de log para entender as informações fornecidas em cada linha de log. Depois de identificar o tipo de transação, você obterá as informações do originador de cada linha de log. O tipo de transação e as informações do originador de cada linha de log fornecem as informações de origem necessárias de cada linha de log do nó.

Nota: Os tipos de script SYS_UI_MACRO e SERVICE_PORTAL_WIDGET na atribuição não são relatados.

Tipos de transação

A seguir está a lista de tipos de transação:

- Lista
- Formulário
- XMLHttp
- Relatório
- SOAP
- Exportar
- Scheduler
- Pesquisa de texto
- Outro
- REST
- JSON
- AMB
- Arquivamento
- Lote REST
- Instance Scan

Propriedades do sistema

Estas são as propriedades do sistema necessárias para o recurso:

- Glide.log.append.attribution: esta propriedade está habilitada por padrão. Ativa/desativa as informações de atribuição de cada linha de nó
- Glide.db.log.append.classname.attribution: esta propriedade está habilitada por padrão. Ativa/desativa o registro em log da atribuição de nome de classe Java

Evitar adulteração de log

Configure as regras de proteção da tabela de log do sistema para limitar o escopo de modificação e exclusão de registros de log da aplicação. As regras permitem que você determine o registro em log de mudanças ou tentativas de mudanças nessas tabelas.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Se você for um security_admin, ative o plug-in Tabelas protegidas (com.glide.protected_tables) que permite que a plataforma restrinja as operações de atualização, inserção e exclusão nas seguintes tabelas de log do sistema:

- syslog
- syslog_transaction
- sys_outbound_http_log
- sysevent
- sys_audit
- sys_push_notification
- syslog_app_scope
- protected_table_configuration (configuração não modificável)

Nota: O plug-in com.glide.protected_tables oferece proteção somente às tabelas de log do sistema mencionadas acima. Qualquer tentativa de atualizar, inserir ou excluir um registro registra uma mensagem na tabela protected_table_log.

Consulte Instalar e configurar o plug-in Log Protection para obter mais detalhes.

Você pode especificar um dos seguintes níveis do Log Protection para cada tabela de log do sistema.

- Bloquear e registrar a tentativa: bloqueia qualquer modificação e registra a tentativa
- Somente bloquear a tentativa: bloqueia qualquer modificação e não registra a tentativa
- Somente registrar a tentativa: não bloqueia qualquer modificação, mas registra a tentativa
- Não bloquear e não registrar a tentativa: não bloqueia a modificação e nem registra a tentativa

A plataforma usa os níveis do Log Protection especificados para cada uma das tabelas de log do sistema para bloquear e/ou registrar em log qualquer tentativa de modificar um registro após sua criação inicial.

Nota: Se você for um security_admin, poderá substituir os níveis do Log Protection padrão em cada uma das tabelas de log do sistema para se adaptar às personalizações em sua instância.

Se houver tentativas de modificar as tabelas de log do sistema, elas serão conectadas à tabela protected_table_log.

Nota: Se o nível de proteção não for especificado para uma tabela, as tentativas de modificação não serão registradas na tabela protected_table_log.

Para desabilitar as operações de plug-in em tabelas no Painel do administrador, defina a propriedade com.glide.security.protected_table.enabled como falsa. Consulte Criar propriedade do Log Protection para obter mais informações.

Configurar o plug-in Log Protection

Configure as regras de proteção para cada tabela e operação para concluir a configuração do plug-in Log Protection.

Antes de Iniciar
Função necessária: security_admin

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegue até **Todos** > **Tabelas protegidas** > **Proteção de registro em log**.
   A página do Painel do administrador é exibida.

   Nota: Iniciado na versão Utah, o plug-in Tabelas protegidas é instalado por padrão, mas desabilitado.

2. Eleve sua função para security_admin para continuar configurando o plug-in.

   a. Selecione **Administrador do sistema**.

   b. Selecione **Elevar função**.
   O modal Elevar função é exibido.

   c. Selecione a opção security_admin para elevar sua função e selecione **Atualizar**.

3. Configure as regras de proteção para cada tabela e operação. As regras de proteção se aplicam para atualizar, inserir e excluir. Os níveis de proteção não podem ser alterados para algumas tabelas. As tabelas syslog e syslog_app_scope têm valores fixos para proteções de atualização e exclusão. A tabela Protected_table_configuration fixou valores de proteção para todas as três operações.

   Nota: Para a tabela sysevent, as proteções de inserção não podem ser definidas como bloqueadas.

   Se a opção **Aplicar a tabelas secundárias** estiver ativada para o syslog na versão anterior, as tabelas secundárias serão adicionadas ao Log Protection com as mesmas regras de proteção do syslog no upgrade para a versão Utah. Isso só acontece com o syslog, e não com outras tabelas.

4. Habilite o recurso selecionando a alternância **Habilitar Log Protection**.

   Nota: Você pode desabilitar este plug-in somente alterando a propriedade com.glide.security.protected_table.enabled na tabela sys_properties.

Criar propriedade do Log Protection

Crie uma propriedade do Log Protection para evitar o risco de adulteração de log.

Antes de Iniciar
Função necessária: administrador

Procedimento

1. Se a propriedade *com.glide.security.protected_table.enabled* não existir na lista Propriedades do sistema, selecione **Novo**.
   O novo formulário de propriedade do sistema é exibido.
2. No formulário, preencha os detalhes

Campos	Descrição
Nome	Nome da propriedade como com.glide.security.protected_table.enabled

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campos	Descrição
Aplicação	A aplicação que tem a propriedade.
Descrição	Descrição da propriedade
Escolhas	
Tipo	Tipo de valor - verdadeiro ou falso
Valor	Valor real da propriedade
Ignorar cache	Opção para ignorar o conteúdo do cache
Privado	Opção para tornar a propriedade privada ◦ Funções de leitura ◦ Funções de gravação

3. Selecione **Enviar** para criar a propriedade.

Registro em log, auditoria e erros (proteção de segurança da instância)

Aplique uma estratégia de registro em log e auditoria para que você possa identificar e agir em atividades suspeitas em tempo hábil.

Para saber mais sobre o que pode ser registrado na instância, consulte Logs do sistema. Certifique-se de que haja uma programação para monitorar eventos do sistema, como logins e logins com falha usando **Logs do sistema** > **Eventos**.

Desabilitar mensagens de erro de SQL (proteção de segurança da instância)

Utilize a propriedade *glide.db.loguser* para desabilitar a renderização de mensagens de erro de SQL em um navegador.

Mais informações

Atributo	Descrição
Nome da propriedade	glide.db.loguser
Tipo de configuração	Propriedades do sistema (/sys_properties_list.do)
Configurável na Central de segurança da instância	Não
Finalidade	Desabilitar a exibição de mensagens de erro de SQL no navegador.
Tipo	verdadeiro | falso
Valor recomendado	falso
Impacto funcional	(Baixo) Esta correção desabilita a renderização de mensagens de erro de SQL. Não há impacto em nenhuma funcionalidade.
Risco à segurança	(Médio) Nenhuma informação confidencial do SQL que possa ajudar um invasor deve aparecer como

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo	Descrição
	parte de uma mensagem de erro em uma página da Web.

Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

Gestão de segredos

Use a Gestão de segredos da ServiceNow para gerenciamento granular de acesso às suas senhas para atender às suas necessidades de negócio.

Explorar

Conheça os principais recursos e o valor comercial da Gestão de segredos.

Analisar

Aprenda mais sobre o Painel da gestão de segredos

Configurar

Planeje suas configurações principais.

Explorando a Gestão de segredos

Use a Gestão de segredos da ServiceNow para gerenciamento granular de acesso às suas senhas para atender às suas necessidades de negócio.

Importante: Os administradores devem ter a função de ver módulos e registros relacionados à Gestão de segredos. Para obter informações sobre a função de gestão de segredos, consulte Funções de gestão de segredos.

Selecione a partir das versões Core e Enterprise da Gestão de segredos

Escolha entre a Gestão de segredos Core e a Gestão de segredos Enterprise, dependendo das necessidades do seu negócio.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Gestão de segredos Core	Gestão de segredos Enterprise
A Gestão de segredos Core está disponível para ativação na instância sem custo adicional. Com o plug-in, é possível usar grupos de segredos com critérios em tabelas não personalizadas fornecidas na plataforma ServiceNow que foram criadas pelas equipes de engenharia de aplicações da ServiceNow.	A Gestão de segredos Enterprise inclui funções adicionais para ajudar os administradores a criar e gerenciar grupos de segredos. O Enterprise fornece os seguintes recursos, além daqueles listados no Core. • Use controles de acesso granulares para criar grupos de segredos com base em qualquer um desses critérios. ◦ Escopo ◦ Tabela ◦ Coluna ◦ Registro • Crie segredos acessíveis ao cliente, que são criptografados com sua própria chave, mas que a ServiceNow não pode acessar. • Use o painel da Gestão de segredos para revisar os grupos de segredos configurados em sua instância e aprender sobre possíveis problemas de segurança. **Nota:** A Gestão de segredos Enterprise é um plug-in pago que a equipe da ServiceNow deve ativar em sua instância de produção.

Use grupos secretos para organizar seus segredos

Use a Gestão de segredos para organizar seus segredos em grupos e aplique políticas de acesso a esses segredos no nível de grupo.

Grupo secreto básico

Esses grupos se aplicam a todos os segredos em um escopo. Esses segredos são descriptografados por um módulo criptográfico comum e políticas de acesso ao módulo.

Grupo secreto com critérios

Grupos secretos com critérios funcionam da mesma forma que um grupo secreto básico, mas refinam ainda mais o que está incluído usando critérios. Esses critérios incluem:

- Escopo da aplicação
- Pacote
- Tabela
- Coluna secreta
- Registro de filtro

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Grupos secretos de qualquer tipo podem se tornar acessíveis à instância ou ao cliente.

Grupos secretos do lado da instância

Os grupos secretos do lado da instância contêm segredos que podem ser descriptografados pela sua instância.

Grupos secretos do lado do cliente

Os grupos de segredos do lado do cliente usam um par de chaves pública e privada para que somente o cliente possa descriptografar os segredos. Ao criar um grupo de segredos acessível ao cliente, você carrega a chave pública na instância e mantém a chave privada no MID Server. A instância usa a chave pública para criptografar seus segredos, mas eles só podem ser descriptografados usando a chave privada.

Nota: Para obter mais informações sobre esses tipos de grupo, consulte Aprender sobre a Gestão de segredos do lado do cliente.

Usar grupos de segredos para um controle mais granular

Embora a password2 esteja disponível na plataforma da ServiceNow, a Gestão de segredos fornece esses recursos adicionais.

Controles de acesso granulares	Password2 Com password2, os administradores podem controlar o acesso a um escopo da aplicação, mas não podem restringir o acesso aos elementos dentro do escopo. Gestão de segredos Com a Gestão de segredos, os administradores podem restringir o acesso com base nos critérios que definem. Os tipos de critérios podem ser baseados em critérios como pacote, tabela ou coluna.
Armazenamento seguro	Para grupos secretos do lado do cliente, a Gestão de segredos usa um novo esquema de criptografia. Neste esquema de criptografia, a ServiceNow não salva a chave de criptografia. Por este motivo, a segurança dos seus dados não depende da segurança da ServiceNow.

Aplicar políticas de acesso ao módulo aos seus grupos

Depois de agrupar seus segredos em um grupo secreto, você pode aplicar políticas que determinam como os usuários podem acessar esses segredos em um nível de grupo. As políticas de acesso ao módulo são os mecanismos de controle de acesso que você aplica aos módulos criptográficos para definir controles no nível de instância, como um intervalo de tempo de validade para a chave criptográfica. Para obter mais informações sobre políticas de acesso ao módulo, consulte Visão geral da política de acesso ao módulo.

Tabelas instaladas com a Gestão de segredos

A Gestão de segredos adiciona ou modifica essas tabelas.

Novas tabelas	
[sn_sm_secret_group]	Armazena grupos secretos

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países. Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

[sn_sm_secret_group_criteria]	Armazena grupos secretos de critérios
[sn_sm_secret]	Armazena segredos encapsulados
[sn_sm_identity_group]	Define o grupo de identidades para mapeamento de um grupo de identidades para a chave pública
[sys_kmf_wrapped_module_key]	Armazena as chaves criptográficas simétricas encapsuladas
Tabelas modificadas	
[sys_kmf_crypto_module]	Tipo de módulo criptográfico adicionado. (Módulo criptográfico de identidade ou módulo criptográfico de grupo secreto)
[sys_kmf_module_key]	• Armazena a chave de criptografia secreta conceitual (sem material de chave) • Armazena a chave pública da identidade
[sys_kmf_crypto_caller_policy]	Novo tipo de política de acesso ao módulo adicionado

Exemplos de casos de uso da Gestão de segredos

Garantia de uma Descoberta do ITOM segura

Este infográfico mostra uma arquitetura de referência simplificada de como sua organização pode implantar a Descoberta do ITOM (IT Operations Management) da ServiceNow. Como mostra o infográfico, vários servidores Windows e Linux se conectam ao MID Server, e vários agentes do MID Server permitem que o processo de descoberta atualize o CMDB. Todas as transações do MID Server exigem uma autenticação segura; portanto, gerenciar as credenciais de autenticação é essencial de um ponto de vista de segurança.

Como acelerar com segurança a conectividade de fluxos de trabalho ao Integration Hub

Use o Integration Hub da ServiceNow para se conectar a diferentes sistemas usando APIs (Application Programming Interfaces, interfaces de programação de aplicações) automatizadas. Sempre que o Integration Hub se conecta a um sistema usando uma API, é necessário informar uma credencial de autenticação para estabelecer conectividade. A gestão de uma infinidade de aplicações e APIs de conectividade requer uma solução de gestão de segredos.

A Gestão de segredos é uma peça fundamental para garantir a segurança cibernética da sua organização. Ela abrange todos os processos e ferramentas relacionados à criação, ao armazenamento, à transmissão e à gestão de credenciais digitais, como chaves de criptografia, tokens de API e senhas. Para gerenciar segredos com segurança e eficácia, é possível criar uma política principal de gestão de segredos que estabeleça regras e procedimentos padrão para todas as fases do ciclo de vida de um segredo.

Aprender sobre a Gestão de segredos do lado do cliente

Saiba como usar a Gestão de segredos para gerenciar o acesso a segredos e grupos.

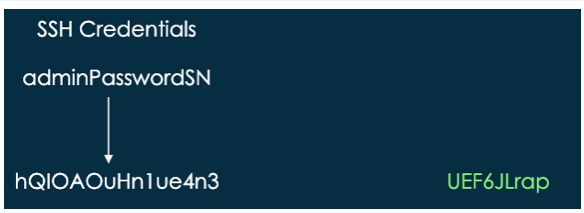
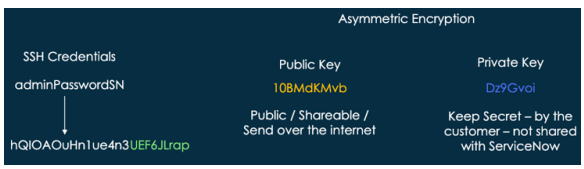
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Terminologia

A gestão de segredos do lado do cliente foi projetada para fornecer um método de gestão de segredos sem o uso de proxies e sem conceder acesso da ServiceNow aos dados descriptografados. Para entender este processo, comece com os termos de criptografia a seguir.

Termo	Descrição
Criptografia simétrica	A criptografia simétrica usa uma única chave para criptografar e descriptografar dados. Se os dados estiverem criptografados com uma chave simétrica, essa chave será suficiente para descriptografá-los.
Chave simétrica	A chave simétrica criptografa um segredo, transformando sua senha de texto não criptografado em texto cifrado ilegível.
Criptografia assimétrica	A criptografia assimétrica usa duas chaves, uma para criptografar e outra para descriptografar.
Chave pública	A chave pública é a metade do par de chaves assimétricas. Esta chave é armazenada em sua instância, que usa a chave para criptografar uma chave simétrica. Esta chave simétrica criptografada só pode ser descriptografada quando emparelhada com a chave privada.
Chave privada	A chave privada é a metade do par de chaves assimétricas. Esta chave é armazenada em um armazenamento de chaves no MID Server. A ServiceNow não tem acesso a esta chave. Combinada com a chave pública, o par de chaves assimétricas é usado para descriptografar seus segredos.

Processo de criptografia do lado do cliente

Uma chave simétrica criptografa uma credencial (neste caso, uma senha de administrador), mudando-a de texto não criptografado para texto cifrado criptografado.	
A chave simétrica (representada em verde) pode ser aplicada à credencial para criptografá-la ou descriptografá-la.	
Neste ponto, a criptografia assimétrica começa a usar uma chave pública (amarela) e uma chave privada (azul).	

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A chave pública criptografa a credencial junto com a chave simétrica. A chave simétrica agora está protegida, portanto, não pode ser usada para descriptografar a credencial. Embora a chave pública possa executar essa criptografia, ela não pode ser usada sozinha para descriptografar.

Depois de criptografada com a chave pública, a chave privada é necessária para descriptografar a credencial. Como apenas o cliente tem essa chave, ele é o único que pode acessar a credencial criptografada.

Configurando segredos acessíveis ao cliente

Saiba como configurar sua instância para usar segredos acessíveis ao cliente.

Use esta implementação de exemplo para configurar Gestão de segredos sem usar proxies ou conceder a ServiceNow acesso aos seus dados descriptografados.

Para mais detalhes sobre como usar o Gestão de segredos do lado do cliente a fim de gerenciar o acesso a senhas e grupos, consulte Aprender sobre a Gestão de segredos do lado do cliente.

Estas instruções pressupõem que você tenha um MID Server configurado em sua rede local. Para informações sobre este processo, consulte MID Server.

Visão geral do processo

1. Criação de chaves de criptografia e certificado

   Crie chaves de criptografia e um certificado usando o terminal de comandos em seu ambiente local.

2. Como adicionar seu certificado ao Trusted Key Store da ServiceNow

   Carregue sua chave e certificado para o ServiceNow Trusted Key Store.

3. Como criar um grupo secreto com critérios

   Crie um grupo para seus segredos. Use grupos secretos para organizar seus segredos em grupos. Usando esses grupos, você pode aplicar políticas de acesso a esses segredos no âmbito do grupo. Em seguida, associe seu grupo de segredos a um grupo de identidade e adicione seu servidor MID a esse grupo de identidade.

4. Como fazer o carregamento do par de chaves público/privado para o MID Server

   Carregue seu par de chaves público/privado para o MID server. Este par de chaves permite que o MID server lide com as solicitações de autenticação da sua instância.

5. Criação de credenciais e testagem da criptografia de credenciais

   Crie uma credencial para autenticar em um sistema de terceiros e testar se ServiceNow não pode acessar a credencial.

6. Configuração do Flow Designer para gerenciamento de integração

   Em sua instância, use o Flow Designer para gerenciar uma integração entre sua rede local e sua instância.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

7. Testar a integração de segredos criptografados de ponta a ponta do lado do cliente

   Teste sua integração e revise os detalhes da execução para confirmar se a sua configuração está funcionando.

Criação de chaves de criptografia e certificado

Crie chaves de criptografia e um certificado usando o terminal de comandos em seu ambiente local.

Antes de Iniciar

Função necessária: nenhuma

Procedimento

1. No seu local, abra o Terminal (no Max ou Linux) ou Linha de comando (no Windows).
2. Usando o terminal, use `cd` para mover para a pasta onde você deseja armazenar suas chaves de criptografia.
3. Usando o terminal, insira o seguinte:

```
openssl req -newkey rsa:4096 -nodes -keyout sm_private_key.pem -x509
 -days 365 -out sm_public_cert.pem
```

   Nota: Este exemplo usa o OpenSSL para gerar chaves e certificados. Você pode substitui-lo por outras ferramentas comparáveis com base nos seus requisitos.

   O comando gera uma chave privada e um certificado público (com a chave pública correspondente). Será solicitado uma série de informações para dar continuidade, começando com "Nome do país".

4. Preencha os prompts com as informações solicitadas.
   Os prompts a seguir serão exibidos.
   - Nome do país
   - Nome do estado
   - Nome da localidade (por exemplo, cidade)
   - Nome da Organização (por exemplo, empresa)
   - Nome da unidade organizacional (por exemplo, seção)
   - Nome comum (por exemplo, nome de host totalmente qualificado)
   - Endereço de e-mail

   Trabalhe com sua equipe de segurança para garantir que você insira as informações de certificado corretas.

5. Verifique se a chave privada e o certificado público foram criados na pasta que você escolheu na etapa 2.
   Se você usou os mesmos nomes de arquivo do exemplo da etapa 3, consulte os seguintes arquivos:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- sm_private_key.pem
- sm_public_cert.pem

6. Na mesma pasta, use o seguinte comando:

Importante: O comando específico a ser usado depende do sistema operacional.

Para Linux:	`cat sm_private_key.pem sm_public_cert.pem > sm_keypair_bundle.pem`
Para Windows:	`sm_private_key.pem sm_public_cert.pem > sm_keypair_bundle.pem`

Este comando agrupa a chave privada e o certificado público em um único arquivo para carregar no seu MID Server em etapas posteriores.

7. Verifique a pasta novamente para ter certeza de que o novo arquivo que contém sua chave privada (sm_keypair_bundle.pem) e o certificado público foi criada.

Como adicionar seu certificado ao Trusted Key Store da ServiceNow

Carregue sua chave e certificado para o ServiceNow Trusted Key Store.

Antes de Iniciar

Função necessária: nenhuma

O certificado público que você criou neste exemplo é considerado um certificado "assinado automaticamente" (o que significa que não veio de uma autoridade raiz confiável). Adicione o certificado ao ServiceNow Trusted Key Store para que ele seja usado. Se estiver usando um certificado de uma autoridade, você não precisa concluir esta etapa.

Procedimento

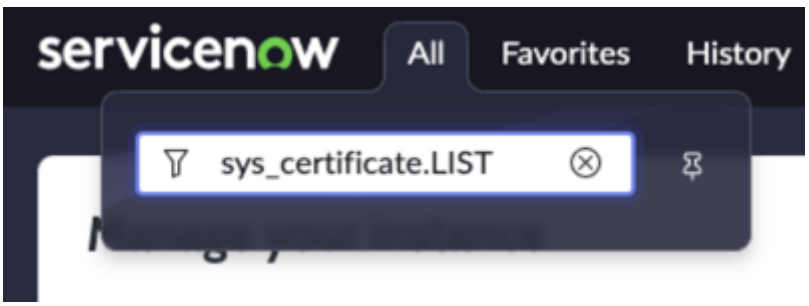
1. No seu local, abra o Terminal (no Max ou Linux) ou Linha de comando (no Windows).
2. Usando o terminal, use `cd` para mover para a pasta onde você criou suas chaves de criptografia.
3. No terminal, insira o seguinte comando:

```
cat sm_public_cert.pem
```

Você deve exibir o conteúdo do seu certificado público para copiá-lo para o Trusted key store. Este comando `cat` exibe o certificado.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Copie as informações do certificado para a área de transferência.
   Inicie e inclua a linha com `-----BEGIN CERTIFICATE-----` e termine e inclua a linha `-----END CERTIFICATE-----`.
5. Em sua instância ServiceNow, navegue até a lista de **certificados X.509** inserindo `sys_certificate.LIST` no filtro de navegação.



6. Selecione **Novo** para criar um registro de **Certificado X.509**.
7. Preencha os campos a seguir no formulário.

Campos da certificação X.509

Campo	Valor
Nome	Nome do Certificado. Este nome pode ser qualquer nome que você escolher.
Formato	Selecione **"PEM"**

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Valor
	Nota: Os arquivos PEM (Privacy Enhanced Mail, Correio eletrônico com privacidade aprimorada) são um tipo de arquivo de PKI (Public Key Infrastructure, Infraestrutura de chave pública) usado para chaves e certificados. Os registros que você criou nas etapas anteriores são desse tipo de arquivo.
Tipo	Selecione **Trusted Store Certificate**
Descrição resumida	Descrição do certificado. Insira um valor que permita você identificar para que o certificado está sendo usado.
Certificado PEM	Cole as informações do certificado que você copiou na etapa 4.

8. Selecione **"Enviar"** para salvar o registro.

Como criar um grupo secreto com critérios

Crie um grupo para seus segredos. Organize seus segredos em grupos secretos e aplique condições de acesso a esses segredos em um nível de grupo. Em seguida, associe seu grupo de segredos a um grupo de identidade e adicione seu MID Server a esse grupo de identidade.

Antes de Iniciar

Função necessária: admin, KMF_admin, sn_secrets.secret_manager e sn_kmf.cryptographic_manager

Procedimento

1. Navegue até **"Todos"** > **"Gestão de segredos"** > **"Grupos secretos com critérios"**.

2. Selecione **"Novo"** para criar o registro de um **Grupo secreto com critérios**.

3. Preencha os campos a seguir no formulário.

Campos dos grupos secretos com critérios

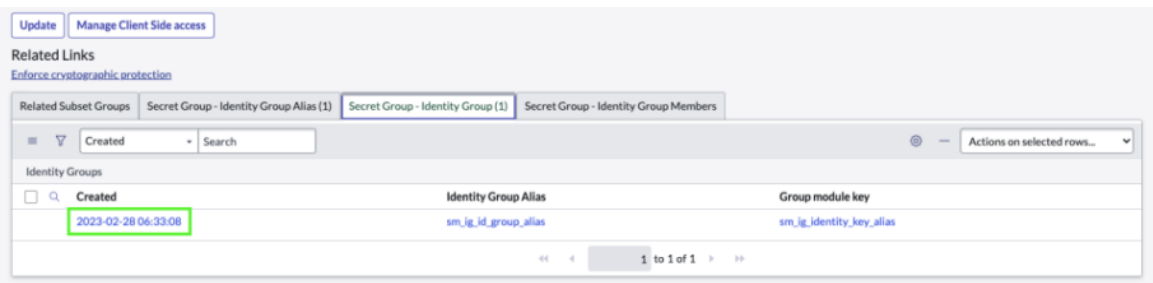
Campo	Valor
Nome do grupo	Nome do grupo secreto. Este nome pode ser qualquer nome que você escolher.
Tipo de segredo	Selecione **"Acessível ao cliente"**
Módulo Autogen	Selecione a caixa
Descrição resumida	Descrição do grupo de segredos. Digite um valor que indique para que esse grupo é usado.
Tipo de critério	Selecione **"Tabela de destino"**
Tabela de destino	Selecione **Credenciais SSH [ssh_credentials]**

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Selecione e mantenha pressionado (ou clique com o botão direito) o cabeçalho do formulário e selecione **Salvar** no menu contextual para salvar o registro.
5. Certifique-se de que a caixa de seleção **Ativo** não esteja marcada.
6. Selecione o botão **"Gerenciar acesso do cliente"** para criar um grupo de identidade. Uma janela com **Alias do grupo de identidade** será exibida.
7. Selecione o botão **"Novo"**.
8. Selecione o ícone de referência ( ) ao lado do campo **Alias do grupo de identidade**.
9. No campo **Nome do alias do grupo**, insira um valor. O nome pode ter qualquer valor que você desejar.
10. Se você escolheu um nome exclusivo na Etapa 9, selecione **Enviar**.
11. Selecione o botão **Carregar chave de identidade**. A janela **Importar certificado de chave pública de identidade** será exibida.
12. Insira um valor no campo **Alias da chave de identidade**.

> **Importante:** Escolha o valor que quiser, mas deve ser uma correspondência exata do que você inserir no MID Server nas etapas posteriores.

13. Selecione **"Importar"**. A janela **"Anexo"** será exibida.
14. Selecione **Escolher arquivo**.
15. Selecione o certificado público que você criou nas etapas anteriores. Esse certificado deve ser o arquivo `sm_public_cert.pem`.
16. Feche a janela clicando no X.
17. Selecione **"OK"** para fechar a janela **Importar certificado de chave pública de identidade**. Uma faixa azul de **Chaves e certificados importados com sucesso para a instância** será exibida para confirmar que a importação foi bem-sucedida.
18. Selecione **"Enviar"**. A lista **Grupos de identidade** será exibida.
19. Marque a caixa de seleção à esquerda do registro do grupo de identidade na lista.
20. Selecione o botão **"Associar grupo secreto"**. Você será levado de volta ao registro do seu **Grupo secreto com critérios**. As listas relacionadas **Grupo de segredos – Alias do grupo de identidade** e **Grupo de segredos – Grupo de identidade** estarão visíveis. Essas listas relacionadas exibem os registros que você criou nas etapas anteriores.
21. Na lista relacionada **Grupo de segredos – Grupo de identidade**, selecione o campo **Criação** para o registro nessa lista.



Um registro de **Grupo de identidade** será exibido.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

22. Na lista relacionada **Membros do grupo de identidade**, selecione o botão **"Novo"**.
    Um registro de **Membro do grupo de identidade** será exibido.
23. No campo **Tabela de membros**, selecione **"MID Server [ecc_agent]"**.
24. Selecione o ícone de referência ( ) ao lado do campo **Registro de membros do grupo de identidade** e selecione o seu MID Server.

    Nota: Se você habilitar a caixa de seleção **Incluir todos os registros**, todos os MID Servers conectados à sua instância serão adicionados ao grupo de identidade.

25. Para fechar a janela **"Selecionar o documento"**, clique em **"OK"**.
26. Selecione **"Enviar"**.
27. Navegue de volta para **"Todos"** > **"Gestão de segredos"** > **Grupos secretos com critérios**e abra o registro que você criou na etapa 2.
28. Habilite o campo **"Ativo"**.
29. Clique em **"Atualizar"** para salvar o registro.

Como fazer o carregamento do par de chaves público/privado para o MID Server

Carregue seu par de chaves público/privado para o MID Server. Este par de chaves permite que o MID Server lide com as solicitações de autenticação da sua instância.

Antes de Iniciar

Função necessária: nenhuma

Como ServiceNow não tem acesso à chave privada, não é possível emparelhá-lo com a chave pública para descriptografar a chave simétrica e, em seguida, descriptografar a credencial. Se o MID Server tentar usar esta credencial criptografada, ele não poderá descriptografar a credencial para autenticação sem ter acesso à chave privada.

Nestas etapas, você carrega a chave privada no MID Server para concluir as chaves públicas/privadas. Este carregamento concede acesso ao MID Server sem conceder acesso ao ServiceNow.

Para conceder ao MID Server acesso à chave privada, você deve criar um comando a ser executado como administrador no Powershell. Neste exemplo, o comando é para a máquina virtual Azure do Windows.

Importante:

Certifique-se de que o sistema em que você executa essas etapas tenha acesso ao MID Server e ao arquivo com o par de chaves.

Procedimento

1. Em seu ambiente local, localize a pasta em que você criou seu par de chaves nas etapas Criação de chaves de criptografia e certificado.
2. Localize e copie o caminho completo para o arquivo `manage-certificates.bat`.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Este arquivo está localizado na pasta do MID Server. Dependendo de onde você armazenou a pasta do MID Server, o caminho pode ser semelhante a este exemplo:

```
C:
\Users\<your_user_account>\Documents\SM_Implementation\mid.utah-07-
08-2022__patch4b01-31-2023_02-07-2023_1702.windows.x86-64\sm_ig_M
IDS\bin\scripts\manage-certificates.bat
```

3. Crie um arquivo de texto e cole o caminho no arquivo.
4. No arquivo de texto, adicione o seguinte informação após o caminho:
   `-a your_identity_key_alias`

   Substitua `your_identity_key_alias` pelo nome do alias da chave de identidade que você criou ao carregar seu certificado público.
5. Localize e copie o caminho completo para o arquivo do par de chaves.

   Nota: Se você usou os nomes nestas etapas, o arquivo será chamado `de sm_keypair_bundle.pem`.
6. No seu arquivo de texto, adicione este caminho ao final da linha, adicionando um espaço entre este caminho e as informações anteriores.
   O texto dentro do seu arquivo de texto deve ser semelhante a este exemplo:

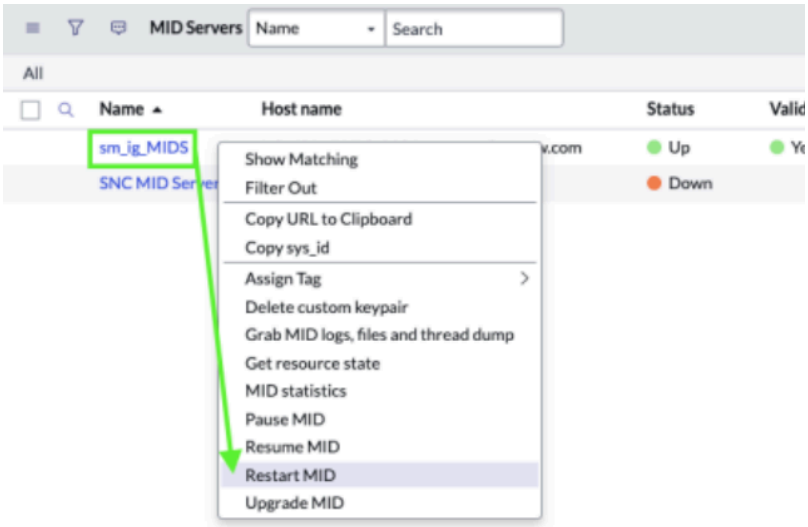
```
C:
\Users\<your_user_account>\Documents\SM_Implementation\mid.utah-07-08-2
022__patch4b01-31-2023_02-07-2023_1702.windows.x86-64\sm_ig_MIDS\bin\sc
ripts\manage-certificates.bat -a your_identity_key_alias
 C:\Users\<your_user_account>\Desktop\sm_keypair_bundle.pem
```

   Nota: Neste exemplo, o arquivo `sm_keypair_bundle.pem` está na área de trabalho para tornar o caminho mais curto.
7. Copie o texto inteiro do arquivo de texto para a área de transferência.
8. Encontre o Powershell no seu sistema e escolha a opção **Executar como administrador**.
9. Cole o texto do arquivo de texto no Powershell e pressione Enter.
   Se for bem-sucedido, você verá a seguinte mensagem:

```
Installed certificate with alias: <your_identity_key_alias> into the
 MID keystore.
```

   Dica: Se você não vir esta mensagem, verifique se o comando não tem erros, espaços ou aspas desnecessárias. Certifique-se de que o caminho completo tenha sido digitado corretamente.
10. Reinicie o MID Server navegando até o registro do MID Server, clicando com o botão direito do mouse no registro e selecionando **Reiniciar MID**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Reiniciar o MID Server sincroniza o par de chaves carregado no armazenamento de chaves MID para uso com as operações. Antes de continuar, aguarde o MID Server reiniciar e apresentar um status de **Operante** e um valor validado de **Sim**.

Criação de credenciais e testagem da criptografia de credenciais

Crie uma credencial para autenticar em um sistema de terceiros.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Navegue até a lista **Credenciais SSH** inserindo `ssh_credentials.list` no filtro de navegação.
2. Selecione **"Novo"** para criar um registro de **Credencial SSH**.
3. Preencha os campos a seguir no formulário.

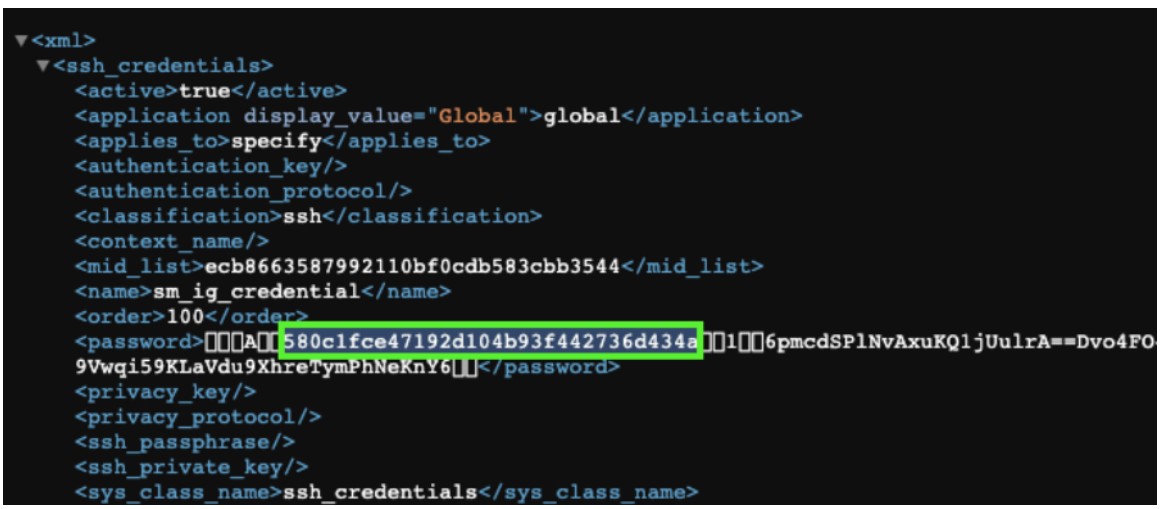
Formulário de Credenciais SSH

Campo	Valor
Nome	Insira um nome para o registro de credenciais. Escolha qualquer nome que desejar.
Aplica-se a	Selecione **MID Servers específicos**
MID Servers	Selecione o seu MID Server.
Nome de usuário	Insira o nome de usuário.
Senha	Insira a senha correspondente ao usuário no campo **Nome de usuário**.

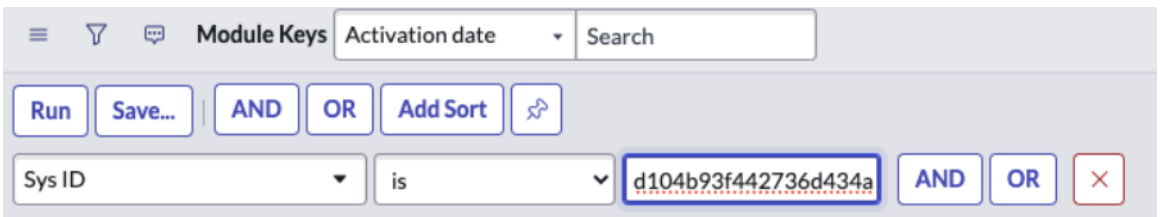
4. Selecione o ícone de cadeado ( ) ao lado do campo **Alias de credencial**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Selecione o ícone de referência ( ) para abrir a lista de **Aliases de conexão e credencial**.
6. Selecione **"Novo"** para criar um registro de **Aliases de conexão e credencial**.
7. Digite um nome no campo **Nome**.
8. Selecione **"Credencial"** no campo **Tipo**.
9. Selecione **"Enviar"**.
   Você será levado de volta ao registro de **Credenciais SSH**. Nas próximas etapas, você irá testar se a credencial está criptografada.
10. Selecione e mantenha pressionado (ou clique com o botão direito) o cabeçalho do formulário e escolha **Mostrar XML**.
11. Encontre o marcador `<password>` contido no XML.
12. Copie o sys_id contido nesse marcador de `<password>` para a área de transferência.
    O sys_id é um código de 32 caracteres que representa a chave simétrica que está sendo usada para criptografar esta credencial. A senha criptografada que você inseriu na tabela Credenciais SSH está à direita dos dois conjuntos de caixas de seleção nesta mesma linha.



13. Navegue até a lista **Chaves do módulo** inserindo `sys_kmf_module_key.list` no filtro de navegação.
14. Filtre a lista de registros em que o campo **Sys ID** do sistema corresponda ao sys_id que você copiou na etapa 12 e selecione **"Executar"**.



Sua pesquisa deve retornar um único registro de **Chave de módulo**. Esse registro mostra que você criou uma chave simétrica e a está usando com sucesso.

15. Navegue até a lista **Chaves do módulo encapsulado** inserindo `sys_kmf_wrapped_module_key.list` no filtro de navegação.
16. Filtre a lista de registros em que o campo **Módulo de criptografia** corresponda ao módulo criptográfico que você criou nas etapas anteriores e selecione **Executar**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Sua pesquisa deve retornar um único registro de **Chave de módulo encapsulado**. Nessa lista, você pode verificar o seguinte:

- A coluna **Material de chave encapsulado** mostra que a chave simétrica no módulo de criptografia (que está sendo usada para criptografar a credencial SSH) é criptografada pela chave pública que você carregou para o Grupo de identidade.
- O campo **ID do sistema de encapsulamento de chaves** mostra que é a chave (a chave simétrica do módulo de criptografia) que está sendo criptografada pelo **ID do sistema de encapsulamento de chaves** (a chave pública carregada no Grupo de identidade).

Se os campos anteriores não estiverem na sua lista por padrão, você poderá adicioná-los à lista selecionando o ícone **"Personalizar lista"** ( ).

Nota: Sua instância executa um trabalho de limpeza a cada dez minutos, o que remove chaves órfãs e impede a proliferação de chaves não associadas após a atualização de suas credenciais.

Configuração do Flow Designer para gerenciamento de integração

Em sua instância, use o Flow Designer para gerenciar uma integração entre sua rede local e sua instância.

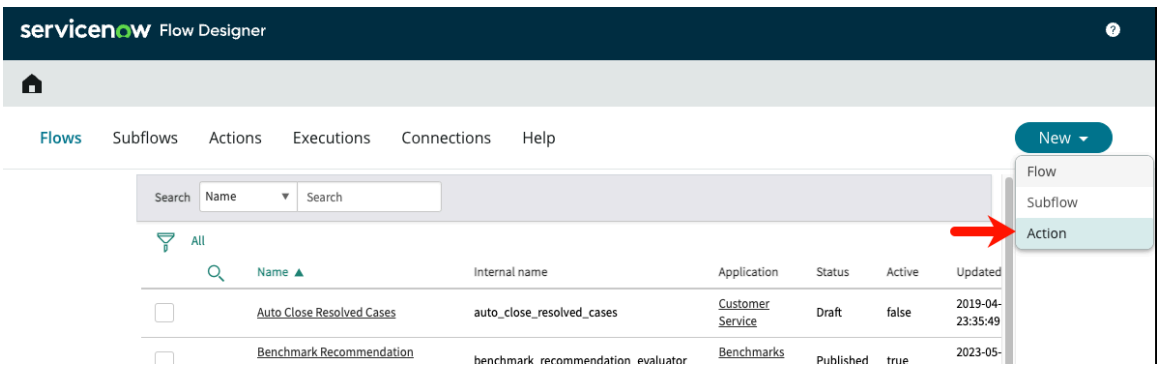
Antes de Iniciar

Função necessária: admin

Seguindo estas etapas, você criará um fluxo de trabalho de Flow Designer para criar um arquivo de texto em seu sistema local.

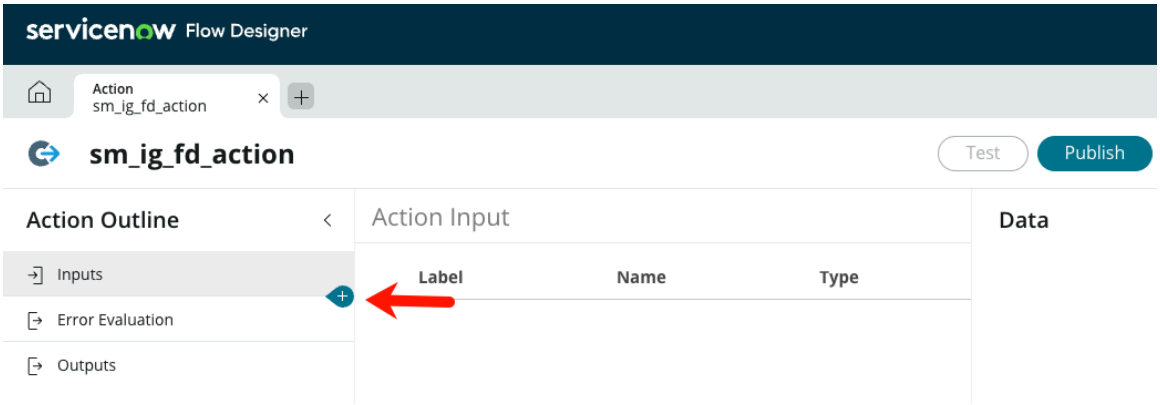
Procedimento

1. Na sua instância, navegue até **"Todos"** > **"Automação de processo"** > **"Flow Designer"**.
2. Crie uma ação em ServiceNow selecionando **"Novo"** e **"Ação"**.

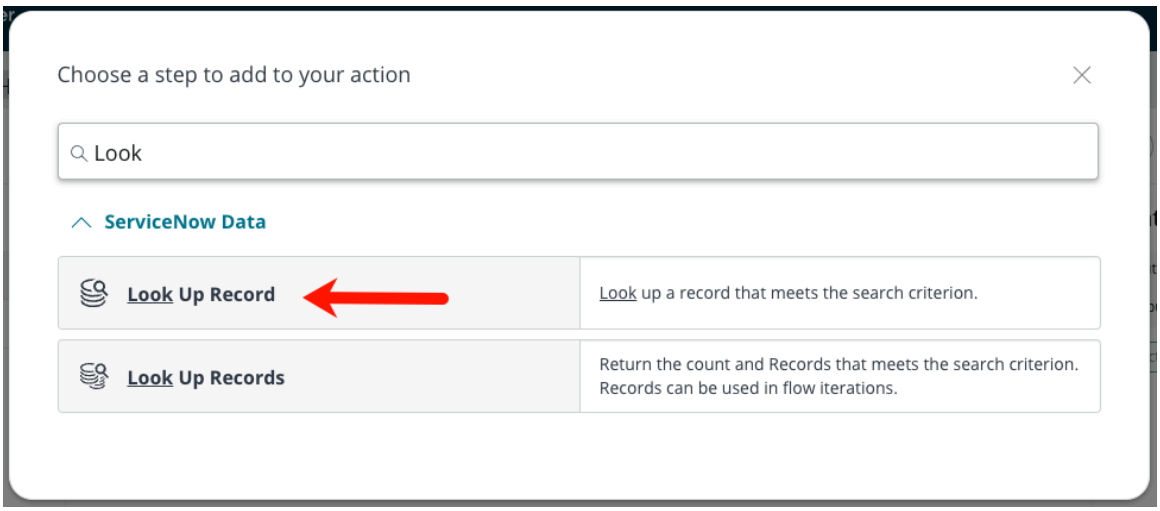


3. Insira um nome no campo **"Nome da ação"** e selecione **"Enviar"**.
4. Crie uma etapa selecionando o sinal de adição entre **Entradas** e **Avaliação de erro** em **Descrição da ação**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Na janela **"Escolha uma etapa para adicionar à sua ação"**, selecione **"Pesquisa de registro"**.



6. Na etapa **Pesquisar registro**, selecione **MID Server [ecc_agent]** no campo **Tabela**.
7. Crie outra etapa selecionando o sinal de adição na etapa **Pesquisar registro**.
8. Na janela **"Escolha uma etapa para adicionar à sua ação"**, selecione **"SSH"**.

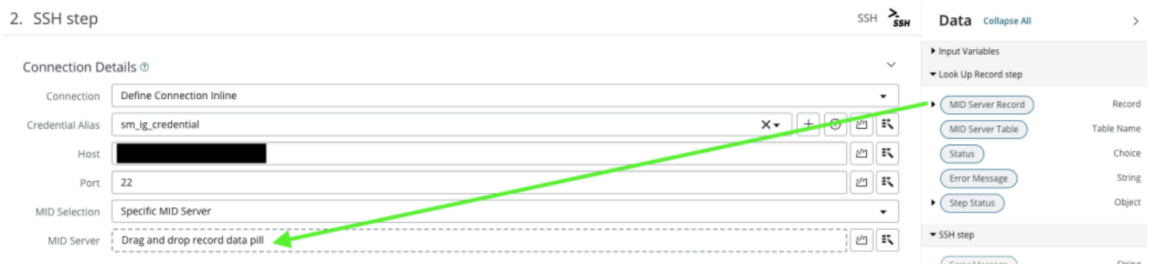
> **Nota:** Se você não vir a opção **"SSH"**, ative o plug-in necessário.

9. Na etapa **SSH**, insira as informações a seguir:

Campo	Valor
Conexão	Selecione **"Definir conexão em linha"**
Alias de credencial	Selecione o alias de credencial para a credencial SSH que foi criada nas etapas anteriores.
Host	Insira o endereço IP do host ao qual você está se conectando via SSH.
Porta	Insira `22`.
Seleção de MID	Selecione **MID Server específico**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

10. Para preencher o campo do **MID Server**, arraste a cápsula **Registro do MID Server** da seção **Dados** para o campo.



> ⚠ **Aviso:** Ao arrastar a cápsula para o campo, selecione a cápsula e não a seta preta ao lado dela.

11. Na seção **Configuração do SSH**, insira o valor a seguir no campo **Comando**.

```
/bin/date > sm_ig_text_file.txt
```

Esse comando cria um arquivo de texto em seu sistema local usando os segredos descriptografados do MID Server. O MID Server concede acesso à instância da ServiceNow (por meio do Flow Designer) sem nunca conceder acesso da instância da ServiceNow ao segredo descriptografado.

> **Dica:** O comando `/bin/date` insere a data/hora atual no arquivo de texto criado. Este comando demonstra que a integração está acontecendo em tempo real com base na data/hora atuais em relação a quando o arquivo de texto foi criado.

12. Selecione o botão **Salvar** para salvar o fluxo de trabalho.

Testar a integração de segredos criptografados de ponta a ponta do lado do cliente

Teste sua integração e revise os detalhes da execução para confirmar se a sua configuração está funcionando.

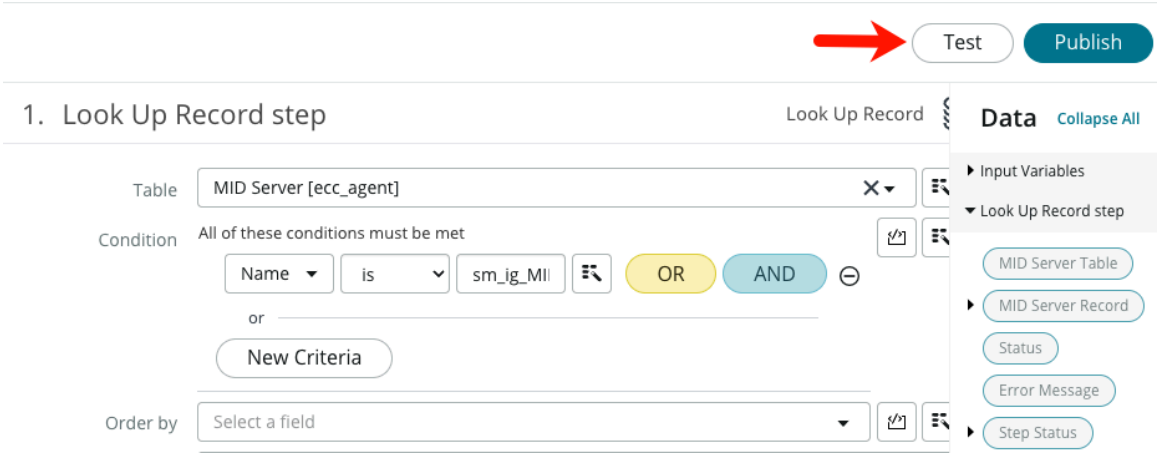
Antes de Iniciar

Função necessária: admin

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Em Flow Designer, selecione o botão **Testar** no canto superior direito da tela.



2. Na janela **Ação de teste**, selecione **Executar teste**.
3. Selecione **A execução do seu teste foi concluída. Visualize os detalhes de execução da ação.**
4. Atualize sua tela até ver **Execução de teste - Concluída** no canto superior direito da tela.
5. Selecione a seta de **Etapas**, na parte inferior esquerda da tela.
6. Role para baixo até ver o título **Dados de Saída da Etapa** com a seguinte mensagem de sucesso:

```
{"Step Status";{"code";0,"message";"Success"}}
```

7. Depois de ver esta mensagem no Flow Designer, verifique se o arquivo de texto foi criado no sistema local.

Como testar uma credencial do Windows Management Instrumentation criptografada com a Gestão de segredos

Verifique se sua credencial do WMI (Windows Management Instrumentation) está criptografada com a Gestão de segredos e use um fluxo de trabalho do IntegrationHub para concluir o teste de ponta a ponta.

Antes de Iniciar

Função necessária: administrador

- O Integration Hub Enterprise deve estar ativo na sua instância. Para obter detalhes, consulte Solicitar um plug-in Integration Hub.
- Você deve ter um grupo de segredos configurado em sua instância. Consulte as etapas 1 a 3 listadas em Configurando segredos acessíveis ao cliente.
- Você deve ter uma credencial configurada criptografada com a Gestão de segredos. Consulte as etapas 1 a 9 listadas em Criação de credenciais e testagem da criptografia de credenciais.

Procedimento

1. Confirme se o MID Server desejado está associado ao grupo de segredos.
   Abra o registro Grupo de segredos com critérios [sn_sm_criteria_secret_group] e procure seu MID Server na lista **Grupo de segredos - Membros do grupo de identidade**. Se o seu

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

MID Server não estiver associado a um grupo, consulte Como criar um grupo secreto com critérios.

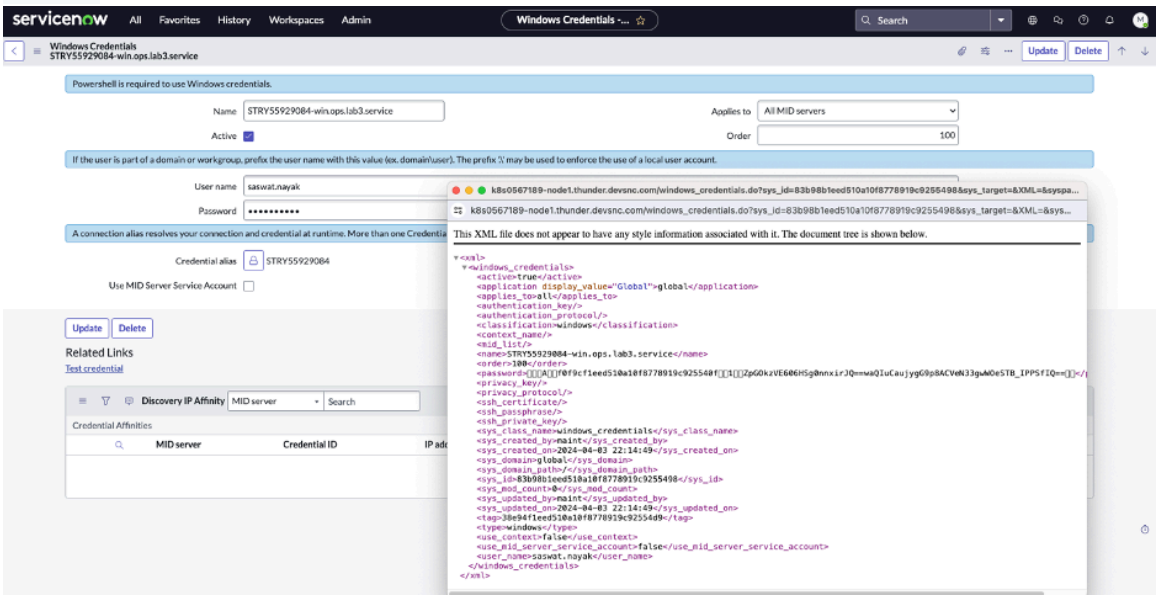
2. Confirme se a credencial está criptografada com a Gestão de segredos.

   a. Navegue até **Todos** > **IntegrationHub** > **Conexões e credenciais** > **Credenciais**.

   b. Abra seu registro de credencial.
   Verifique se você tem um alias de credencial listado no campo **Alias de credencial**. Se você ainda não criou um, consulte Crie um alias de Conexão e Credenciais.

   c. Selecione e mantenha pressionado (ou clique com o botão direito) o cabeçalho do registro de credenciais e selecione **Mostrar XML** na lista.

   d. Na exibição XML do registro, localize a senha e confirme se o valor começa com □□□A□□.



3. Crie um fluxo de trabalho de teste no Workflow Studio.

   a. Navegue até **Todos** > **Automação de processo** > **Workflow Studio**.

   b. Selecione **Novo** e, em seguida, selecione **Ação** na lista.

   c. Digite um nome no campo **Nome da ação**.
   Deixe o campo **Aplicação** definido como "Global".

   d. Selecione o botão **Criar ação**.

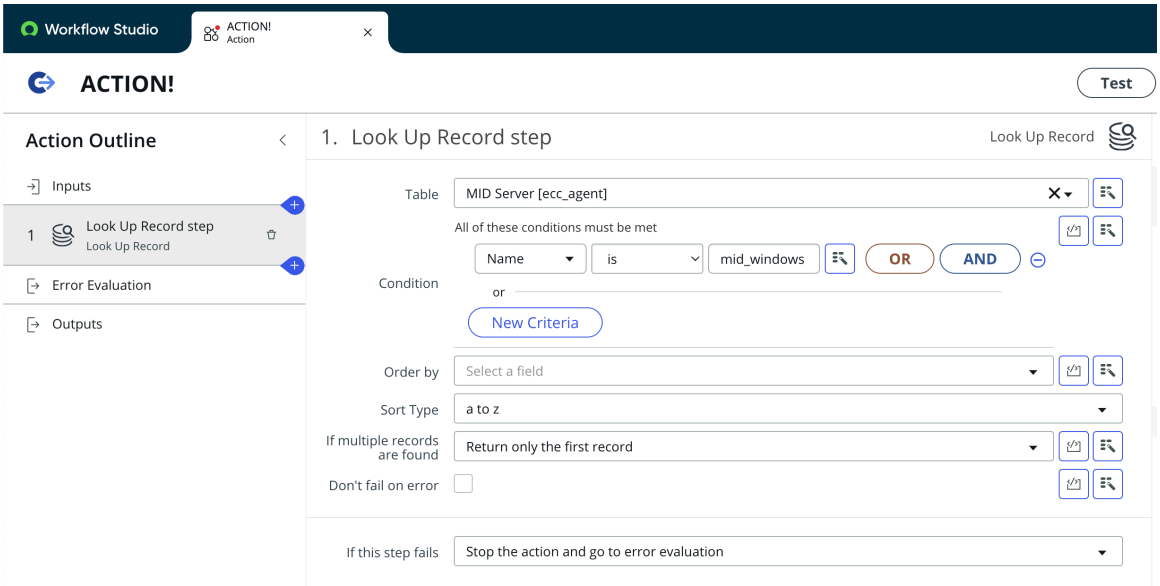
4. Configure uma etapa de pesquisa de registro no Workflow Studio.

   a. Em **Descrição da ação**, selecione o botão de adição para incluir uma nova etapa.
   Localize e selecione o tipo de etapa **Pesquisar registro**.

   b. No campo **Tabela**, selecione **MID Server [ecc_agent]**.

   c. Para a condição, selecione **O nome é**, seguido pelo nome do seu MID Server.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Importante: Certifique-se de que o MID Server selecionado seja o mesmo associado ao grupo de segredos.

5. Configure uma etapa de pesquisa de registro no Workflow Studio.

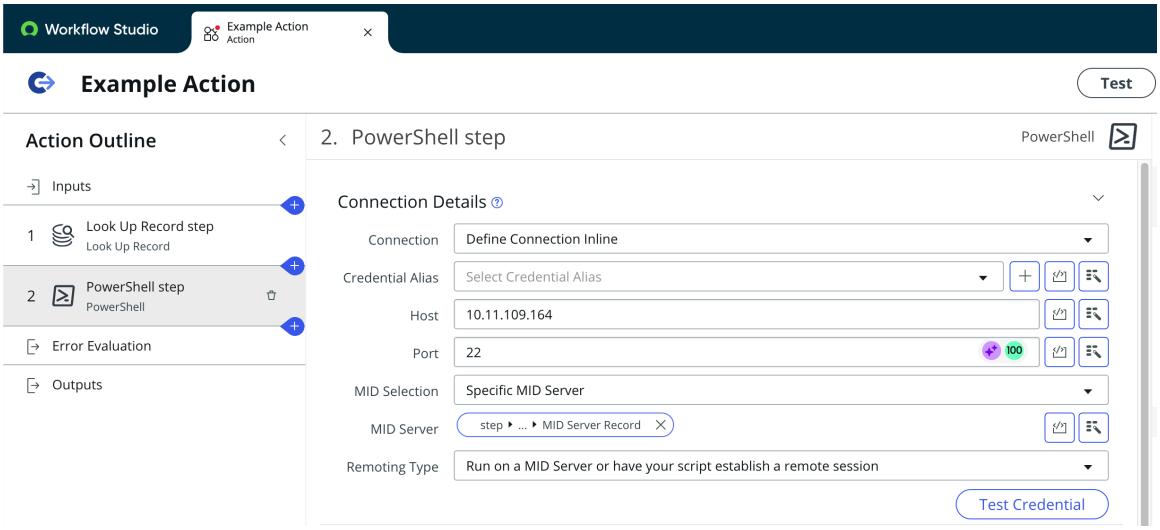
   a. Em **Descrição da ação**, selecione o botão de adição para incluir uma nova etapa abaixo da etapa "Pesquisar registro".
   Encontre e selecione o tipo de etapa **PowerShell**.

   b. No formulário **Etapa de PowerShell**, preencha os campos conforme necessário.

Campos da etapa de PowerShell

Campo	Valor
Conexão	Selecione **"Definir conexão em linha"**
Alias de credencial	Selecione seu alias de credencial
Host	Digite o endereço IP do servidor Windows de destino
Porta	Digite 22 caso ainda não seja o padrão.
Seleção de MID	Selecione **MID Server específico**
MID Server	Arraste a cápsula **Registro do MID Server** a partir do painel **Dados** Essa cápsula de dados está visível no painel **Dados** na borda direita da tela, sob a etapa **Pesquisar registro**.
Tipo de comunicação remota	Selecione **Executar em um MID Server ou fazer com que o script estabeleça uma sessão remota**

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



6. Crie um script para sua ação de teste.

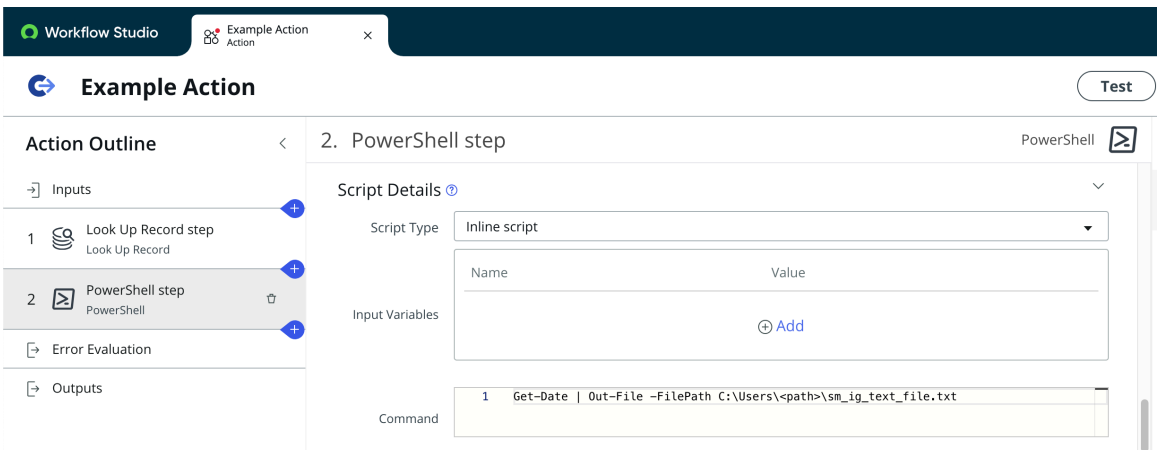
   a. No campo **Tipo de script**, selecione **Script em linha**.

   b. Use o script abaixo, substituindo o caminho de exemplo pelo caminho do seu host de teste.

```
Get-Date | Out-File -FilePath C:\Users\<path>\sm_ig_text_file.txt
```

   Nota: Também é possível executar seu próprio script que se adapta à sua configuração de host remoto. É importante confirmar se uma conexão foi estabelecida usando o valor criptografado pela SM.

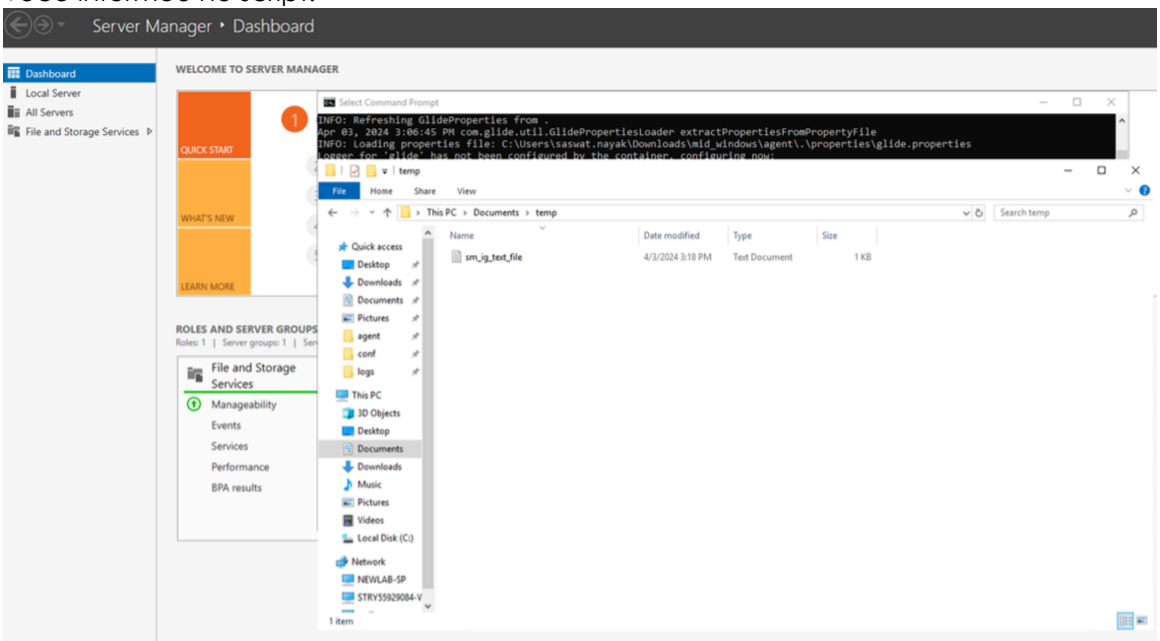
   c. Selecione o botão **Salvar** para salvar sua ação.



7. Selecione o botão **Testar** para testar sua ação.
8. Revise os logs de saída em busca de mensagens de erro.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

9. Verifique se um arquivo de teste foi criado no servidor host, no caminho do arquivo que você informou no script.



Clonagem e gestão de segredos

Saiba como reconfigurar os grupos de segredos e os grupos de segredos do cliente após um clone.

Depois de clonar uma instância, talvez seja necessário reconfigurar os grupos de segredos e os grupos de segredos do cliente para que funcionem conforme o esperado.

Origem do grupo de segredos	Comportamento após um clone
Grupos de segredos da instância originais da instância de destino	Funciona conforme o esperado depois de importar manualmente o módulo criptográfico ausente. Consulte Exportando e importando dados via XML.
Grupos de segredos do cliente originais da instância de destino	Funciona conforme o esperado depois de importar manualmente o módulo criptográfico ausente. Consulte Exportando e importando dados via XML.
Grupos de segredos da instância clonados da instância de origem	Só funcionará se houver a configuração manual
Grupos de segredos do cliente clonados da instância de origem	Funcionará se houver a configuração manual de sg/identity group/alias/mid

Painel da Gestão de segredos

Use o painel da Gestão de segredos para revisar os grupos de segredos configurados em sua instância e aprender sobre problemas de segurança.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Visão geral do grupo secreto

A guia **Visão geral do grupo secreto** exibe informações sobre os grupos secretos configurados. Use esta guia para ver informações sobre os grupos de segredos configurados em sua instância.

Grupo secreto por tipo

Exibe um gráfico de pizza mostrando grupos de segredo instalados em sua instância, agrupados por tipo de segredo (lado da instância do lado do cliente).

Grupo secreto por tipo de critério

Exibe um gráfico de pizza mostrando grupos secretos com critérios configurados em sua instância pelo tipo de critério usado.

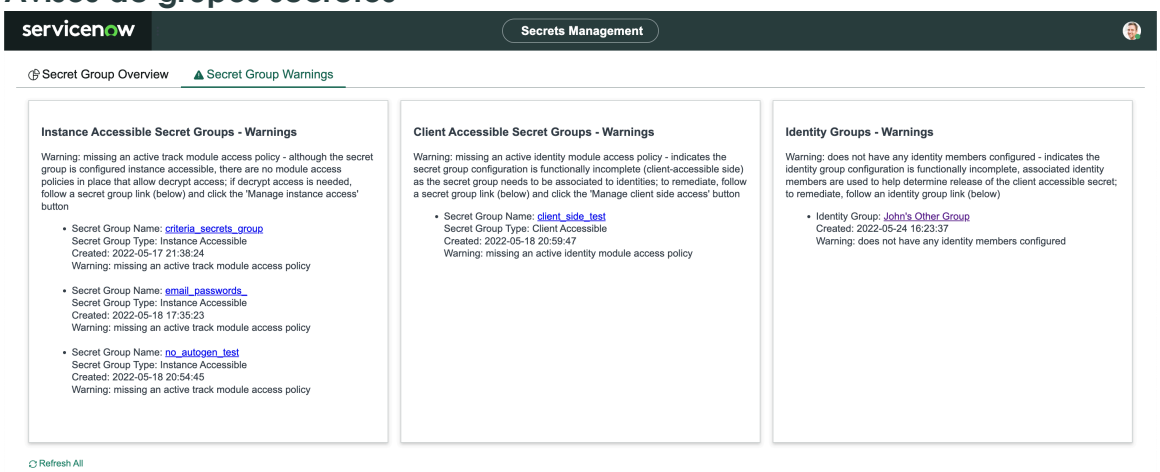
Número de grupos secretos inativos

Exibe uma contagem dos grupos secretos inativos configurados em sua instância.

Número de segredos dedicados

Exibe uma contagem de segredos em grupos de segredos básicos.

Avisos de grupos secretos



A guia **Avisos de grupos secretos** exibe avisos relacionados aos seus grupos secretos e grupos de identidade.

Grupos secretos acessíveis para a instância - Avisos

Este cartão exibirá avisos se houver grupos secretos sem políticas de acesso ativas em vigor. Selecione o nome de um grupo secreto para exibir esse registro.

Grupos secretos acessíveis para o cliente - Avisos

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Este cartão exibirá avisos se houver grupos secretos acessíveis pelo cliente que não tenham uma MAP (module access policy, política de acesso ao módulo) de identidade ativa. Selecione o nome de um grupo secreto para exibir esse registro.

Grupos de identidade - Avisos

Este cartão exibirá avisos se houver grupos de identidade que não tenham membros do grupo configurados. Selecione o nome do grupo de identidade para exibir o registro.

Nota: O Painel de gestão de segredos faz parte do Gestão de segredos Enterprise. A Gestão de segredos Enterprise é um plug-in pago que a equipe da ServiceNow deve ativar em sua instância de produção.

Funções de gestão de segredos

A gestão de segredos adiciona essas funções

Administrador de segredos [sn_secrets.admin]

Atribua funções de segredos de não administrador a outros usuários. Os administradores de segredos têm os mesmos privilégios que o gerente e o visualizador de segredos.

Contém funções

Lista de funções contidas na função.

Nenhum.

Grupos

Lista de grupos aos quais esta função está atribuída por padrão.

Nenhum.

Considerações especiais

Importante: Evite conceder uma função de administrador quando houver mais funções especializadas disponíveis.

- Um usuário deve ter as funções admin e security_admin para ser atribuído à função sn_secret.admin.
- Evite conceder uma função de administrador quando houver mais funções direcionadas disponíveis.

Gerente de segredos [sn_secrets.manager]

Conceda esta função a usuários que devem ser capazes de executar qualquer uma das seguintes funções.

- Exibir segredo e registros de grupo secreto
- Exibir histórico de acesso e outras informações de atividade de uso
- Criar grupos secretos e filtros
- Criar provedores secretos

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Mover segredos entre grupos secretos
- Alterar configurações de grupo secreto e provedor secreto

Contém as funções

Lista de funções contidas na função.

Nenhum.

Grupos

Lista de grupos aos quais esta função está atribuída por padrão.

Nenhum.

Considerações especiais

Importante: Os gerentes de segredos não podem ver os segredos em texto sem formatação.

Visualizador de segredos [sn_secrets.viewer]

Conceda esta função a usuários que devem ser capazes de exibir segredo e registros de grupo secreto.

Contém funções

Lista de funções contidas na função.

Nenhum.

Grupos

Lista de grupos aos quais esta função está atribuída por padrão.

Nenhum.

Considerações especiais

Nenhum.

Criar um módulo criptográfico de grupo de segredos

Crie um módulo criptográfico de grupo de segredos para executar criptografia e descriptografia.

Antes de Iniciar
Função necessária:

- admin
- sn_secrets.admin
- sn_secrets.secret_manager
- sn_kmf.cryptographic_manager
- sn_kmf.admin

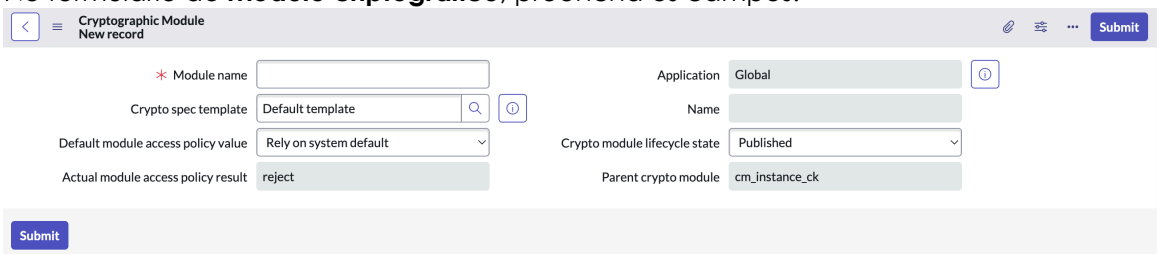
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegue até **Todos** > **Gestão de segredos** > **Criar módulo de criptografia de grupo secreto**.
2. Selecione o tipo de módulo criptográfico de grupo que você deseja criar.

Criptografia do tipo módulo	Descrição
Criar um módulo secreto de criptografia com acesso à instância	Crie segredos acessíveis da instância que podem ser descriptografados por sua instância.
Criar um módulo de criptografia de segredos acessível ao cliente	Crie segredos acessíveis ao cliente, que são criptografados usando sua própria chave, inacessível para ServiceNow.

3. No formulário do **Módulo criptográfico**, preencha os campos.



Campo	Descrição
Nome do módulo	Nome descritivo do seu módulo
Aplicação	O escopo da aplicação que contém seu módulo. O campo é preenchido automaticamente com o módulo atual.
Modelo de especificação de criptografia	**Modelo padrão** é selecionado por padrão.
Nome	Nome do módulo. Este nome é gerado automaticamente com base na aplicação e no nome do módulo.
Valor da política de acesso ao módulo padrão	◦ Depende de padrão do sistema ◦ Rejeitar ◦ Rastreamento
Estado do ciclo de vida do módulo de criptografia	Se o módulo está no estado **Rascunho** ou **Publicado**.
Resultado real da política de acesso ao módulo	Este campo é para fins informativos e é somente para leitura.
Módulo de criptografia primário	O módulo de criptografia primário, que é determinado pelo tipo de módulo de criptográfico selecionado na etapa anterior. Este campo é só de leitura.

4. Selecione **Enviar**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Criação de um grupo de segredo básico

Crie um grupo de segredo básico para agrupar quaisquer segredos, independentemente de seus critérios.

Antes de Iniciar

Função necessária: admin

Grupos de segredo básicos podem conter qualquer segredo adicionado a eles, independentemente de tabela, escopo ou aplicação. Depois de criado, você adiciona segredos ao grupo. Para criar um grupo especificamente para todos os segredos que compartilham um atributo comum, como esses, crie um grupo de segredo com critérios usando as instruções em Como criar um grupo secreto com critérios.

Procedimento

1. Navegue até **Todos** > **Gestão de segredos** > **Grupos secretos**.
2. Selecione **Novo**.
3. Em **Que tipo de grupo secreto você deseja criar?** selecione **Grupo secreto básico**.
4. No formulário **Grupo secreto**, preencha os campos.

Campos de grupo secreto

Campo	Descrição
Nome do grupo	Nome para o grupo **Nota:** Os nomes dos grupos secretos podem conter somente caracteres minúsculos, números e sublinhados (_)
Tipo de segredo	Se o grupo é **Acessível à instância** ou **Acessível ao cliente**.
Módulo Autogen	Gera um novo módulo de criptografia para este grupo secreto. Este módulo criptografa e descriptografa seus dados. Este campo está habilitado por padrão.
Aplicação	Aplicação com escopo para este registro. Este campo somente-leitura é preenchido automaticamente com o escopo atual.
Descrição resumida	Descrição do grupo
Módulo de criptografia	Selecione o módulo de criptografia a ser usado com este grupo. Este módulo criptografa e descriptografa seus dados. Este campo só fica visível quando o **Módulo Autogen** não está selecionado. Para obter detalhes sobre políticas de acesso ao módulo, consulte Visão geral da política de acesso ao módulo.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: Você pode revisar as políticas de acesso ao módulo relacionadas ao seu grupo secreto usando o botão **Gerenciar acesso à instância**.

5. Clique em **Enviar**.

Nota: Quando criado, um grupo secreto fica inativo por padrão. Retorne ao registro do grupo e selecione **Ativo** para ativar o grupo.

Como criar um grupo secreto com critérios

Crie um grupo secreto com critérios para organizar automaticamente os segredos inseridos nos campos Password2 quando eles tiverem critérios comuns, como tabela, escopo ou aplicação.

Antes de Iniciar

Função necessária: admin

Os segredos neste tipo de grupo secreto devem compartilhar critérios comuns. Para grupos sem essa restrição, considere a criação de um grupo secreto básico. Saiba mais sobre como criar um grupo secreto básico em Criação de um grupo de segredo básico.

Procedimento

1. Navegue até **Todos** > **Gestão de segredos** > **Grupos secretos**.
2. Selecione **Novo**.
3. No aviso **Que tipo de grupo de segredos você deseja criar?**, selecione **Grupo secreto contendo critérios**.
4. No formulário **Grupo secreto**, preencha os campos.

Campos de grupo secreto

Campo	Descrição
Nome do grupo	Nome para o grupo **Nota:** Os nomes dos grupos secretos podem conter somente caracteres minúsculos, números e sublinhados (_)
Tipo de segredo	Se o grupo é **Acessível à instância** ou **Acessível ao cliente.**
Módulo Autogen	Gera um novo módulo de criptografia para este grupo secreto. Este módulo criptografa e descriptografa seus dados. Este campo está habilitado por padrão.
Aplicação	Aplicação com escopo para este registro. Este campo somente-leitura é preenchido automaticamente com o escopo atual.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Descrição resumida	Descrição do grupo
Tipo de critério	Os critérios que os segredos deste grupo compartilham. ◦ Escopo ◦ Pacote ◦ Tabela de destino ◦ Coluna secreta ◦ Registro de filtro
Módulo de criptografia	Selecione o módulo de criptografia a ser usado com este grupo. Este módulo criptografa e descriptografa seus dados. Este campo só fica visível quando o **Módulo Autogen** não está selecionado. Para obter detalhes sobre políticas de acesso ao módulo, consulte Visão geral da política de acesso ao módulo. **Nota:** Você pode revisar as políticas de acesso ao módulo relacionadas ao seu grupo secreto usando o botão **Gerenciar acesso à instância**.

Nota: Dependendo da sua configuração, o **Módulo de criptografia** pode usar um valor selecionado automaticamente.

Quando o campo **Tipo de critério** é definido como `Pacote` e o campo **Módulo Autogen** é selecionado:	O campo **Módulo de criptografia** fica vazio e é somente leitura. Utiliza-se um submódulo Password2 existente. Se um submódulo Password2 não for encontrado, o módulo Criptografia do Glide em nível de instância será usado.
Quando o campo **Tipo de critério** é definido como `Pacote` e o campo **Módulo Autogen** é desmarcado: (somente usuários Enterprise podem desmarcar o campo **Módulo Autogen**)	O campo **Módulo de criptografia** é editável e os administradores podem selecionar um módulo de criptografia para usar.

5. Selecione e segure (ou clique com o botão direito) o cabeçalho do formulário e escolha **Salvar**.

   Nota: Quando criado, um grupo secreto fica inativo por padrão.

6. Depois de salvar o registro, campos adicionais podem aparecer com base em como você configurou seu grupo.

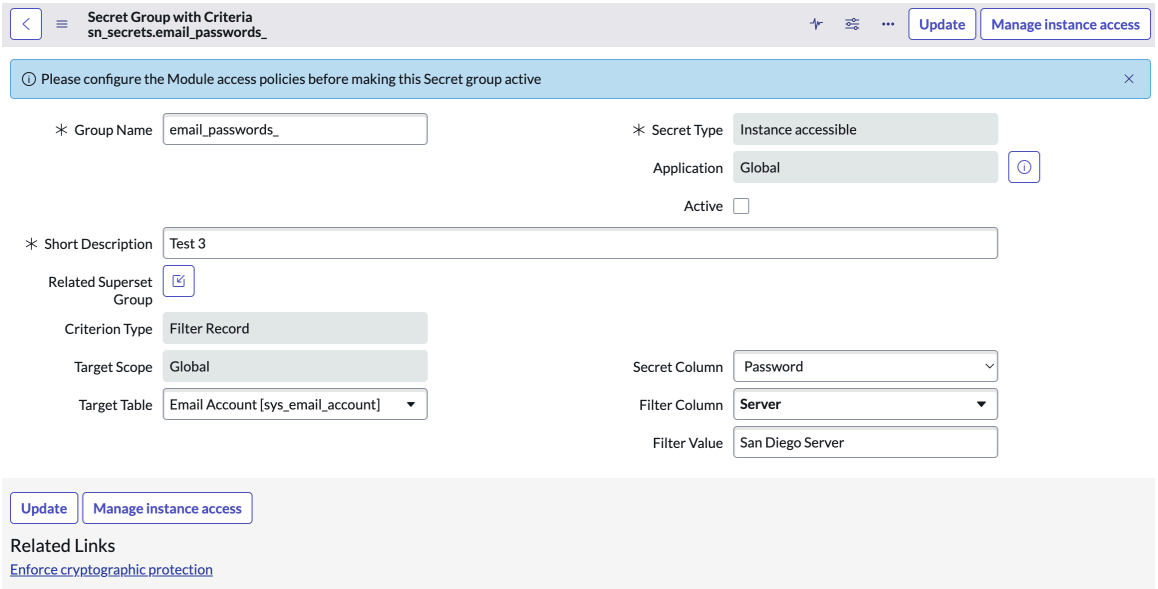
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campos de grupo secreto adicionais

Campo	Descrição
Escopo de destino	Escopo compartilhado pelos segredos a serem atribuídos a este grupo. Este campo só está disponível quando você seleciona `Escopo` no campo **Tipo de critério**.
Pacote de destino	Pacote compartilhado pelos segredos a serem atribuídos a este grupo. Este campo só está disponível quando você seleciona `Pacote` no campo **Tipo de critério**.
Tabela de destino	Tabela compartilhada pelos segredos a serem atribuídos a este grupo. Este campo só está disponível quando você seleciona `Tabela` ou `Coluna secreta` no campo **Tipo de critério**.
Escopo de destino	Escopo da aplicação da tabela selecionada no campo **Tabela de destino**. Esse campo só fica visível quando você seleciona `Tabela`, `Filtrar coluna` ou `Coluna secreta` no campo **Tipo de critério**.
Coluna secreta	Coluna da tabela que contém os segredos de password2 que você inclui nesse grupo. Os campos disponíveis nesta lista são determinados pela tabela selecionada no campo **Tabela de destino**. **Nota:** Se não houver colunas na tabela selecionada que contenham segredos, este campo exibirá somente `– Nenhum --` como uma seleção.
Filtrar coluna	A coluna da tabela selecionada em **Tabela de destino** que você deseja usar como filtro. Este campo não pode ser um campo Password2.
Valor de filtro	O valor que você deseja usar como filtro. Este filtro se aplica ao campo selecionado no campo **Coluna de filtro**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Example: Um grupo acessível pela instância que contém todas as senhas de contas de e-mail de um servidor de e-mail.



O que Fazer Depois

Depois de criar seu grupo, todos os novos registros correspondentes aos critérios serão criptografados. Para criptografar registros existentes usando o módulo criptográfico desse grupo, é necessário executar um trabalho de segurança. Para obter detalhes, consulte Executar trabalhos de segurança da gestão de segredos.

Os grupos acessíveis pelo cliente precisam de uma chave pública fornecida pelo cliente para criptografar seus segredos. Para conferir as etapas para carregar essa chave, consulte Carregar uma chave pública para a Gestão de segredos.

Carregar uma chave pública para a Gestão de segredos

Carregue uma chave pública para criptografar seus segredos.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Acesse **Todos** > **Gestão de segredos** > **Grupos secretos** e abra o registro do grupo secreto.
2. No registro, selecione o botão **Gerenciar acesso do cliente**.
   Um novo registro de grupo de identidades será aberto.
3. Selecione o botão **Carregar chave de identidade**.
   A janela **Importar certificado de chave pública de identidade** será exibida.
4. Insira um alias para a chave no campo **Alias da chave de identidade**.
5. Selecione o botão **Importar** para carregar a chave pelo ambiente local.
6. Selecione o botão **OK**.
   O campo **Chave do módulo de grupo** usa o alias da chave de identidade.
7. Selecione **Enviar** para salvar o registro do grupo de identidade.

Executar trabalhos de segurança da gestão de segredos

Programe um trabalho de gestão de segredos para executar tarefas de criptografia em campos de segredos em sua instância.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Função necessária: sn_kmf.admin, security_admin e sn_secrets.admin

Para realizar essas etapas, você deve ser elevado à função security_admin. Para obter detalhes sobre esse processo, consulte Elevar para uma função privilegiada.

Procedimento

1. Navegue até **Todos** > **Segurança do sistema** > **Trabalhos de segurança** > **Criar novo**.
2. No prompt **Que tipo de trabalho de segurança você deseja criar?** selecione **Trabalho de Gestão de segredos**.
3. No formulário, preencha os campos.

Formulário de trabalho de gestão de segredos

Campo	Descrição
Nome	Nome do trabalho de segurança
Estado	O estado inicial do trabalho é Novo. Após sua execução conforme programado, o estado será atualizado de acordo
Início da janela de tempo	Hora de início do trabalho no formato 24h. O trabalho começa a ser executado no horário escolhido.
Fim da janela de tempo	Hora de finalização do trabalho no formato 24h. Se o trabalho não estiver concluído até essa hora, ele continuará durante a próxima janela de processamento especificada até que o trabalho seja concluído.
Nível de aplicação	Se o trabalho afeta todas as tabelas ou uma seleção de tabelas ou campos específicos. Selecione a partir de ◦ Todas as tabelas ◦ Tabelas específicas ◦ Campos específicos ◦ Pacotes específicos ⚠ **Aviso:** Selecionar a opção **"Todas as tabelas"** pode afetar o desempenho da instância. Considere programar em horários fora do pico.
Packages	Os pacotes a serem incluídas neste trabalho. A criptografia será aplicada aos pacotes selecionados. Esta opção será exibida somente quando o campo **Nível de aplicação** estiver definido como **Pacotes específicos**
Tabelas	As tabelas a serem incluídas neste trabalho. A criptografia é aplicada a todos os campos aplicáveis nas tabelas

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	selecionadas. Esta opção será exibida somente quando o **Nível de aplicação** estiver definido como **Tabelas específicas**
Campos	As tabelas a serem incluídas neste trabalho. A criptografia é aplicada a todos os campos selecionados. Esta opção será exibida somente quando o **Nível de aplicação** estiver definido como **Campos específicos**
Modo de trabalho	Selecione a partir de Password2 para Gestão de segredos Criptografe todos os campos password2 em seus grupos de segredos usando os módulos de criptografia definidos na política de acesso ao módulo de cada grupo. Gestão de segredos para Password2 Criptografe novamente os dados em seus grupos de segredos usando a criptografia de password2. Para obter detalhes sobre esta criptografia, consulte Criptografia de Password2 com KMF. Imposição do grupo secreto Consulta todos os dados que devem corresponder ao grupo selecionado no campo **Grupo secreto**. Se todos os dados encontrados pela consulta já estiverem no grupo, o trabalho não fará mudanças. Se a consulta encontrar dados que ainda não estão no grupo, o trabalho criptografará novamente esses dados no Grupo secreto. **Nota:** Se os dados encontrados nesta consulta já estiverem criptografados e suas instâncias não conseguirem descriptografar esses dados, eles não serão criptografados e adicionados ao grupo de segredos.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Grupo secreto	Grupo secreto que contém os segredos a serem criptografados. Este campo só está disponível quando o **Grupo secreto** for selecionado no campo **Modo de trabalho**.
Forçar rechaveamento de dados	
Resumo	Exibe informações sobre o andamento do trabalho. O resumo também exibe os registros que não puderam ser criptografados pelo trabalho.

4. Selecione **Enviar**.

O que Fazer Depois

O trabalho consulta todos os dados que devem corresponder ao grupo secreto selecionado. Se todos os dados encontrados pela consulta já estiverem no grupo, o trabalho não fará mudanças. Se a consulta encontrar dados que ainda não estão no grupo, o trabalho criptografará novamente esses dados no Grupo secreto. (Se a instância puder descriptografá-la, o que pode não ser o caso de segredos criptografados no lado do cliente).

Assinatura de código

A assinatura de código cria assinaturas digitais para que os dados que posteriormente serão verificados confirmem a autenticidade e a integridade dos dados. A assinatura de código é um módulo licenciado como um componente de ServiceNow Vault.

Assinatura de código e Círculo de confiança

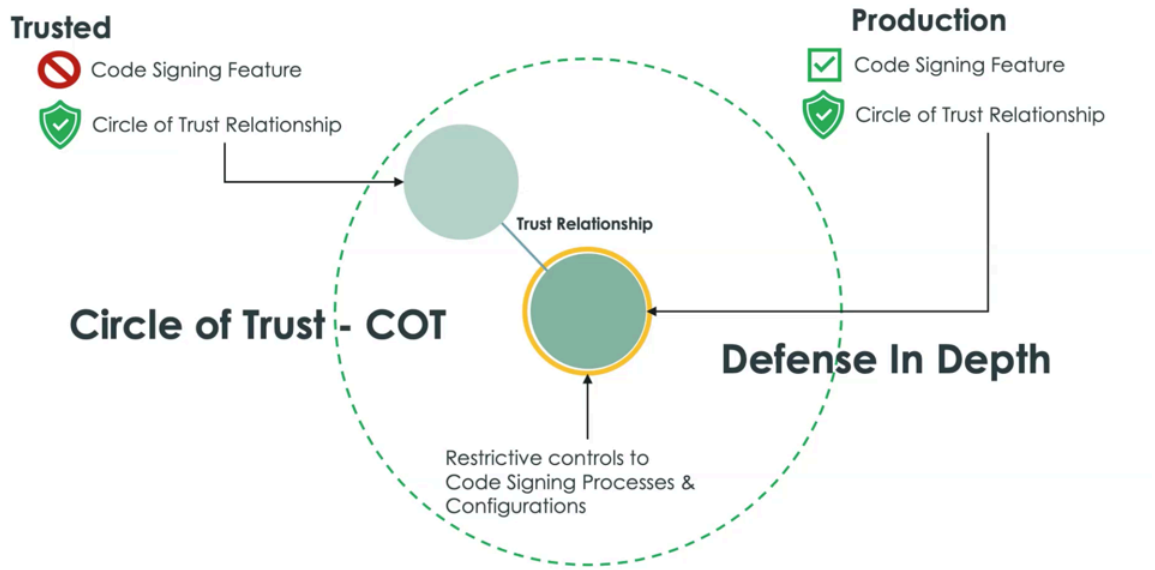
O Circle of Trust (COT) é um pré-requisito para a Assinatura de código que cria comunicação segura entre suas instâncias de produção confiáveis para assegurar que apenas usuários autorizados possam acessar o recurso de Assinatura de código.

Várias medidas de segurança ajudam a impedir que agentes mal-intencionados desabilitem ou usem indevidamente a assinatura de código caso uma instância de produção fique comprometida. Como parte da estratégia de defesa em profundidade, o COT usa os seguintes componentes:

- Controles que impedem até mesmo a mais poderosa conta de administrador são estabelecidos na instância de produção para ajudar a proteger os processos e a configuração da assinatura de código.
- As instâncias confiáveis devem funcionar juntamente com as instâncias de produção para estabelecer o relacionamento de Circle of Trust. É necessário ter pelo menos uma instância confiável, mas é possível configurar várias instâncias confiáveis para colaborar com a instância de produção.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

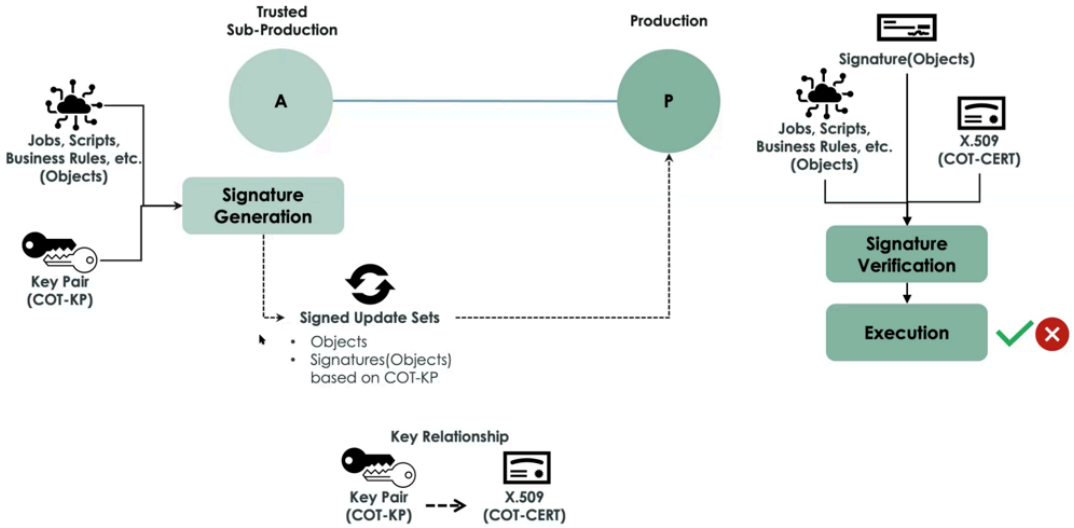
Visão geral do Círculo de confiança



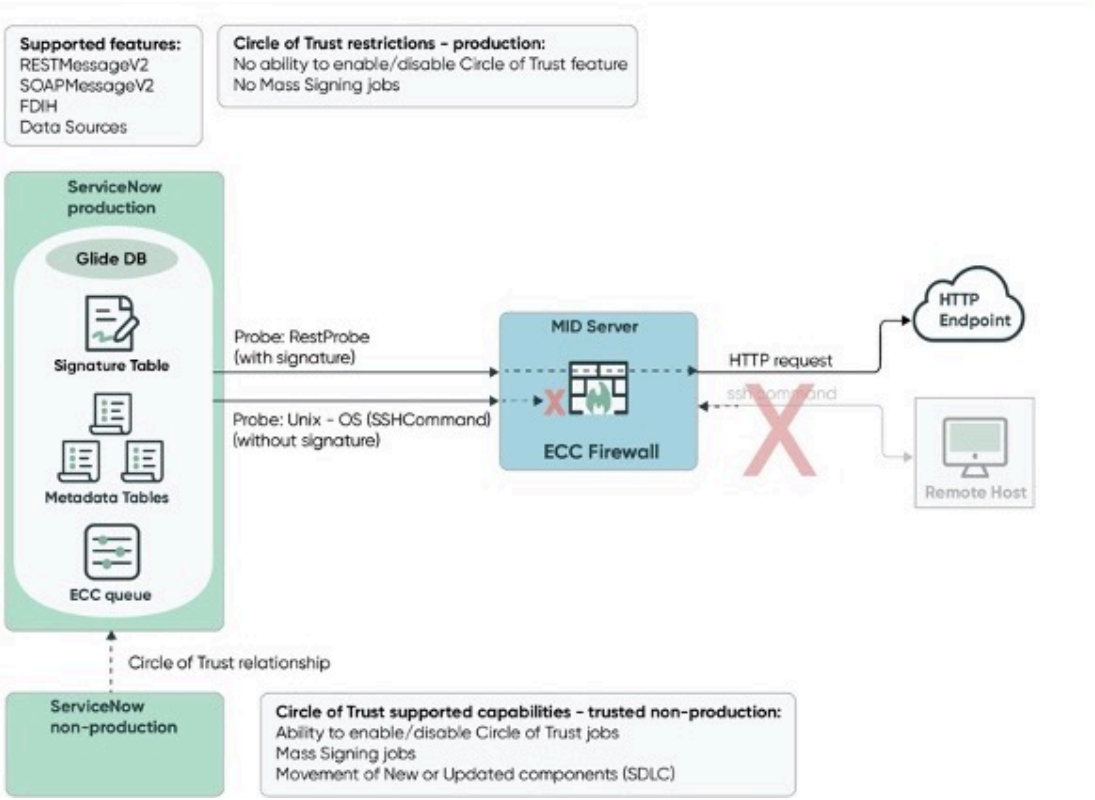
O Circle of Trust usa trabalhos, scripts e regras de negócios junto com um par de chaves para gerar assinaturas para assinar conjuntos para atualização para a instância de produção. Quando o trabalho é chamado, a assinatura é verificada junto com o certificado confiável para executar atualizações de instância de produção.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Processo de conjuntos para atualização confiáveis



Fluxo de Assinatura de código



O Circle of Trust requer um relacionamento de confiança inicial entre as instâncias confiáveis de produção que evita que qualquer usuário não autorizado com qualquer nível de autorização acesse atividades não aprovadas.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Iniciar

Explorar	Configurar	Referência
Saiba mais sobre os principais recursos e o valor comercial da Assinatura de código.	Ative e configure a Assinatura de código.	Veja os detalhes sobre propriedades e solução de problemas
	Usar Saiba como usar a Assinatura de código para ajudar a verificar a autenticidade e integridade dos seus dados.	

Solucionar problemas e obter ajuda

- https://www.servicenow.com/community/secops/ct-p/security-operations
- Pesquise artigos de erros conhecidos no portal de erros conhecidos
- ContatoSuporte e atendimento ao cliente

Explorando a assinatura de código

A assinatura de código pode ajudar a melhorar a segurança validando dados e scripts de configuração de aplicação confidenciais antes de serem usados.

A assinatura de código cria assinaturas digitais para os dados, que posteriormente são verificadas para confirmar a autenticidade e a integridade dos dados. A assinatura de código é um módulo licenciado como um componente de ServiceNow Vault.

Nota: A equipe Suporte e atendimento ao cliente deve conceder acesso à assinatura de código.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A assinatura de código declara a intenção por trás da operação que está sendo realizada e valida se o recurso ou registro pode ser usado para a finalidade pretendida. Para facilitar a assinatura de código, o Estrutura de gestão principal (KMF) usa certificados digitais e criptografia assimétrica padrão do setor para assinaturas digitais.

Use a assinatura de código internamente no lado da plataforma e infraestrutura. A assinatura de código fornece uma maneira de assinar o conteúdo de tabelas específicas ou de um subconjunto de registros em uma determinada tabela de metadados.

A assinatura de código usa um sinal seguro Circle of Trust (COT) entre suas instâncias confiáveis e de produção para garantir que apenas instâncias confiáveis autorizadas e seguras possam acessar o recurso de assinatura de código.

Casos de uso

A assinatura de código pode ser usada para operações com MID Server e Integration Hub. Notarização é o uso de assinatura de código para criar assinaturas digitais para registros de fila do ECC usados em operações do MID Server e operações do Integration Hub.

Por exemplo, uma inclusão de script gravada por ServiceNow para criar registros de fila do ECC no tempo de execução é assinada como "conteúdo do sistema de base". Isso é assinado como "emitido corretamente pela instância ServiceNow", em oposição a uma inserção na fila do ECC de um script em segundo plano ou outra origem que não esteja validada e assinada.

O Integration Hub pode usar a Assinatura de código para assinar o conteúdo dinâmico gerado na plataforma e validar as partes críticas dos dados da aplicação.

Dica:

Os carimbos de data/hora garantem que os registros assinados não expirem quando o certificado expirar, desde que o registro tenha sido assinado antes da expiração do certificado. Existe um período de carência de 4 horas em torno da janela de validade do certificado para garantir que as diferenças de tempo entre os servidores não invalidem os certificados intencionalmente.

Validação de assinatura de código e trabalhos

Todas as tabelas de metadados com configurações válidas são assinadas no momento da construção usando o plug-in de metadados Assinatura de códigos (*com.glide.code_signing*). Se você optar por assinar as tabelas, os usuários administradores com função de administrador de segurança terão acesso aos trabalhos de criptografia de assinatura de códigos:

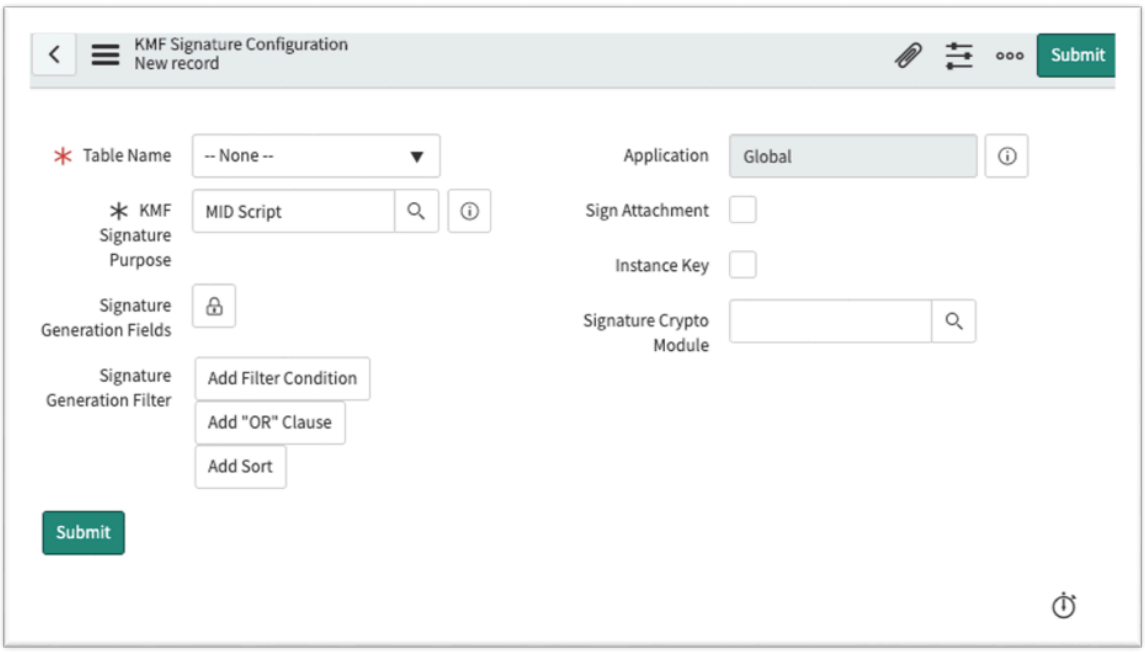
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Assinar conjuntos para atualização.
- Assinar registros em massa.
- Anexos de assinatura em massa.

Assinar conjunto de atualizações

Este trabalho assina os registros que correspondem a uma configuração de assinatura no conjunto de atualizações. O trabalho também adiciona todos os novos registros de assinatura e certificados de verificação no conjunto de atualizações.

Registro de assinatura KMF para o conjunto de atualizações



Assinar registros em massa

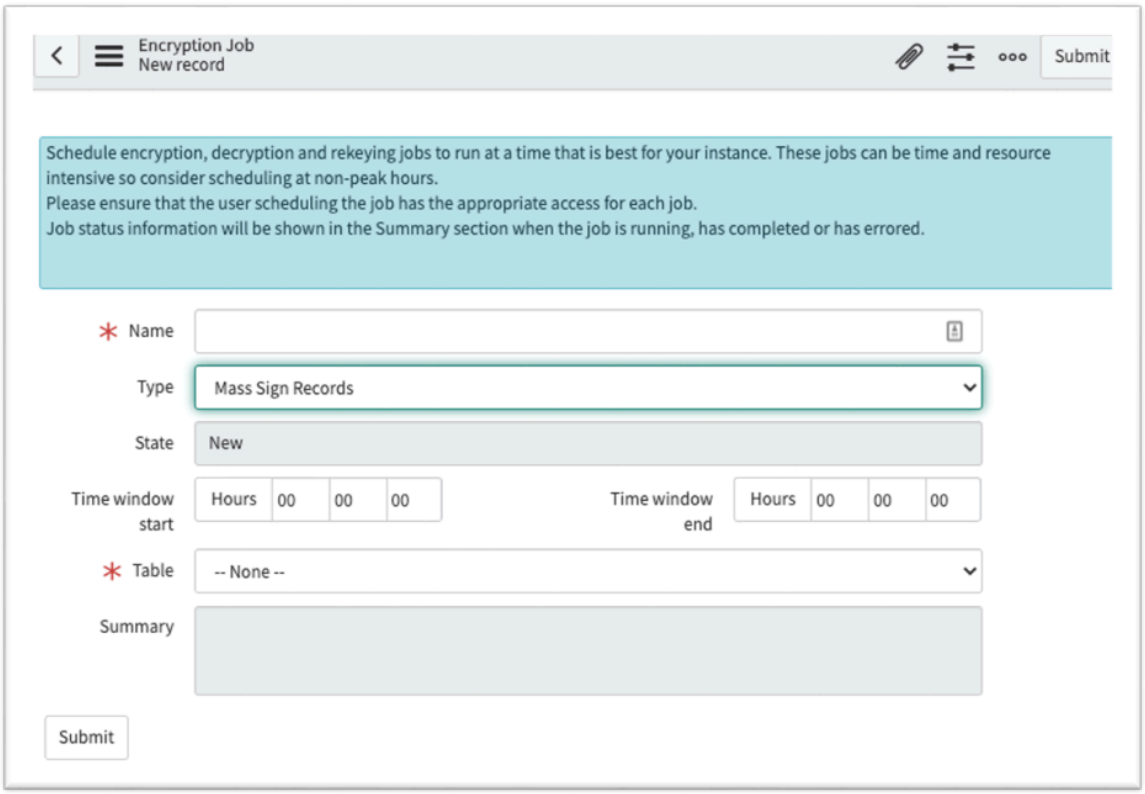
Este trabalho assina todos os registros que correspondem à configuração de assinatura aplicada em uma tabela de metadados específica.

Assinar anexos em massa

Esta tarefa assina todos os registros de anexo incluídos em uma tabela que corresponde a uma configuração de assinatura especificada.

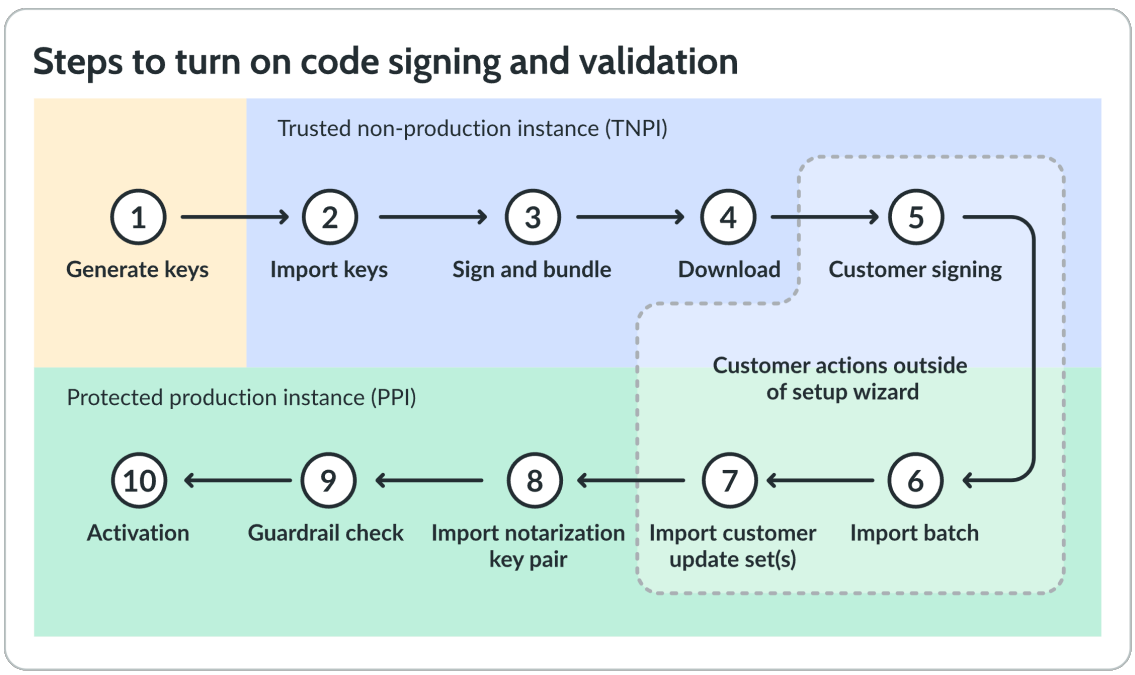
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Trabalho de criptografia para assinar registros em massa



Configuração da assinatura de código

Ative e configure a Assinatura de código para verificar a autenticidade e a integridade dos seus dados.



A Assinatura de código Enterprise requer um relacionamento de confiança inicial entre as instâncias confiáveis e de produção para evitar que qualquer usuário não autorizado com qualquer nível de autorização acesse atividades não aprovadas.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Consulte cada tópico para concluir as etapas de configuração para estabelecer o Circle of Trust com a Assinatura de código Enterprise:

Atribuição da função de Administrador da assinatura de código

Atribua a função de Administrador da assinatura de código a um usuário para que ele acesse a experiência de configuração da Assinatura de código.

Como configurar a Assinatura de código Enterprise em sua instância de não produção confiável

Ative a Assinatura de código em sua TNPI (Trusted Non-Production Instance, Instância de não produção confiável).

Como carregar seu arquivo de configuração de Assinatura de código na sua instância de produção protegida

Carregue o arquivo de configuração gerado em sua instância de não produção confiável.

Como configurar a Assinatura de código Enterprise em sua instância de produção protegida

Ative e configure a Assinatura de código em sua PPI (Protected production instance, instância de produção protegida).

Como ativar a validação de certificados

Ative a validação de certificado em sua instância.

Como desativar a Assinatura de código

Desative a Assinatura de código em sua PPI.

Nota: Essa etapa opcional não faz parte da configuração inicial da Assinatura de código

Como atribuir a função de Administrador da assinatura de código

Atribua a função de Administrador da assinatura de código a um usuário para que ele acesse a experiência de configuração da Assinatura de código.

Antes de Iniciar

Funções necessárias:

- administrador
- security_admin

Importante: O usuário designado à função de Administrador da assinatura de código deve estar no escopo "Global".

Procedimento

1. Selecione uma instância de não produção para usar como sua TNPI (Trusted Non-Production Instance, Instância de não produção confiável).
   Usa-se a TNPI para criar trabalhos, assinar registros e realizar outras tarefas necessárias antes de ativar a validação de assinatura em sua PPI (Protected Production Instance, Instância de produção protegida).
2. Navegue até **Todos** > **Assinatura de código** > **Administração da função de assinatura de código**.
3. Conceda a um usuário a função de Administrador de assinatura de código movendo-o da lista **Usuários disponíveis** para a lista **Usuários selecionados**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Selecione **Salvar**.

> **Importante:** O usuário designado à função deve se desconectar e fazer login novamente para realizar as tarefas de Assinatura de código.

Resultados
O usuário selecionado tem a função de Administrador da assinatura de código. Um usuário com essa função pode acessar a experiência de configuração da Assinatura de código e atribuir outras funções de Assinatura de código aos usuários.

Para saber mais sobre as funções de Assinatura de código, consulte Funções instaladas com a Assinatura de código.

Como configurar a Assinatura de código Enterprise em sua instância de não produção confiável

Ative e configure a Assinatura de código em sua TNPI (Trusted Non-Production Instance, Instância de não produção confiável).

Antes de Iniciar
Funções necessárias:

- administrador
- security_admin
- codesigning_admin

> **Nota:** É possível designar a função codesigning_admin usando o processo detalhado em Como atribuir a função de Administrador da assinatura de código.

- sn_kmf.cryptographic_manager

É necessário ter pelo menos um par de chaves criptográficas e um certificado (extensão de arquivo p12) para assinatura do cliente e administração do COT (Circle of Trust). Para melhorar a segurança, considere o uso de pares de chaves criptográficas separadas para assinatura do cliente e para administração do COT.

> **Aviso:** Depois de concluir esse processo, você terá baixado um arquivo de configuração que precisa instalar na sua PPI em até uma hora. Verifique se você tem tempo disponível após esse processo para carregar o arquivo de configuração na sua instância de produção. Para obter detalhes sobre esse processo, consulte Como carregar seu arquivo de configuração de Assinatura de código na sua instância de produção protegida.

Procedimento

1. Na sua TNPI, navegue até **Todos** > **Assinatura de código** > **Configuração de assinatura de código** para abrir a página de configuração da Assinatura de código.
2. No campo **Tipo de instância**, selecione **Instância de não produção confiável**.
3. Selecione o botão **Avançar**.
4. No campo **Ação**, em **Selecione a ação que você deseja realizar**, selecione **Ativar assinatura de código**.
5. Ao lado de **Anexos** na seção **Par de chaves de assinatura do cliente e certificado**, selecione **+Adicionar arquivo** para carregar um par de chaves criptográficas (extensão de arquivo p12) para usar como assinatura do cliente.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

> **Dica:** Se a opção **+Adicionar arquivo** não estiver disponível, verifique se você está no escopo "Global" e se tem a função sn_kmf.cryptographic_manager.

6. No campo **Senha**, digite a senha do par de chaves carregado.
7. Selecione **Importar**.
8. Selecione **Continuar** para avançar para a próxima seção.
9. Ao lado de **Anexos** na seção **Certificado e par de chaves de administração de COT**, selecione **+Adicionar arquivo** para carregar um par de chaves criptográficas (extensão de arquivo p12) que será usado para assinatura do cliente.
10. No campo **Senha**, digite a senha do par de chaves carregado.
11. Selecione **Importar**.
12. Selecione **Continuar** para avançar para a próxima seção.
13. Na seção **Executar tarefas de não produção confiáveis**, aguarde a conclusão de todas as tarefas.

    Sua instância gerará e executará essas tarefas automaticamente. Se você usou a Assinatura de código antes da versão Vancouver, as tarefas serão criadas e executadas para atualizar suas assinaturas.

    Em alguns casos, nenhuma tarefa é necessária. **Nenhuma tarefa necessária** será exibida nesta página.
14. Selecione **Continuar** para avançar para a próxima seção.
15. Na página **Exportar arquivo de configuração**, selecione **Exportar** para criar e baixar um arquivo de configuração usado para ativar a Assinatura de código em sua instância de produção protegida.
    O processo de exportação baixará um arquivo XML em sua máquina local para uso nos detalhes de etapas de Como configurar a Assinatura de código Enterprise em sua instância de produção protegida.

Como carregar seu arquivo de configuração de Assinatura de código na sua instância de produção protegida

Carregue o arquivo de configuração gerado em sua instância de não produção confiável.

Antes de Iniciar

Funções necessárias:

- administrador
- security_admin
- codesigning_admin

> **Nota:** É possível designar a função codesigning_admin usando o processo detalhado em Como atribuir a função de Administrador da assinatura de código.

- sn_kmf.cryptographic_manager

Você também precisa do arquivo de configuração gerado nas etapas detalhadas em Como configurar a Assinatura de código Enterprise em sua instância de não produção confiável.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegue até **Todos** > **Conjuntos de atualizações do sistema** > **Conjuntos de atualizações recuperados**.
2. Na parte inferior da lista **Conjuntos de atualizações**, selecione **Importar conjunto de atualizações do XML**.
3. Selecione **Escolher arquivo** e selecione seu arquivo de configuração (extensão de arquivo xml).
4. Selecione **Carregar**.
   Você deve ver o conjunto de atualizações de **Configuração da assinatura de código** na lista **Conjuntos de atualizações recuperados**.
5. Selecione e abra o conjunto de atualizações **configuração da assinatura de código**.
6. Selecione **Visualizar lote de conjunto de atualizações**.
   Se ocorrer algum conflito durante a visualização, resolva-o selecionando **Aceitar atualização remota** ou **Resolver conflitos conhecidos de CS**.
7. Depois de resolver todos os conflitos, selecione **Confirmar lote de conjunto de atualizações**.

Como configurar a Assinatura de código Enterprise em sua instância de produção protegida

Ative e configure a Assinatura de código em sua PPI (Protected production instance, instância de produção protegida).

Antes de Iniciar

Funções necessárias:

- administrador
- security_admin
- codesigning_admin

> **Nota:** É possível designar a função codesigning_admin usando o processo detalhado em Como atribuir a função de Administrador da assinatura de código.

- sn_kmf.cryptographic_manager

Procedimento

1. Na PPI, navegue até **Todos** > **Assinatura de código** > **Configuração de assinatura de código** para abrir a página de configuração da Assinatura de código.
2. No campo **Tipo de instância**, selecione **Instância de produção protegida**.
3. Selecione o botão **Avançar**.
4. Marque a caixa de seleção **Confirme se a atualização definida de configuração da Assinatura de código foi importada e confirmada**.
5. Selecione o botão **Avançar**.
6. Aguarde a conclusão da instalação do certificado.
   Uma mensagem de alerta em azul será exibida, indicando que os itens do arquivo de configuração estão em instalação. O alerta desaparecerá em alguns segundos, após a conclusão da instalação.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

7. Ao lado de **Anexos** na seção **Par de chaves e certificado para notarização/execução**, selecione **+Adicionar arquivo** para carregar um par de chaves criptográficas (extensão de arquivo p12) que será usado para fins de tempo de execução/notarização.
   É possível reutilizar um par de chaves da TNPI (Trusted Non-Production Instance, instância de não produção confiável) ou carregar um novo especificamente para esse uso.

   Dica: Se a opção **+Adicionar arquivo** não estiver disponível, verifique se você está no escopo "Global" e se tem a função sn_kmf.cryptographic_manager.

8. No campo **Senha**, digite a senha do par de chaves carregado.
9. Selecione **Importar**.
10. Selecione **Continuar** para passar para a próxima seção.
11. Aguarde enquanto a instância realiza uma verificação da proteção.
    Essa verificação analisa a instância em busca de assinaturas inválidas e a conclusão dela pode levar algum tempo. Não saia da página nem a atualize antes da conclusão da verificação.
12. Se a verificação encontrar assinaturas inválidas, selecione **Baixar relatório**.

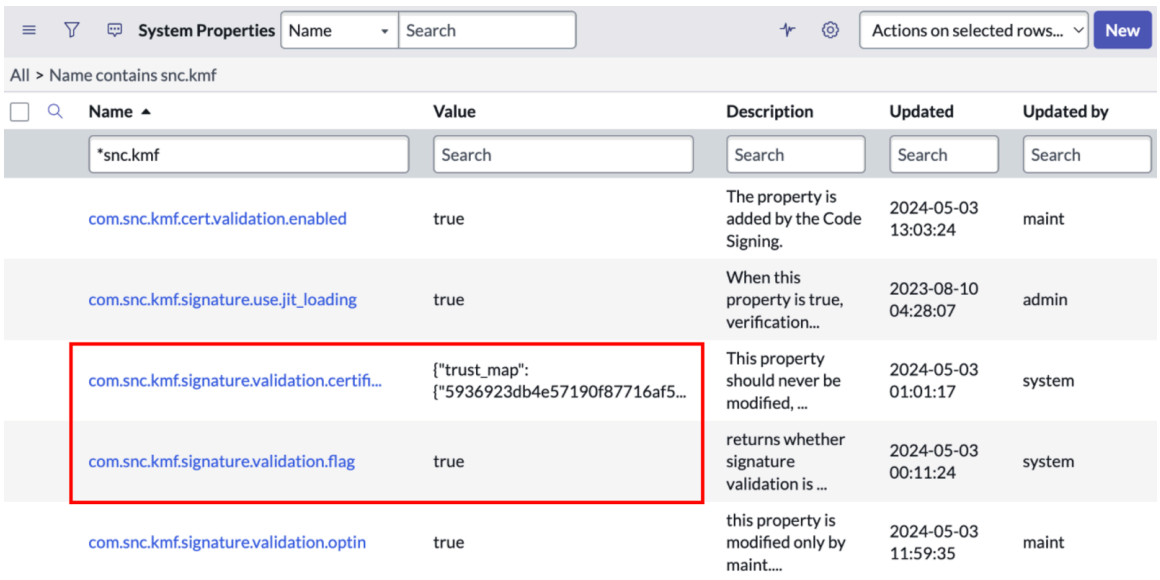
    Selecionar **Baixar relatório** fará download de um relatório (`scan_report.txt`) que você pode usar para investigar e corrigir as assinaturas inválidas.

    Depois de resolver os erros, atualize a página para executar a verificação novamente.

13. Se não houver erros, selecione **Concluir a configuração**.
14. Aguarde a conclusão dos trabalhos de configuração.
    A instância executará um ou mais trabalhos para concluir o processo de configuração. Não saia da página nem a atualize até a conclusão dos trabalhos. Ao terminar, você verá uma mensagem **Configuração de Assinatura de código concluída com sucesso**.

Resultados

Agora, a validação da assinatura é imposta na sua instância de produção. É possível verificar a conclusão bem-sucedida analisando as propriedades do sistema. Procure a propriedade **com.snc.kmf.signature.validation.flag** na tabela "Propriedades do sistema" [sys_property] e verifique se ela tem um valor **verdadeiro**. Verifique se a propriedade **com.snc.kmf.signature.validation.certificate_trust** não tem um valor vazio.



© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Como ativar a validação de certificados

Proteja sua instância com a validação baseada em certificado.

Antes de Iniciar

Função necessária:

- codesigning_admin
- security_admin
- sn_kmf.cryptographic_manager

Procedimento

1. Em sua TNPI (Trusted Non-Production Instance, instância de não produção confiável), navegue até **Todos** > **Assinatura de código** > **Configuração da assinatura de código** para abrir a página "Configuração da assinatura de código".
2. No campo **Tipo de instância**, selecione **Instância de não produção confiável**.
3. Selecione o botão **Avançar**.
4. No campo **Ação**, em **Selecione a ação que você deseja realizar**, selecione **Ativar validação de certificado**.
5. Selecione o botão **Avançar**.
6. Ao lado de **Anexos** na seção **Par de chaves de assinatura do cliente e certificado**, selecione **+Adicionar arquivo** para carregar um par de chaves criptográficas (extensão de arquivo p12) para usar como assinatura do cliente.

   Dica: Se a opção **+Adicionar arquivo** não estiver disponível, verifique se você está no escopo "Global" e se tem a função sn_kmf.cryptographic_manager.

7. No campo **Senha**, digite a senha do par de chaves carregado.
8. Selecione **Importar**.
9. Selecione **Continuar** para avançar para a próxima seção.
10. Ao lado de **Anexos** na seção **Certificado e par de chaves de administração de COT**, selecione **+Adicionar arquivo** para carregar um par de chaves criptográficas (extensão de arquivo p12) que será usado para assinatura do cliente.
11. No campo **Senha**, digite a senha do par de chaves carregado.
12. Selecione **Importar**.
13. Selecione **Continuar** para avançar para a próxima seção.
14. Na seção **Executar tarefas de não produção confiáveis**, aguarde a conclusão de todas as tarefas.

    Sua instância gerará e executará essas tarefas automaticamente. Se você usou a Assinatura de código antes da versão Vancouver, as tarefas serão criadas e executadas para atualizar suas assinaturas.

    Em alguns casos, nenhuma tarefa é necessária. **Nenhuma tarefa necessária** será exibida nesta página.

15. Selecione **Continuar** para avançar para a próxima seção.
16. Na página **Exportar arquivo de configuração**, selecione **Exportar** para criar e baixar um arquivo de configuração usado para ativar a Assinatura de código em sua instância de produção protegida.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O processo de exportação baixará um arquivo XML em sua máquina local para uso nas etapas detalhadas em Como configurar a Assinatura de código Enterprise em sua instância de produção protegida.

17. Em sua PPI (Protected Production Instance, instância de produção protegida), navegue até **Todos** > **Conjuntos de atualizações do sistema** > **Conjuntos de atualizações recuperados**.
18. Na parte inferior da lista **Conjuntos de atualizações**, selecione **Importar conjunto de atualizações do XML**.
19. Selecione **Escolher arquivo** e selecione seu arquivo de configuração (extensão de arquivo xml).
20. Selecione **Carregar**.
21. Retorne à página de configuração da assinatura de código em **Todos** > **Assinatura de código** > **Configuração da assinatura de código**.
22. Use o assistente para concluir a configuração, selecionando as opções para concluir a ativação da validação de certificado.

Como desativar a Assinatura de código

Desative a assinatura de código em sua PPI (Protected Production Instance, instância de produção protegida).

Antes de Iniciar

Função necessária: administrador, codesigning_admin

Procedimento

1. Em sua TNPI (Trusted Non-Production Instance, instância de não produção confiável), navegue até **Todos** > **Assinatura de código** > **Configuração da assinatura de código** para abrir a página "Configuração da assinatura de código".
2. No campo **Tipo de instância**, selecione **Instância de não produção confiável**.
3. Selecione o botão **Avançar**.
4. No campo **Ação**, em **Selecione a ação que você deseja realizar**, selecione **Desativar a assinatura de código**.
5. No painel **Exportar arquivo de configuração**, selecione **Exportar** para baixar o conjunto de atualizações.
   O processo de exportação baixará um arquivo XML na sua máquina local para uso nas próximas etapas.
6. Selecione **Concluído**.
7. Faça login na sua PPI.
8. Carregue seus arquivos de configuração usando as etapas de Como carregar seu arquivo de configuração de Assinatura de código na sua instância de produção protegida.
9. Navegue até **Todos** > **Assinatura de código** > **Configuração da assinatura de código** para abrir a página "Configuração da assinatura de código".
10. No campo **Tipo de instância**, selecione **Instância de produção protegida**.
11. Selecione o botão **Avançar**.
12. Marque a caixa de seleção **Confirme se a atualização definida de configuração da Assinatura de código foi importada e confirmada**.
13. Selecione o botão **Avançar**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

14. Aguarde a conclusão da instalação do certificado.
    Após a conclusão, uma mensagem **Conclusão com sucesso da configuração de assinatura de código** será exibida.

Resultados

É possível verificar a conclusão bem-sucedida analisando as propriedades do sistema. Procure a propriedade **com.snc.kmf.signature.validation.flag** na tabela "Propriedades do sistema" [sys_property] e verifique se ela tem um valor **falso**.

Carregar pares de chaves e certificados necessários para a assinatura de código

Estabeleça o relacionamento em uma instância de não produção designada usando a assinatura de código. Esta primeira etapa carrega duas chaves criptográficas no ambiente de não produção para estabelecer uma fonte confiável de atualizações para a instância de produção.

Antes de Iniciar

Funções necessárias: security_admin e sn_kmf.cryptographic_manager

Por Que e Quando Desempenhar Esta Tarefa

A primeira etapa em estabelecer o relacionamento é estabelecer a fundação confiável em uma instância designada de não produção usando a assinatura de código. Para executar esta tarefa:

- É necessário ter um par de chaves público/privado RSA de 4096 bits para carregar nos módulos criptográficos de assinatura de código:
  - Um par para o módulo criptográfico cm_code_signing
  - Um par para o módulo criptográfico cm_code_attest

  Para obter mais informações sobre essas chaves, consulte Criar pares de chaves e certificados de assinatura de código.

  > **Importante:** Esses pares de chave devem ser assinados por uma autoridade de certificação pública ou assinado pela autoridade de certificação interna da sua organização. O certificado não pode ser autoassinado.

- Um arquivo .p12 (Public Key Cryptography Standard #12) que contém seus certificados finais e intermediários.

Procedimento

1. Importe suas chaves do armazenamento de chaves.
   a. Navegue até **Todos** > **Gerenciamento de chaves** > **Módulos criptográficos** > **Todos**.
   b. Encontre e abra o módulo criptográfico chamado `cm_code_signing`.
   c. Na lista **Especificações de criptografia**, clique no nome da especificação criptográfica para abri-la.
   d. Na tela **Importar chave do armazenamento de chaves**, selecione **"Importar chave"**.
2. Repita a primeira etapa para importar o módulo criptográfico chamado `cm_code_attest`.
3. No campo **Inserir senha de armazenamento de chaves**, insira a senha de desafio que você criou quando gerou seu certificado RSA.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: A senha de desafio que você criou é chamada aqui de **senha de armazenamento de chaves**. Em outras partes do processo, isso pode ser chamado de **senha de importação** ou **senha de exportação**. Se necessário, essa senha é a mesma do desafio que você criou nas etapas anteriores.

4. Selecione o botão **Procurar** ao lado de **Importar armazenamento de chaves/Certificado**.
5. Selecione um arquivo .p12 que contenha seu certificado de distribuição (mencionado na seção "Antes de começar", na parte superior deste documento).
6. Selecione **OK**.

Importante: Se você estiver usando uma autoridade de certificação própria, carregue os certificados intermediários da autoridade de certificação usando o processo das etapas 5 a 6.

Com uma importação bem-sucedida da sua chave e do certificado(s), será exibida uma mensagem de confirmação.

Você pode validar se a chave e os certificados estão presentes em sua instância na tabela Certificados X.509 [sys_certificate]. Esses registros têm um tipo de **Trust Store Certificate**.

Você pode validar sua chave na tabela Módulos criptográficos [sys_kmf_crypto_module].

O que Fazer Depois

Exporte o certificado para produção. Consulte Preparar certificados do Círculo de confiança para obter detalhes.

Preparar certificados do Círculo de confiança

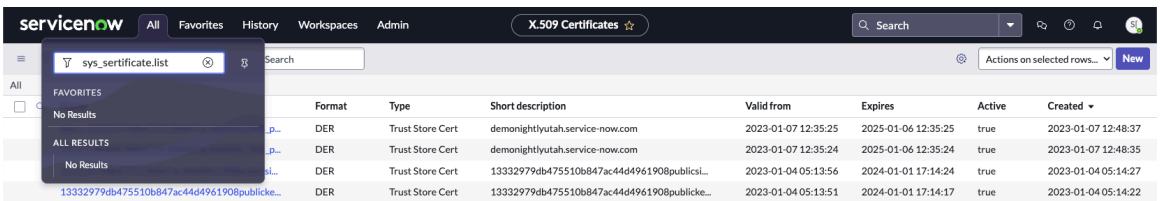
Crie um conjunto para atualização no ambiente confiável para exportar o certificado confiável para o ambiente de produção.

Antes de Iniciar

Funções necessárias: administrador, security_admin

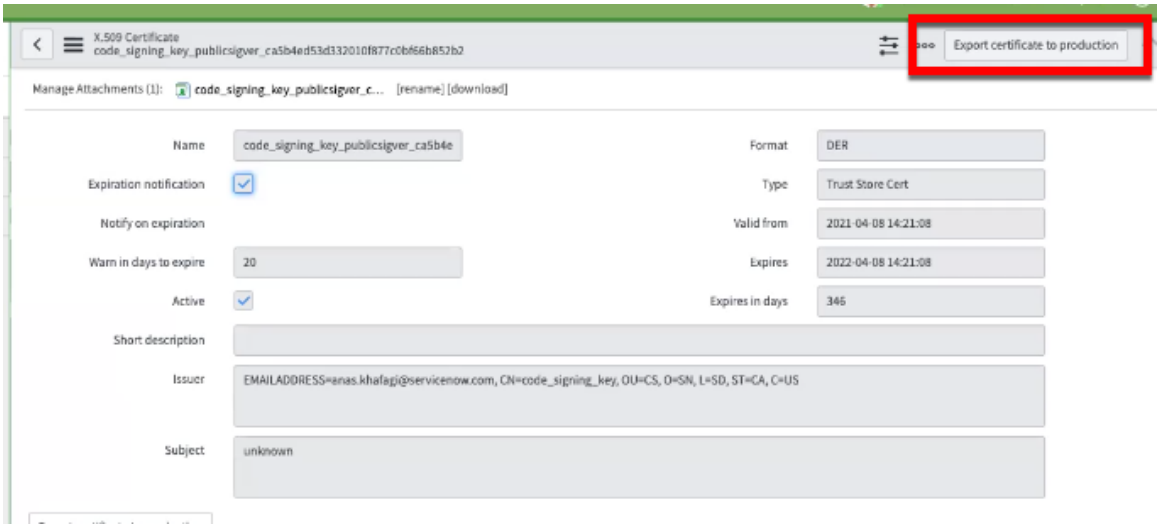
Procedimento

1. No ambiente confiável, navegue até **sys_certificate.list** .



2. Abra o Certificado X.509 criado mais recentemente que foi gerado com o tipo **Certificado de armazenamento confiável**.
   Pode ser necessário adicionar o campo **Criado** à lista para encontrar o registro mais recente. Consulte Listas pessoais .
3. Selecione **Exportar certificado para produção**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



É criada uma assinatura com o certificado.

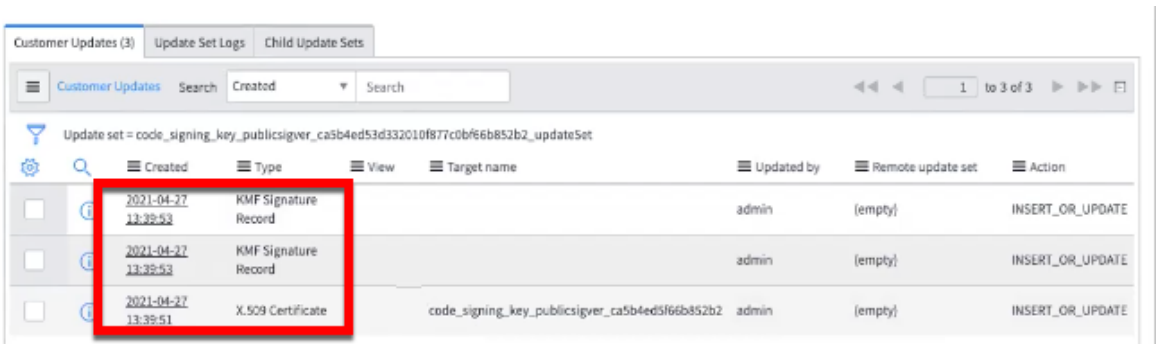
4. Navegue até **Conjuntos de atualizações do sistema** > **Conjuntos de atualizações locais**.
5. Encontre e abra a atualização de assinatura de código.

   Esta atualização começará com o texto `code_signing_key_publicsigver`.

   Um novo registro de conjunto para atualização de assinatura de código foi criado pelas etapas anteriores. Para encontrar este registro, classifique a lista usando o campo **Criado por** e procure os registros com o campo **Nome**.

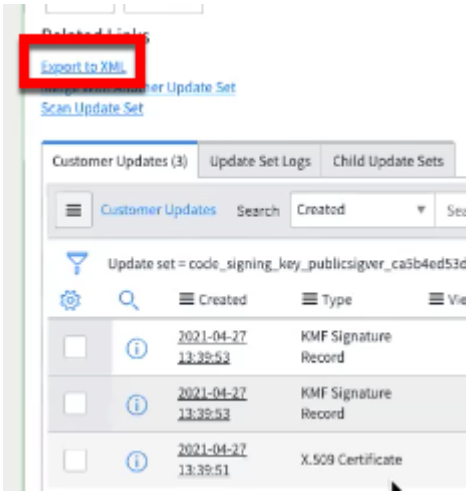
6. Exiba os Registros de assinatura relevantes e o certificado X.509.

   O conjunto de atualizações inclui o anexo para o registro de assinatura junto com a entrada da assinatura na tabela e o certificado.



7. Selecione o link relacionado **Exportar para XML**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



8. Recupere o conjunto de atualizações na produção.
   Consulte Recuperar um conjunto de atualizações para obter detalhes.

> **Importante:** Repita essas etapas para o segundo par de chaves. Lembre-se de que há uma chave para os módulos criptográficos cm_code_attest e cm_code_signing.

Importar e instalar certificados para o Círculo de confiança

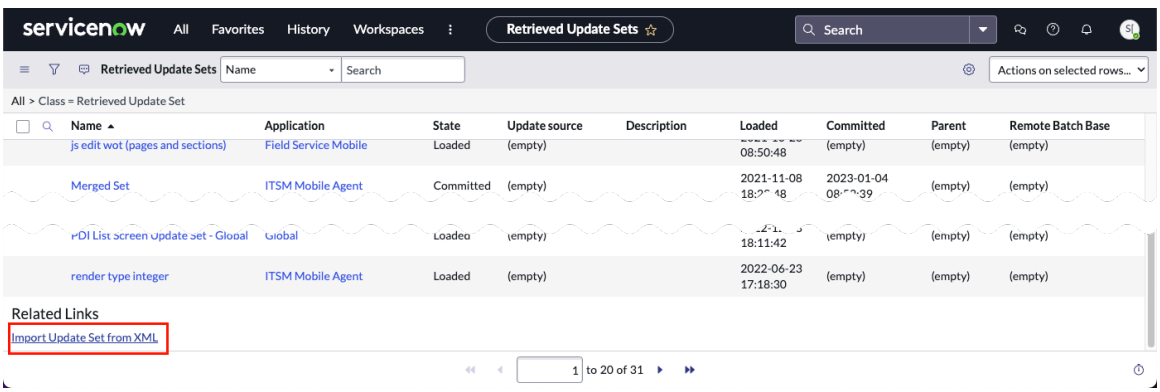
Recupere o conjunto para atualizações na produção para estabelecer o relacionamento de confiança entre as duas instâncias. Os certificados que foram criados para representar confiança na instância confiável devem ser aceitos na instância de produção.

Antes de Iniciar

Funções necessárias: administrador, security_admin

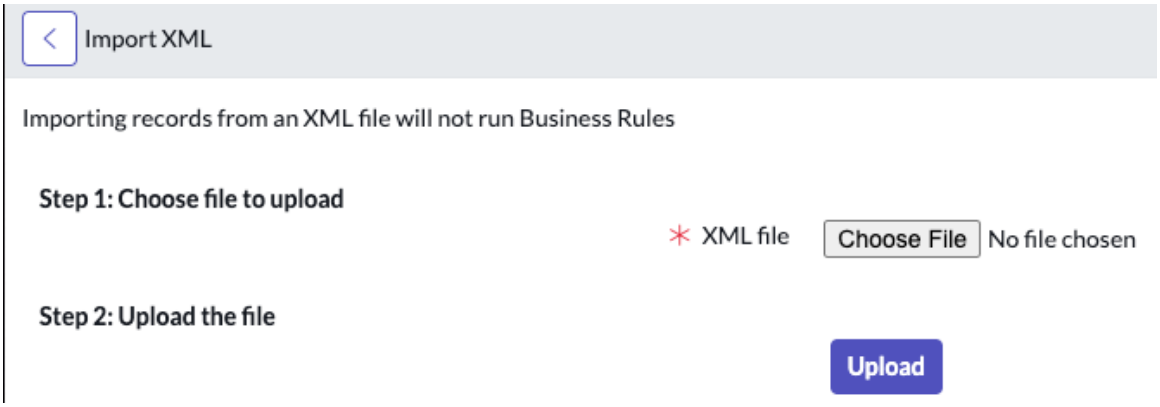
Procedimento

1. Na instância de produção, navegue até **Conjuntos de atualizações do sistema** > **Conjuntos de atualizações recuperados**.
2. Selecione o botão **Importar conjuntos para atualização de XML** no canto inferior esquerdo da tela.

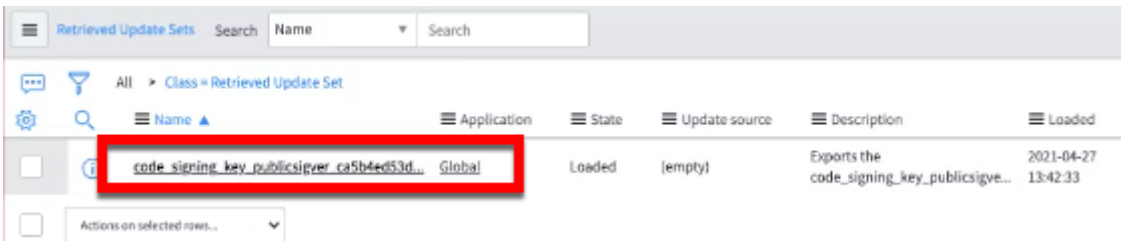


3. Clique em **Escolher arquivo** e navegue para selecionar o arquivo XML que você exportou em Preparar certificados do Círculo de confiança.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

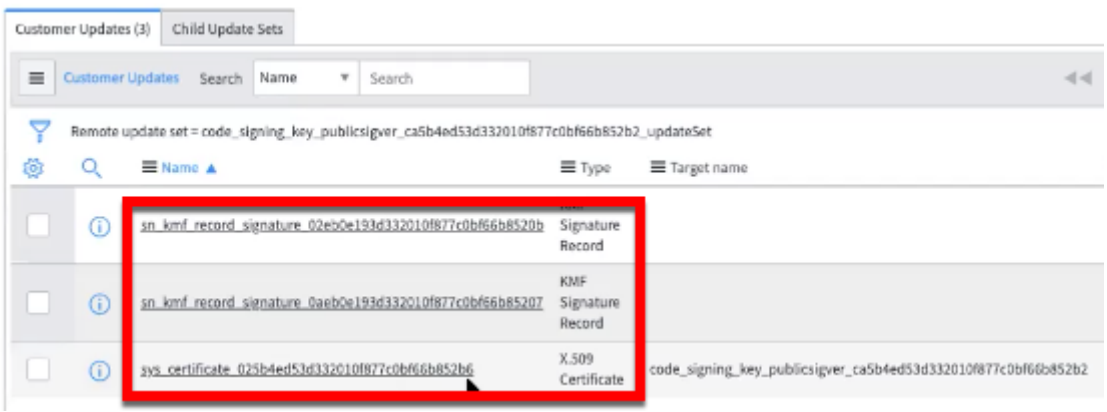


4. Selecione **Carregar**.
   O conjunto de atualizações de assinatura de código é adicionado à tabela conjuntos para atualização recuperados.



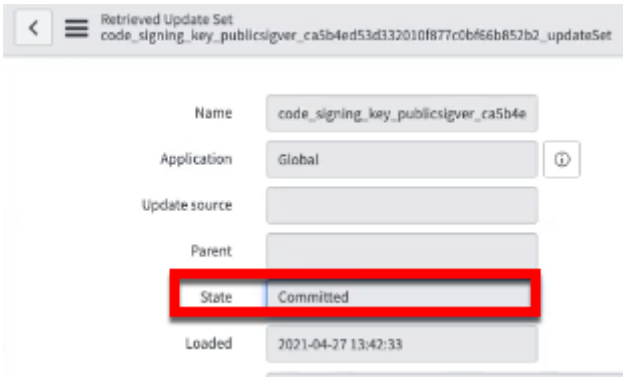
Nota: Se você não encontrar seu conjunto para atualização, filtre sua lista para registros no estado Carregado e classifique a lista pelo campo **Carregado**.

5. Abra o registro do conjunto de atualizações para verificar se a tabela Atualizações do cliente contém os três registros a seguir:
   - Dois registros de assinatura KMF
   - Certificado X.509



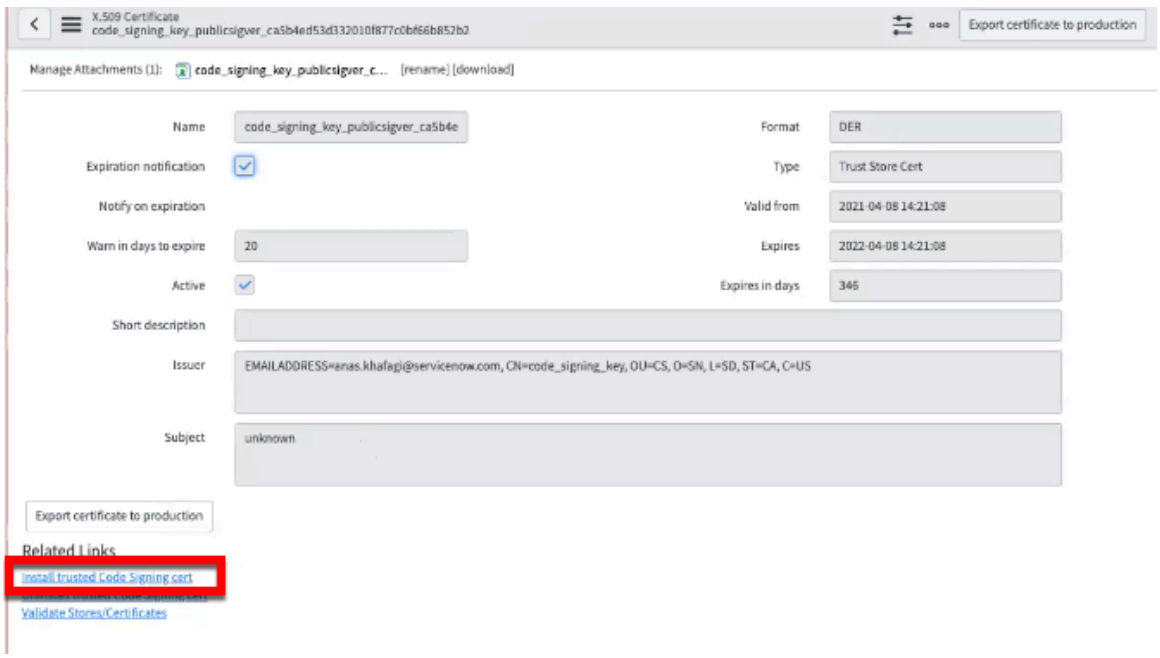
6. Selecione **Visualizar Conjunto para atualização**.
7. Clique em **"Confirmar Update Set"**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



O **Estado** Update Set recuperado é atualizado para Confirmado.

8. No navegador, insira `sn_kmf_record_signature.list` para abrir a lista **Registros de assinatura KMF**.
9. Localize os dois registros de assinatura KMF.
   Estes são os registros criados mais recentemente onde o campo **Finalidade da assinatura KMF** tem um valor de `Círculo de confiança`. Pode ser necessário adicionar o campo **Criado** à sua lista ou filtrar os registros criados na data atual.
10. No navegador, insira `sys_certificate.list` e abra o registro com um valor **Descrição resumida** de *`code_signing_key`* e um valor **Tipo** de `Certificado de armazenamento de confiança`.
11. Selecione **Instalar certificado de assinatura de código confiável**.



O tipo de certificado é atualizado para *`Certificado CodeSigning confiável`*.

> **Importante:** Repita essas etapas para o seu segundo certificado. Lembre-se de que há um certificado para os módulos criptográficos cm_code_attest e cm_code_signing.

Resultados

O relacionamento de confiança agora é estabelecido entre instâncias confiáveis e de produção. Você está pronto para habilitar a assinatura de código. Consulte Ativar a Assinatura de código para concluir as etapas.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Ativar a Assinatura de código

Ative a assinatura de código na sua instância confiável de não produção para identificar as instâncias confiáveis vinculadas à sua instância de produção.

Antes de Iniciar

Funções necessárias: security_admin e sn_kmf.crypto_manager ou sn_kmf.admin

Entre em contato com a equipe de Suporte e atendimento ao cliente para ativar o plug-in [com.glide.code_signing] da estrutura de Assinatura de código, antes de habilitá-la.

Por Que e Quando Desempenhar Esta Tarefa

Os trabalhos da Assinatura de código com conjuntos para atualização assinados são usados para ativar e desativar o recurso Assinatura de código. Não há outro método para esta funcionalidade. Este processo inclui o seguinte:

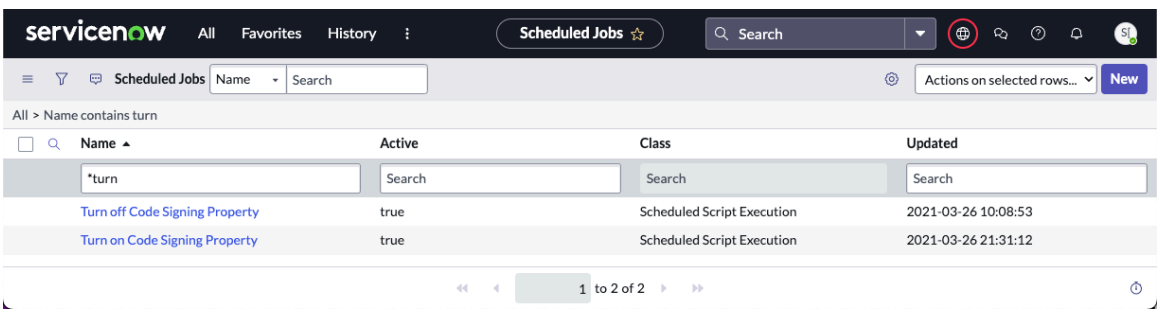
- Crie dois trabalhos de Assinatura de código na instância confiável: um para ativar a Assinatura de código e um para desativar a Assinatura de código.
  - O trabalho agendado **Ativar** inicia o processo de validação do MID Server de código assinado.
  - O trabalho agendado **Desativar** para a validação do MID Server de código assinado.

  Nota: Ao desligar a Assinatura de código, a propriedade do sistema é marcada como **falsa**, mas a lista de amigos confiáveis de Assinatura de código ainda está disponível.

- Coloque o trabalho **Ativar propriedade de assinatura de código** em um conjunto de atualizações.
- Traga o trabalho para produção.
- Use o trabalho **Ativar propriedade de assinatura de código** em produção se a assinatura for verificada como originada de uma instância confiável.

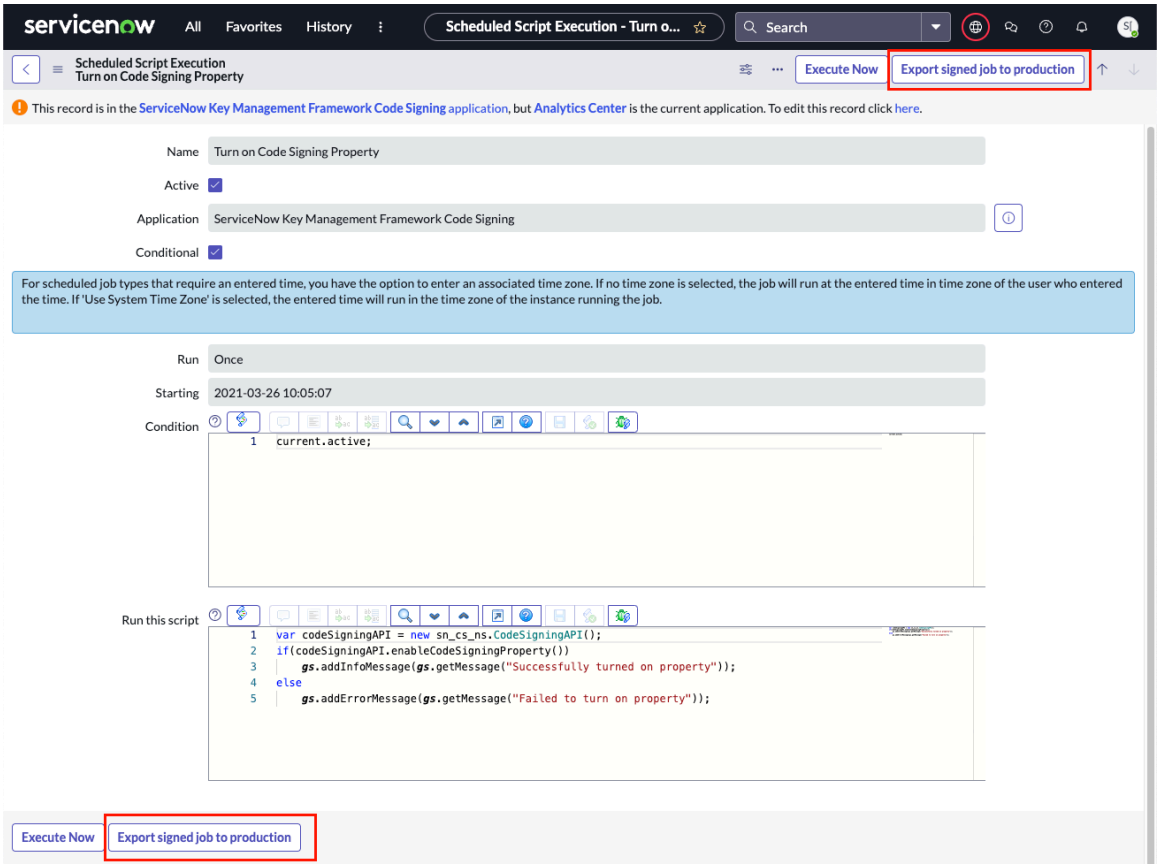
Procedimento

1. Na sua instância confiável, navegue até **Todos** > **Definição do sistema** > **Trabalhos agendados**.
2. Pesquise "*Turn" no campo de nome.
3. Selecione **Ativar propriedade de Assinatura de código**.



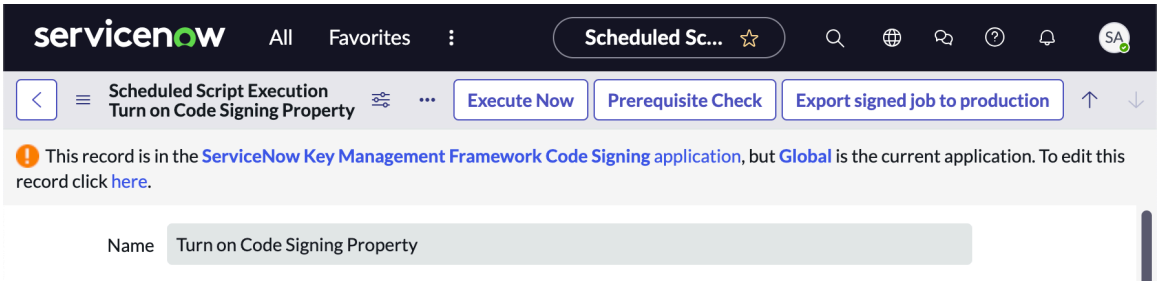
O formulário **Execução de script agendada** é carregado. Este formulário contém informações para habilitar a propriedade Assinatura de Código. Os trabalhos criam conjuntos para atualização que contêm os trabalhos e as assinaturas validadas por meio do processo de assinatura de código.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Para executar o script imediatamente, assine o certificado, crie o conjunto para atualização e selecione **Exportar trabalho assinado para produção**.
   Também é possível configurar o script para ser executado em uma programação designada.
5. Navegue até **Conjuntos de atualizações do sistema** > **Conjuntos de atualizações locais**.
6. Abra cada um dos conjuntos para atualização da propriedade de Assinatura de código e selecione **Exportar para XML**.
7. Faça login na instância de produção.
8. Navegue até **Conjuntos de atualizações do sistema** > **Conjuntos de atualizações recuperados**.
9. Selecione o botão **Importar conjunto de atualizações do XML** e selecione o conjunto de atualizações da propriedade de Assinatura de código.
10. Selecione **Escolher arquivo** e carregue e confirme os conjuntos para atualização.
11. Retorne à lista de trabalhos agendados navegando até **Todos** > **Definição do sistema** > **Trabalhos agendados**.
12. Abra o registro de trabalho **Ativar propriedade de assinatura de código**.
13. Selecione o botão **Verificação de pré-requisito** na parte superior do formulário.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



14. Selecione o botão **Executar agora** após a conclusão da verificação de pré-requisito. O trabalho agendado **Ativar propriedade de assinatura de código** inicia o processo de validação MID Server de código assinado.
15. No navegador, insira `sn_kmf_record_signature.list` para abrir a lista **Registros de assinatura KMF** e filtrar os registros nos quais a **Finalidade de assinatura KMF** é o `Círculo de confiança`.
    O relacionamento de confiança moveu os trabalhos e quando os trabalhos são usados, o processo de verificação de assinatura é executado. Se todos trabalhos, assinaturas e certificados fizerem parte do Circle of Trust, a Assinatura de código com o Circle of Trust poderá ser ativada.
16. No navegador, insira `sys_properties.list` para abrir a lista de propriedades do sistema.
17. Pesquise *`com_snc_kmf_signature.validation.flag`* e verifique se o valor está definido como **verdadeiro**.
18. Verifique se uma nova propriedade *`com_snc_kmf_signature.validation.certificate`* está listada na tabela.

Propriedades do sistema

com.snc.kmf.signature.validation.certifi...	{"trust_map": {"025b4ed53d332010f877c0bf6...	string	ServiceNow Key Management Framework
com.snc.kmf.signature.validation.flag	true	true | false	Global

Use o trabalho Circle of Trust em produção para verificar o relacionamento de confiança. Nenhum trabalho direto pode ser executado na produção que tente assinar código. Consulte Configuração da assinatura de código para obter detalhes sobre as opções de configuração.

Criar pares de chaves e certificados de assinatura de código

Crie dois pares de chaves para certificados assinados para estabelecer confiança entre as instâncias de produção e as instâncias confiáveis.

Para estabelecer confiança entre suas instâncias, você deve criar um par de chaves e um certificado para cada um dos módulos criptográficos `cm_code_attest` e `cm_code_signing`.

A criação de pares de chaves e certificados é feita usando uma ferramenta criptográfica instalada em seu dispositivo local, como a ferramenta OpenSSL. Para obter mais informações sobre essa ferramenta, consulte https://www.openssl.org. Se sua organização usar outras ferramentas criptográficas, como LibreSSL ou GnuTLS, consulte a documentação desses produtos para ver etapas semelhantes.

Especificações do par de chaves

Os pares de chaves criados devem atender a esses requisitos.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tipo	RSA
Comprimento da chave	4096
Algoritmo de assinatura	RSASSA_PKCS1_V1_5_SHA_512

Especificações do certificado

Os certificados devem ser assinados por uma autoridade de certificação pública.

Especifique as regras personalizadas no firewall do ECC

Configure o firewall External Communication Channel (ECC) em seu MID Server especificando as regras personalizadas para permitir ou rejeitar seletivamente a mensagem de entrada e substituir a configuração de assinatura de código.

Os administradores de segurança podem usar os marcadores de firewall do ECC para substituir a configuração de Assinatura de código e permitir ou rejeitar as operações específicas em MID Server. Essas regras personalizadas devem ser especificadas no arquivo YAML localizado em: `agent/boot-config.yaml`.

Esses marcadores são específicos para um protocolo. A configuração especificada para o marcador primário é aplicável ao marcador secundário. Por exemplo, se o protocolo `Http` for permitido, os protocolos `rest` e `soap` também serão permitidos. Esta tabela descreve os marcadores primários e secundários disponíveis.

Marcador primário	Marcador secundário
DNS	
HTTP	• REST • SOAP
DIRECTORY_SERVICES	LDAP
SNMP	
SSH	• SCP • SFTP
SYSLOG	
WINDOWS	• CIM • POWERSHELL • WMI • WINRM
JAVASCRIPT	
GROOVY	
VCS	GIT
DATABASES	JDBC

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Marcador primário	Marcador secundário
DATA_SOURCES	
INTEGRATION_HUB	
ITOM	• CLOUD_PROVISIONING_GOVERNANCE • DISCOVERY • EVENT_MANAGEMENT • HEALTH_LOG_ANALYTICS • SERVICE_MAPPING
Orquestração	

Para configurar as regras personalizadas:

1. No MID Server, identifique o arquivo `boot-config-sample.yaml`.
2. Renomeie o arquivo YAML para `boot-config.yaml` e mova o arquivo para o local: `agent/boot-config.yaml`.
3. No arquivo YAML, especifique as regras personalizadas e salve as mudanças. Um exemplo do arquivo YAML:

```
security:
  eccFirewall:
    mode: enforcing
    rules:
      - tags: [rest]
        action: accept
      - tags: [soap]
        action: accept
      - tags: [jdbc]
        action: reject
```

4. Reinicie o MID Server.

Mudar a configuração de Raiz de confiança

Confie e use seus próprios certificados em vez de depender de certificados de compilação ServiceNow (padrão), alterando para usar sua raiz de confiança (ROT). Componentes ServiceNow, como inclusões de script, regras de negócios etc., são assinados no tempo de compilação usando uma chave de tempo de compilação ServiceNow (o certificado de verificação é o certificado de compilação ServiceNow).

Alterar a raiz de confiança

Para mudar a Raiz de confiança dessas assinaturas de registros, você deve seguir a mudança do processo de Raiz de confiança.

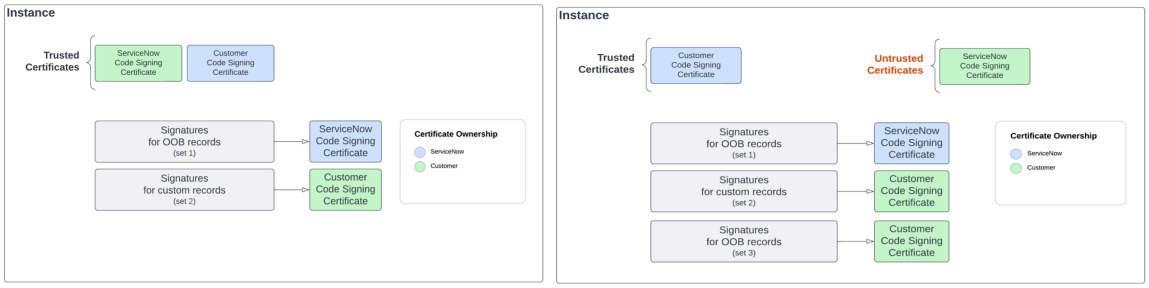
- Gere e migre um novo conjunto de assinaturas para todos os componentes fornecidos usando o certificado fornecido.
- Desabilite a propriedade da Raiz de confiança usando um trabalho agendado.

Saiba mais sobre essas etapas em Migrar assinaturas para usar um certificado do cliente e Desabilitar a raiz de confiança da ServiceNow.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Impacto na geração de assinatura e no processo de verificação

Por padrão, os certificados de compilação de assinatura de código são confiáveis durante o processo de verificação de assinatura. Depois de fazer essa mudança, sua instância aceitará assinaturas somente do seu próprio certificado de assinatura de código.



Propriedade de ROT definida como falsa (padrão)	Propriedade de ROT definida como verdadeira
• Ao verificar, as assinaturas com certificados de compilação são confiáveis. • Ao assinar, se você não fornecer chaves, a chave de assinatura da instância será usada como uma chave de backup. • O endpoint REST de assinatura *api/sn_kmf/signature/certificates* retorna certificados de compilação de assinatura de código ServiceNow junto com outros certificados presentes na instância.	• Ao verificar, as assinaturas com certificados de compilação não são confiáveis. • Ao assinar, se você não fornecer chaves, a assinatura não será realizada. • O endpoint REST de assinatura *api/sn_kmf/signature/certificates* exclui certificados de compilação ServiceNow (San Diego, Vancouver PKI, W PKI).

Impacto no seu MID Server

Se a propriedade ROT for definida como falsa

Se você optar por deixar sua propriedade ROT com o valor padrão (falso), não haverá impacto no seu MID Server.

Quando a assinatura de código está habilitada e a propriedade ROT está definida como verdadeira

- A API *isTrusted()* retorna `falso` para assinaturas com um certificado de compilação.
- A API *isTrusted()* retorna `verdadeiro` para assinaturas com seu certificado.
- A chamada de REST API para certificados exclui certificados de compilação.
- Você pode ver problemas do MID Server, como mensagens de `falha na validação de assinatura` nos logs.

Migrar assinaturas para usar um certificado do cliente

Execute um trabalho de assinatura para migrar suas assinaturas para uma Raiz de confiança (ROT) do cliente.

Antes de Iniciar

Função necessária: admin, security_admin e sn_kmf.cryptographic_manager

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A assinatura de código deve estar habilitada nas suas instâncias de confiança e de produção. Para saber mais, verifique se a propriedade do sistema **com.snc.kmf.signature.validation.flag** está definida como `verdadeira`.

Esse procedimento faz parte de uma série de procedimentos para mudar uma Raiz de confiança (ROT) do cliente nas suas instâncias. Para obter uma visão geral desse processo, consulte Mudar a configuração de Raiz de confiança.

Procedimento

1. Faça login na sua instância de produção.
2. Navegue até **Todos** > **Definição do sistema** > **Trabalhos agendados**.
3. Encontre e abra o trabalho agendado **ROT - Gerar Updateset de registros para migrar assinaturas usando o certificado do cliente**.
4. Na parte inferior do formulário, selecione **Executar agora**.
5. Navegue até **Todos** > **Segurança do sistema** > **Trabalhos de segurança** > **Criar novo**.
6. No prompt, selecione **Trabalho de assinatura**.
7. No formulário **Trabalho de assinatura**, preencha os campos conforme necessário.

Campo	Valor
Nome	Crie um nome exclusivo para o seu trabalho.
Tipo	Selecione **Assinar Update Set**.
Tabela	Selecione o conjunto para atualização criado nas etapas anteriores. O conjunto para atualização tem um nome que começa com `change_root_of_trust_updateSet`.

8. Clique com o botão direito no cabeçalho do formulário e selecione **Salvar** para salvar este registro.
9. Clique com o botão direito no cabeçalho do formulário e selecione **Exportar** > **XML (este registro)** para exportar este registro como um arquivo XML.
10. Faça login na sua instância confiável.
11. Navegue para **Todos** > **Segurança do sistema** > **Trabalhos de segurança** > **Todos**.
12. Clique com o botão direito no cabeçalho de listas e selecione **Importar XML**.
13. No formulário **Importar XML**, selecione **Escolher arquivo** e selecione o arquivo XML que você baixou nas etapas anteriores.
14. Selecione **Carregar**.
15. Na lista, abra o trabalho de segurança importado.
16. Selecione **Exportar trabalho de assinatura de código para produção**.
    Esta ação assina o trabalho e o coloca em um novo conjunto para atualizações que você pode importar para sua instância de produção.

> **Importante:** Depois de assinar o trabalho, você deve executar as próximas etapas em 10 minutos. Se você exceder esse período de tempo, poderá assinar novamente o trabalho usando essas etapas, o que cria outro conjunto para atualização assinado.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

17. Navegue até **Todos** > **Conjuntos de atualizações do sistema** > **Conjuntos de atualizações locais**.
18. Encontre o conjunto para atualização criado nas etapas anteriores.
    O nome começa com `SIGN_UPDATE_SET_updateSet`.
19. Selecione **Exportar XML** para exportar seu conjunto para atualização como um arquivo XML.
20. Faça login na sua instância de produção.
21. Navegue até **Todos** > **Conjuntos de atualizações do sistema** > **Conjuntos de atualizações recuperados**.
22. Na parte inferior da lista, selecione **Importar conjunto para atualização do XML**.
23. No formulário **Importar XML**, selecione **Escolher arquivo** e selecione o arquivo XML que você baixou nas etapas anteriores.
24. Selecione **Carregar**.
25. Navegue até **Todos** > **Conjuntos de atualizações do sistema** > **Conjuntos de atualizações recuperados**e abra o conjunto de atualizações que começa com `SIGN_UPDATE_SET_updateSet`.
26. Selecione **Visualizar conjunto para atualização**.
27. Depois que a exibição for concluída, selecione **Confirmar conjuntos para atualização**.
28. Navegue para **Todos** > **Segurança do sistema** > **Trabalhos de segurança** > **Todos**.
29. Abra o trabalho de segurança importado.
30. Selecione **Iniciar** para executar o trabalho de segurança.

    Depois que o trabalho de segurança for concluído, as informações sobre o status do trabalho serão exibidas no campo **Resumo**.

    Quando o trabalho está no estado Concluído, todas as assinaturas de registros do conjunto para atualizações devem usar o certificado fornecido pelo cliente como certificado de verificação. Você pode verificar isso na tabela Registros de assinatura KMF [sn_kmf_record_signature].

O que Fazer Depois

Para continuar o processo de configuração da Raiz de confiança, consulte Desabilitar a raiz de confiança da ServiceNow.

Desabilitar a raiz de confiança da ServiceNow

Execute um trabalho agendado em sua instância de não produção confiável para desabilitar a Raiz de confiança.

Antes de Iniciar

Função necessária: admin, security_admin e sn_kmf.cryptographic_manager

A assinatura de código deve estar habilitada nas suas instâncias de confiança e de produção. Para saber mais, verifique se a propriedade do sistema **com.snc.kmf.signature.validation.flag** está definida como `verdadeira`.

Este procedimento faz parte de uma série de procedimentos para mudar para uma Raiz de confiança (ROT) do cliente em suas instâncias. Para obter uma visão geral desse processo, consulte Mudar a configuração de Raiz de confiança.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Faça login na sua instância de confiança.
2. Navegue até **Todos** > **Definição do sistema** > **Trabalhos agendados**.
3. Abra o trabalho agendado **Desabilitar Raiz de confiança da ServiceNow**.
4. Selecione **Exportar trabalho assinado para produção**.
5. Navegue até **Todos** > **Conjuntos de atualizações do sistema** > **Conjuntos de atualizações locais**.
6. Encontre e abra o conjunto para atualização **Desabilitar Raiz de confiança da ServiceNow**.
7. Selecione **Exportar XML** para exportar seu conjunto para atualização como um arquivo XML.
8. Faça login na sua instância de produção.
9. Navegue até **Todos** > **Conjuntos de atualizações do sistema** > **Conjuntos de atualizações recuperados**.
10. Na parte inferior da lista, selecione **Importar conjunto para atualização do XML**.
11. No formulário **Importar XML**, selecione **Escolher arquivo** e selecione o arquivo XML que você baixou nas etapas anteriores.
12. Selecione **Carregar**.
13. Navegue até **Todos** > **Conjuntos de atualizações do sistema** > **Conjuntos de atualizações recuperados** e abra o conjunto de atualizações **Desabilitar Raiz de confiança da ServiceNow**.
14. Selecione **Visualizar conjunto para atualização**.
15. Depois que a exibição for concluída, selecione **Confirmar conjuntos para atualização**.
16. Navegue até **Todos** > **Definição do sistema** > **Trabalhos agendados**.
17. Abra o trabalho agendado importado no conjunto para atualização.
18. Selecione o botão **Executar agora** para executar o trabalho.

Resultados

A execução do trabalho agendado define a propriedade ROT como verdadeira. Sua instância está configurada para usar a raiz de confiança do cliente.

Usar a assinatura de código

Aprenda a assinar registros, mensagens e anexos para ajudar a verificar a autenticidade e integridade dos seus dados.

Assine os registros de fonte de dados JDBC na instância de produção

Use os conjuntos de atualizações para assinar e validar as fontes de dados JDBC, habilitando a assinatura de código em instâncias de confiança e de produção.

Assine as mensagens REST e SOAP na instância de produção

Use os conjuntos de atualizações para assinar e validar as mensagens REST e SOAP, habilitando a assinatura de código em instâncias de confiança e de produção.

Assine os fluxos, subfluxos e ações na instância de produção

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Use os conjuntos de atualizações para assinar e validar os fluxos, subfluxos e ações, habilitando a assinatura de código em instâncias de confiança e de produção.

Assine registros e anexos específicos

Crie um trabalho de segurança para assinar registros ou anexos específicos em vez de todos os registros ou anexos de uma tabela.

Ferramenta de assinatura autônoma

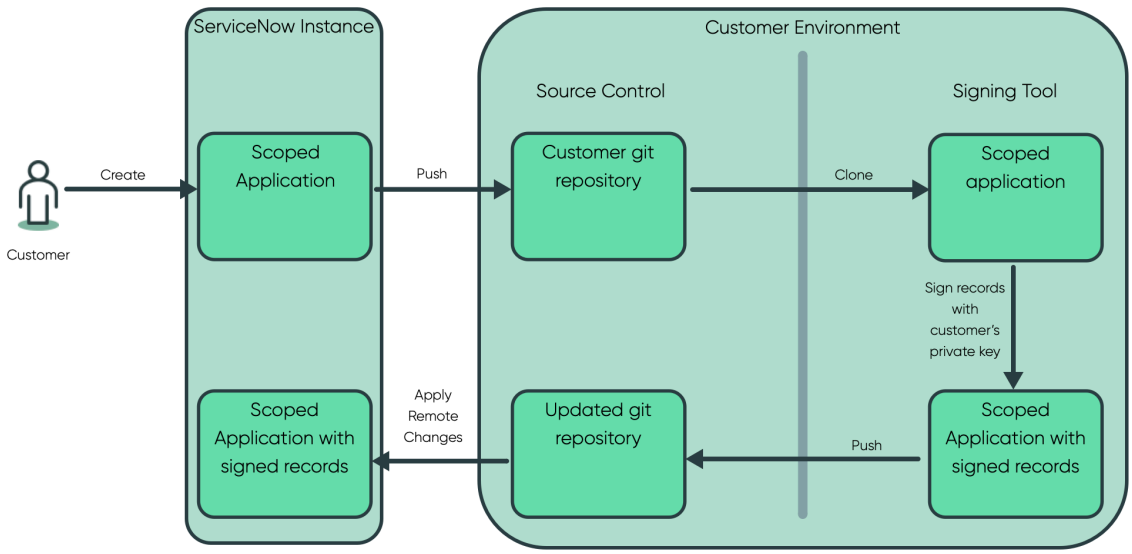
Use a Ferramenta de assinatura autônoma para assinar registros compatíveis em aplicações da ServiceNow usando sua própria chave privada.

Ferramenta de assinatura autônoma

Use a Ferramenta de assinatura autônoma para assinar registros compatíveis em aplicações da ServiceNow usando sua própria chave privada.

Use a ferramenta de assinatura para assinar registros em aplicações da ServiceNow. A ferramenta gera assinaturas para registros em seu ambiente local usando sua própria chave privada.

Fluxo de trabalho da ferramenta de assinatura



1. Crie ou selecione uma aplicação ServiceNow existente com registros a serem assinados, como regras de negócios ou inclusões de script.
2. Envie a aplicação por push para o repositório Git, que reside no seu ambiente.

   Nota: As aplicações podem ser sincronizadas entre um repositório Git e sua instância usando a integração de controle de código-fonte. Para obter detalhes sobre como configurar e usar esta integração, consulte Integração do controle de código-fonte.

3. Clone a aplicação em seu ambiente local.
4. Use a ferramenta de assinatura (também no seu ambiente local) para assinar os registros compatíveis da aplicação da ServiceNow clonada usando sua chave privada. A ferramenta de assinatura cria registros de assinatura e registros de certificado X.509

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

[sys_certificate]. Para obter detalhes sobre como usar a Ferramenta de assinatura, consulte Usando a Ferramenta de Assinatura.

5. Envie por push a aplicação atualizada para o seu repositório Git.
6. Na sua instância, importe a aplicação atualizada aplicando as mudanças remotas.

Usando a Ferramenta de Assinatura

Aprenda a usar a ferramenta de assinatura para assinar registros compatíveis da ServiceNow.

Antes de Iniciar

Função necessária: admin

Para executar essas etapas, você deve ter o seguinte:

- Uma aplicação ServiceNow que tem registros a serem assinados.
- Uma chave privada para assinar registros.
- O script *signRecords.sh* em seu ambiente local, com permissão de execução.

> **Importante:** O script *signRecords.sh* está incluído como parte do arquivo jar da ferramenta de assinatura, que você deve solicitar ao ServiceNow suporte ao cliente.

Procedimento

1. Em seu ambiente local, navegue até o diretório que contém o script *signRecords.sh*.
2. Use o seguinte comando para assinar seus registros:

```
./signRecords.sh -d [Path to the root directory of the ServiceNow
 Application to Sign] -f [Path to the Keystore file]
```

   Por exemplo:

```
./signRecords.sh -d /users/abc/ServiceNow-App-1
 -f /users/abc/codesigning.p12
```

3. Se for solicitado um prompt, insira a senha do armazenamento de chaves. Pressione Enter se não houver senha.
4. Revise a saída para confirmar uma assinatura bem-sucedida.

```
Sep 26, 2022 2:41:09 PM com.snc.java.commands.ACommand start
INFO: CODESIGN: executing codesigning...
Sep 26, 2022 2:41:09 PM com.snc.core.codesigning.CodeSignerSupplier get
INFO: CODESIGN: signing record for documentId:
 65e811327702111057416efe7c5a994f
Sep 26, 2022 2:41:11 PM com.snc.java.commands.ACommand start
INFO: CODESIGN: codesigning successfully completed!
```

   No exemplo de saída anterior, a Ferramenta de assinatura usou o arquivo de armazenamento de chaves para assinar o registro. Você também irá notar que:

   - O script encontrou um registro compatível `65e811327702111057416efe7c5a994f` e o assinou.
   - No diretório ServiceNow-App-1, dois registros foram criados: `sys_certificate.xml` e `sn_kmf_record_signature.xml`.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Importe a aplicação atualizada de volta para sua instância aplicando as mudanças remotas em Studio.
   Para obter mais informações, consulte Aplicar mudanças remotas.

Argumentos da ferramenta de assinatura

Saiba mais sobre os argumentos disponíveis para a ferramenta de assinatura.

Argumentos da linha de comando

Argumento	Necessários	Descrição
-d	Sim	Diretório raiz do projeto a ser assinado. Deve conter o diretório do projeto (alfanumérico aleatório de 32 caracteres), o arquivo sn_source_control.properties e um arquivo <nome_do_projeto>.iml
-f	Sim	O caminho do arquivo do armazenamento de chaves.
-a	Não	Alias usado para acessar uma entrada específica no armazenamento de chaves.
-c	Não	Concatenar assinaturas de registro em um arquivo.
-k	Não	Senha para acessar a chave armazenada no armazenamento de chaves. Você também pode inserir esta senha quando solicitado, em vez de transmiti-la como argumento.
-o	Não	Assine com um novo certificado substituindo qualquer arquivo sys_cert existente.
-p	Não	Senha para acessar o armazenamento de chaves se ele tiver uma senha. Você também pode inserir esta senha quando solicitado, em vez de transmiti-la como argumento.
-w	Não	Limpe todos os arquivos de registro de assinatura existentes.
-h	Não	Mostre esta mensagem de ajuda e saia.

Assine os registros de fonte de dados JDBC na instância de produção

Use os conjuntos de atualizações para assinar e validar as fontes de dados JDBC, habilitando a assinatura de código em instâncias de produção e de não produção confiável.

- Estabeleça Circle of Trust entre as instâncias de produção e de confiança.
- Função necessária: security_admin

Nota:

- MID Server não lida com as fontes de dados do arquivo e, portanto, essas fontes de dados não são assinadas por código.
- As fontes de dados LDAP não podem ser assinadas por código.

Assinar fontes de dados existentes do tipo JDBC

Use conjuntos de atualizações para trazer trabalhos de assinatura em massa para a instância de produção.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: security_admin

Procedimento
1. Na instância de não produção confiável, configure o trabalho de assinatura da KMF para assinar as fontes de dados.

   a. Navegue até **Segurança do sistema** > **Trabalhos de segurança** > **Todos**.

   b. Clique em **Novo**.

   c. No formulário, preencha estes valores.

Campo	Descrição
Nome	Nome para identificar o registro.
Tipo	Tipo de trabalho de criptografia. Selecione **Assinar em massa os registros**.
Tabela	Tabela da qual os registros devem ser assinados. Selecione **Fonte de dados**.

   d. Clique em **Exportar trabalho de Assinatura de código para produção**.
   É exibida uma mensagem de confirmação de que o conjunto de atualizações está assinado.

   e. Exporte o conjunto de atualizações gerado para um arquivo XML.

2. Na instância de produção, importe e confirme o conjunto para atualização para recuperar os trabalhos assinados em massa da instância de confiança.

   a. Navegue até **Segurança do sistema** > **Trabalhos de segurança** > **Todos**.

   b. Abra o conjunto para atualização exportado da instância de confiança.

   c. Clique em **Iniciar**.
   É exibida uma mensagem de confirmação de que os registros estão assinados.

Assinar novas fontes de dados do tipo JDBC

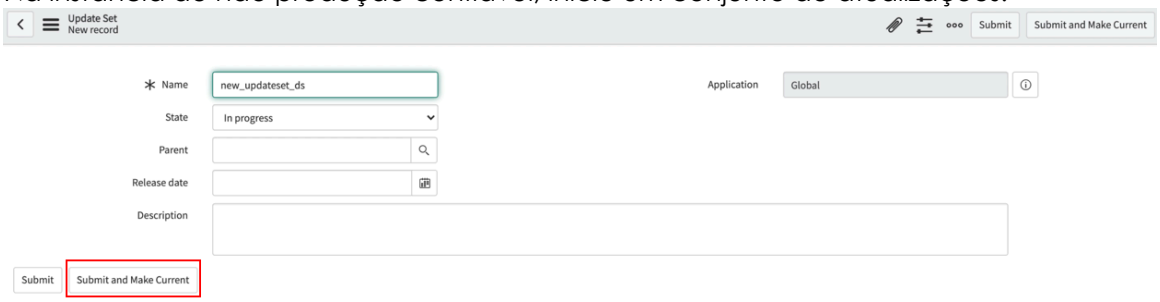
Use os conjuntos de atualizações para trazer o conjunto de atualizações assinado para a instância de produção.

Antes de Iniciar
Função necessária: sn_kmf.cryptographic_manager

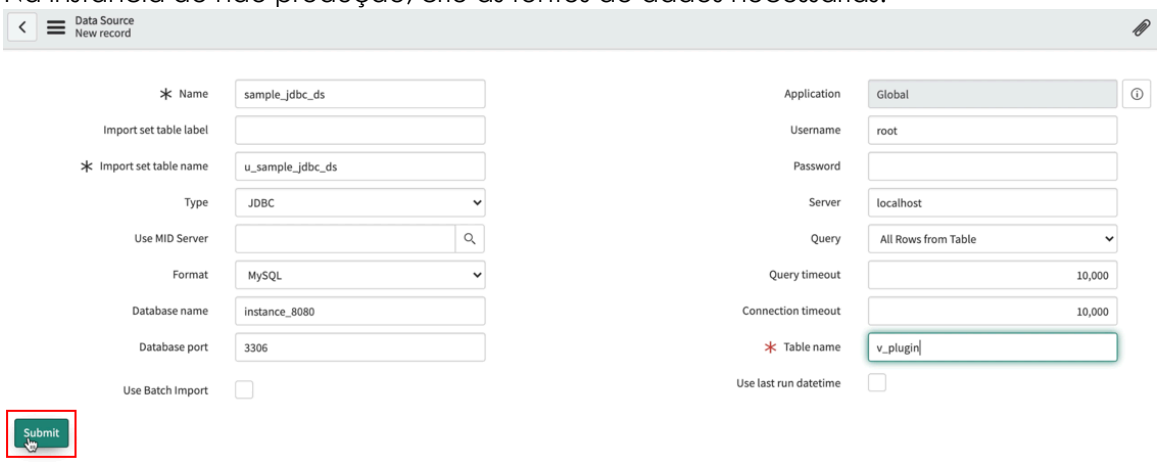
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Na instância de não produção confiável, inicie um conjunto de atualizações.

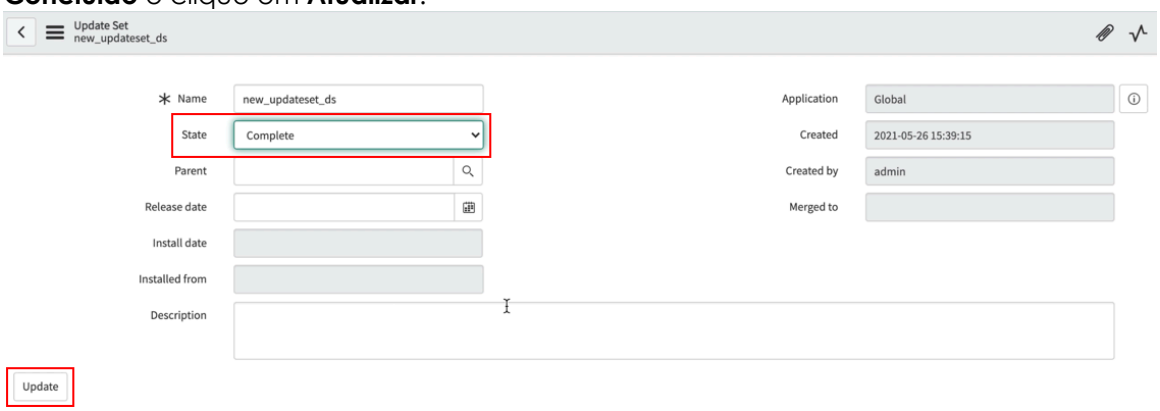


2. Na instância de não produção, crie as fontes de dados necessárias.



   As fontes de dados são adicionadas ao conjunto de atualizações.

3. Na instância de não produção, altere o estado do conjunto de atualizações para **Concluído** e clique em **Atualizar**.



4. Na instância de não produção, assine o conjunto de atualizações criando um trabalho de criptografia.

   a. Navegue até **Segurança do sistema** > **Trabalhos de segurança** > **Todos**.

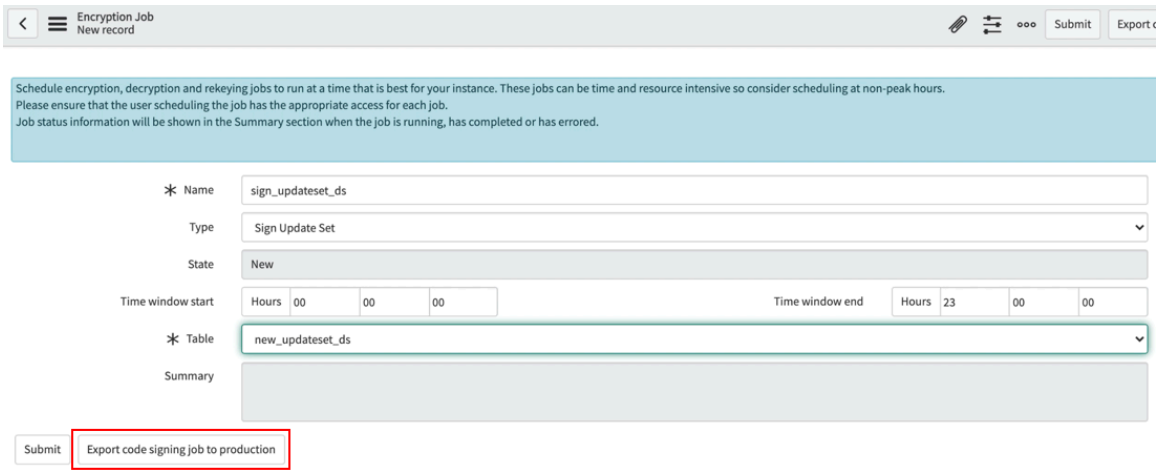
   b. Clique em **Novo**.

   c. No formulário, preencha estes valores.

Campo	Descrição
Nome	Nome para identificar o registro.

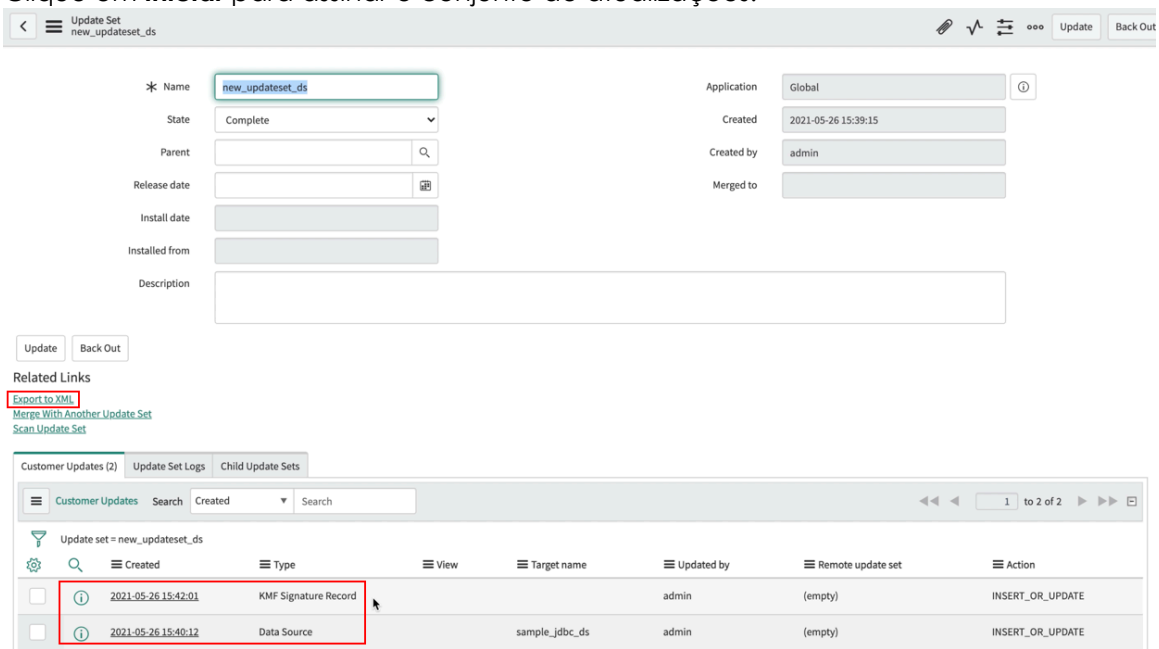
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Tipo	Tipo de trabalho de criptografia. Selecione **Assinar Update Set**.
Tabela	Conjunto de atualizações do qual os registros devem ser assinados.



d. Clique em **Enviar**.

e. Clique em **Iniciar** para assinar o conjunto de atualizações.



- É atualizado o **Resumo** cujos registros estão assinados.
- O conjunto de atualizações é atualizado e inclui a assinatura.

5. Na instância de não produção, abra o registro do conjunto de atualizações assinado e exporte-o para um XML.

6. Na instância de produção, importe o conjunto de atualizações assinado.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Navegue até **Conjuntos de atualizações do sistema** > **Conjuntos de atualizações recuperados**.

b. Clique no link relacionado **Importar conjunto para atualizações do XML** para importar o conjunto de atualizações que é exportado da instância de confiança.
Para obter mais informações, consulte Importar e confirmar o conjunto para atualização de início rápido.
O conjunto de atualizações foi confirmado com sucesso.

Assine as mensagens REST e SOAP na instância de produção

Use os conjuntos de atualizações para assinar e validar as mensagens REST e SOAP habilitando a assinatura de código de produção e as instâncias de não produção.

Antes de Iniciar

- Estabeleça Circle of Trust entre as instâncias de produção e de não produção.
- Função necessária: security_admin

Assine as mensagens REST e SOAP existentes

Assine e valide as mensagens REST e SOAP existentes habilitando a assinatura de código em instâncias de produção e não produção confiáveis.

Antes de Iniciar

Função necessária: sn_kmf.cryptographic_manager

Procedimento

1. Na instância confiável, configure o trabalho de assinatura KMF para assinar as ações de IU.

   a. Navegue até Configuração de assinatura KMF.

   b. No formulário, preencha estes valores.

Formulário de Configuração de assinatura KMF

Campo	Descrição
Nome da tabela	Nome de tabela Glide. Por exemplo, selecione **Ações de IU [sys_ui_action]**.
Finalidade da assinatura KMF	Finalidade de assinar os registros. Selecione **Fila do ECC**.
Campos de geração de assinatura	Campos na fonte de dados que você deseja assinar. Se forem feitas algumas mudanças nos valores em um ou mais desses campos, a assinatura anteriormente gerada se tornará inválida. Selecione **Nome** e **Script**.
Filtro de geração de assinatura	Critérios de filtro que devem ser atendidos para assinar os registros.
Assinar anexo	Opção de assinar o anexo no registro Glide.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Chave de Instância	Opção para usar a chave de instância.

c. Clique com o botão direito no cabeçalho do formulário e clique em **Salvar**.

2. Na instância de confiança, assine os registros necessários.

a. Navegue até **Segurança do sistema** > **Trabalhos de segurança** > **Todos**.

b. Clique em **Novo**.

c. No formulário, preencha estes valores.

Campo	Descrição
Nome	Nome para identificar o registro.
Tipo	Tipo de trabalho de criptografia. Selecione **Assinar em massa os registros**.
Tabela	Tabela da qual os registros devem ser assinados. Selecione **Ação de IU**.

d. Clique em **Exportar trabalho de Assinatura de código para produção**.
São criados dois conjuntos de atualizações assinados localmente.

- Um conjunto de atualizações para a configuração de ação de IU.
- Outro conjunto para atualização do trabalho de criptografia para exportar o trabalho de assinatura de código.

3. Na instância de confiança, exporte o conjunto de atualizações local para um arquivo XML.

a. Navegue até **Conjuntos de atualizações do sistema** > **Conjuntos de atualizações locais**.

b. Abra o conjunto de atualizações que você criou para assinar os registros em massa.

c. Clique no link relacionado **Exportar para XML** e salve o arquivo XML.

4. Na instância de produção, importe os conjuntos de atualizações.

a. Navegue até **Conjuntos de atualizações do sistema** > **Conjuntos de atualizações recuperados**.

b. Clique no link relacionado **Importar conjunto para atualizações do XML** para importar o conjunto de atualizações que é exportado da instância de confiança.
Para obter mais informações, consulte Importar e confirmar o conjunto para atualização de início rápido.
O conjunto de atualizações foi confirmado com sucesso.

5. Na instância de produção, execute o trabalho de criptografia que você criou anteriormente na instância de confiança clicando em **Iniciar**.
É exibida uma mensagem de confirmação mencionando que os registros estão assinados.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Assine novas mensagens REST e SOAP

Assine e valide as novas mensagens REST e SOAP da instância de confiança habilitando a assinatura de código em instâncias de confiança e de produção.

Antes de Iniciar

Função necessária: security_admin

Procedimento

1. Na instância de não produção confiável, inicie um conjunto de atualizações.
2. Na instância de não produção confiável, crie as mensagens REST ou SOAP necessárias. As mensagens são adicionadas ao conjunto de atualizações.
3. Na instância de não produção, altere o estado do conjunto de atualizações para **Concluído** e clique em **Atualizar**.
4. Na instância de não produção, assine o conjunto de atualizações criando um trabalho de criptografia.

   a. Navegue até **Segurança do sistema** > **Trabalhos de segurança** > **Todos**.

   b. Clique em **Novo**.

   c. No formulário, preencha estes valores.

Campo	Descrição
Nome	Nome para identificar o registro.
Tipo	Tipo de trabalho de criptografia. Selecione **Assinar Update Set**.
Tabela	Conjunto de atualizações do qual os registros devem ser assinados. Selecione **Assinar novo conjunto de atualizações Rest V2 - 1**.

   d. Clique em **Enviar**.

   e. Clique em **Iniciar** para assinar o conjunto de atualizações.
      - É atualizado o **Resumo** cujos registros estão assinados.
      - O conjunto de atualizações é atualizado e inclui a assinatura.

5. Na instância de não produção, abra o registro do conjunto de atualizações assinado e exporte-o para um XML.
6. Na instância de produção, importe o conjunto de atualizações.

   a. Navegue até **Conjuntos de atualizações do sistema** > **Conjuntos de atualizações recuperados**.

   b. Selecione o link relacionado **Importar conjunto para atualização do XML** para importar o conjunto de atualização que é exportado da instância de confiança.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para obter mais informações, consulte Importar e confirmar o conjunto de atualizações de início rápido.
O conjunto de atualizações foi confirmado com sucesso.

Assine os fluxos, subfluxos e ações na instância de produção

Use os conjuntos de atualizações para assinar e validar os fluxos, subfluxos e ações, habilitando a assinatura de código em instâncias de confiança e de produção.

- Estabeleça Circle of Trust entre as instâncias de produção e de confiança.
- Função necessária: security_admin

Assinar o fluxo, os subfluxos e as ações existentes

Assine e valide o fluxo, os subfluxos e as ações existentes habilitando a assinatura de código em instâncias de produção e não produção confiáveis.

Antes de Iniciar

Função necessária: sn_kmf.cryptographic_manager

Procedimento

1. Na instância de confiança, assine os registros na tabela Instância de etapa.
   a. Navegue até **Segurança do sistema** > **Trabalhos de segurança** > **Todos**.
   b. Clique em **Novo**.
   c. No formulário, preencha estes valores.

Campo	Descrição
Nome	Nome para identificar o registro.
Tipo	Tipo de trabalho de criptografia. Selecione **Assinar em massa os registros**.
Tabela	Tabela da qual os registros devem ser assinados. Selecione **Instância de etapa**.

   d. Clique em **Exportar trabalho de Assinatura de código para produção**.
   São criados dois conjuntos de atualizações assinados localmente.
      - Um conjunto de atualizações para a assinatura KMF.
      - Outro conjunto de atualizações do trabalho de criptografia para exportar o trabalho de assinatura de código.
2. Na instância de confiança, exporte o conjunto de atualizações local para um arquivo XML.
   a. Navegue até **Conjuntos de atualizações do sistema** > **Conjuntos de atualizações locais**.
   b. Abra o conjunto de atualizações que você criou para assinar os registros em massa.
   c. Clique no link relacionado **Exportar para XML** e salve o arquivo XML.
3. Na instância de produção, importe o arquivo XML.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Navegue até **Conjuntos de atualizações do sistema** > **Conjuntos de atualizações recuperados**.

b. Clique no link relacionado **Importar conjunto para atualizações do XML** para importar o conjunto de atualizações que é exportado da instância de confiança.
Para obter mais informações, consulte Importar e confirmar o conjunto para atualização de início rápido.
O conjunto de atualizações foi confirmado com sucesso.

4. Na instância de produção, execute o trabalho de criptografia que você criou anteriormente na instância de confiança.

a. Navegue até **Segurança do sistema** > **Trabalhos de segurança** > **Todos**.

b. Abra o trabalho de criptografia que você criou anteriormente na instância de confiança.

c. Clique em **Iniciar** para iniciar o trabalho.
É exibida uma mensagem de confirmação mencionando que os registros estão assinados.

Assinar novos fluxo, subfluxos e ações

Assine e valide o novo fluxo, os subfluxos e as ações habilitando a assinatura de código em instâncias de produção e de não produção confiáveis.

Antes de Iniciar

Função necessária: sn_kmf.cryptographic_manager

Procedimento

1. Na instância de confiança, inicie um conjunto para atualização.
2. Na instância de confiança, crie os fluxos, subfluxos ou ações necessários e os publique.
Os fluxos, subfluxos ou ações são adicionados ao conjunto de atualizações.
3. Na instância de confiança, mude o estado do conjunto para atualização para **Concluído** e clique em **Atualizar**.
4. Na instância de confiança, assine o conjunto para atualização criando um trabalho de criptografia.

a. Navegue até **Segurança do sistema** > **Trabalhos de segurança** > **Todos**.

b. Clique em **Novo**.

c. No formulário, preencha estes valores.

Campo	Descrição
Nome	Nome para identificar o registro.
Tipo	Tipo de trabalho de criptografia. Selecione **Assinar Update Set**.
Tabela	Conjunto de atualizações do qual os registros devem ser assinados.

d. Clique em **Enviar**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

e. Clique em **Iniciar** para assinar o conjunto de atualizações.

- É atualizado o **Resumo** cujos registros estão assinados.
- O conjunto de atualizações é atualizado e inclui a assinatura.

5. Na instância de confiança, abra o registro do conjunto para atualização assinado e o exporte para um XML.

6. Na instância de produção, importe o conjunto de atualizações assinado.

a. Navegue até **Conjuntos de atualizações do sistema** > **Conjuntos de atualizações recuperados**.

b. Selecione o link relacionado **Importar conjunto para atualização do XML** para importar o conjunto de atualização que é exportado da instância de confiança.
Para obter mais informações, consulte Importar e confirmar o conjunto de atualizações de início rápido.
O conjunto de atualizações foi confirmado com sucesso.

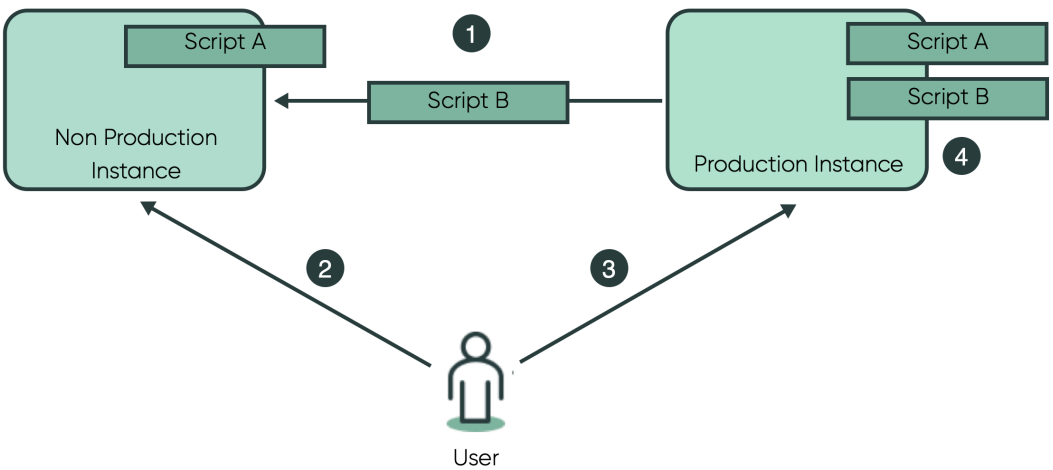
Assine registros e anexos específicos

Crie um trabalho de segurança para assinar registros ou anexos específicos em vez de todos os registros ou anexos de uma tabela.

A partir da versão Vancouver, os administradores de segurança podem usar trabalhos de segurança para assinar registros específicos de uma tabela em vez de todos os registros de uma tabela. Assine registros específicos para evitar assinar acidentalmente códigos não revisados.

Esses trabalhos incluem um arquivo de log anexado que é gerado no final do trabalho de assinatura. Este arquivo de log contém informações sobre registros assinados e a configuração de assinatura usada.

Processo de assinatura



Este diagrama mostra um exemplo de como você pode usar o processo de assinatura. Neste exemplo, um script denominado `Script B` existe apenas na instância de produção e deve ser importado para uma instância de confiança a ser assinada. `O script A` já existe

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

em ambas as instâncias e não precisa ser assinado. Ele já foi revisado ou assinado, ou ainda não foi revisado e não deve ser assinado.

1. Importe o registro para seu ambiente de confiança.
2. Na instância de confiança, crie um trabalho de assinatura para assinar o registro. Este processo é detalhado em Crie um trabalho para assinar registros ou anexos específicos em uma instância de confiança.
3. Importe o trabalho de assinatura assinado para sua instância de produção usando um conjunto de atualizações.
4. Na instância de produção, execute o trabalho de assinatura que foi importado.

Crie um trabalho para assinar registros ou anexos específicos em uma instância de confiança

Assine um registro específico ou grupos de registros definidos por você em uma instância de não produção.

Antes de Iniciar

Funções necessárias: security_admin e sn_kmf.cryptographic_manager

Procedimento

1. Navegue até **Todos** > **Segurança do sistema** > **Trabalhos de segurança** > **Criar novo**.
2. No prompt **Que tipo de trabalho de segurança você deseja criar?** selecione **Trabalho de assinatura**.
   Um novo registro de **Trabalho de assinatura** será exibido.
3. Preencha os campos do formulário conforme necessário.

Campos do trabalho de assinatura

Campo	Descrição
Nome	Nome descritivo para este trabalho.
Tipo	Tipo de trabalho de segurança. Para assinar registros específicos, selecione a opção **"Assinar registros específicos"**. Para assinar anexos específicos, selecione **"Assinar anexos específicos"**.
Estado	Estado deste trabalho. Este campo começa com o valor de **"Novo"**. Este campo é somente leitura.
Tabela	Tabela que contém os registros ou anexos que você deseja assinar. Ao assinar anexos, selecione a tabela com registros que estejam associados aos anexos, não a tabela de Anexo [sys_attachment]. **Dica:** Verifique a tabela de Registo de assinatura KMF (Key Management Framework – Estrutura de gestão de chaves) [sn_kmf_record_signature] para garantir que ainda não haja assinaturas para a tabela selecionada.

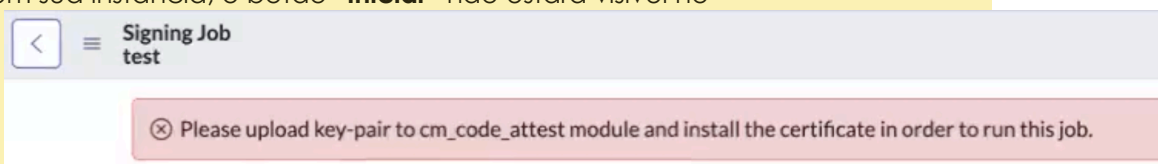
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Filtrar registros	Condições de filtro usadas para limitar quais registros aparecem na tabela **"Selecionar registros para assinatura"**.
Selecionar registros para assinatura	Lista de registros na tabela selecionada no campo **"Tabela"**, limitada pelo filtro criado no campo **"Filtrar registros"**. Mova os registros da janela **"Disponível"** para a janela **"Selecionado"** para incluí-los no trabalho de assinatura.
Início da janela de tempo	O início da janela de tempo para executar este trabalho. O trabalho será executado após a hora inserida neste campo. Os horários válidos devem estar no Tempo Universal Coordenado e em ciclos de 24 horas.
Fim da janela de tempo	O fim da janela de tempo para executar este trabalho. O trabalho é executado antes da hora inserida neste campo. Se o trabalho ainda não tiver sido concluído, ele será pausado e retomado na próxima janela de tempo. A hora de término deve ser posterior à hora de início. Os horários válidos devem estar no Tempo Universal Coordenado e em ciclos de 24 horas.
Resumo	Resumo da execução deste trabalho. Este campo é somente leitura.

4. Clique com o botão direito no cabeçalho do formulário e selecione **"Salvar"**.
5. Na parte inferior do formulário, selecione **"Exportar trabalho de assinatura de código para produção"**.
   Esta ação assina o trabalho de assinatura, e ele estará pronto para ser exportado.
6. Navegue até **Todos** > **Conjuntos de atualizações do sistema** > **Conjuntos de atualizações locais**.
7. Encontre e abra o conjunto de atualizações do seu trabalho de assinatura.
   Na guia de atualizações do cliente, você verá que este conjunto de atualizações inclui o trabalho de assinatura e o registro de assinatura.
8. Selecione **Exportar para XML**.
   Esta ação cria um arquivo XML que contém seu conjunto de atualizações em seu dispositivo local.
9. Na sua instância de produção, navegue até **Todos** > **Conjuntos de atualizações do sistema** > **Conjuntos de atualizações recuperados** > **.**
10. Na parte inferior da página, selecione **"Importar Update Set do XML"**.
11. Selecione o botão **"Escolher arquivo"** e selecione o arquivo XML criado nas etapas anteriores.
12. Selecione **"Carregar"**.
    Seu conjunto de atualizações será carregado e aparecerá na lista **Conjuntos de atualizações recuperados**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

13. Na lista **Conjuntos de atualizações recuperados**, abra o registro para acessar o conjunto de atualizações importadas.
14. Selecione o botão **"Visualizar Update Set"**.
    Depois que a visualização for concluída com sucesso, você verá o botão **"Confirmar Update Set"**.
15. Clique em **"Confirmar Update Set"**.
16. **Todos** > **Segurança do sistema** > **Trabalhos de segurança** > **Todos**.
17. Abra seu trabalho de assinatura.
18. Selecione **"Iniciar"** para executar o trabalho de assinatura.

> ⚠ **Aviso:** Se o par de chaves não tiver sido carregado para sua instância de produção, você verá um aviso na parte superior do formulário de registro. Se esse par de chaves não estiver presente em sua instância, o botão **"Iniciar"** não estará visível no formulário.
>
> 
>

O que Fazer Depois

Quando concluído, o campo **Resumo** exibirá os resultados do trabalho. Há também um arquivo de log anexado ao registro do trabalho de assinatura chamado "Mass_Sign_Records-<sys_id>". Revise esse registro para obter detalhes sobre o trabalho e uma lista de sys_ids para cada registro assinado.

Referência de assinatura de código

Os tópicos de referência apresentam informações adicionais sobre a administração e solução de problemas de assinatura de código.

Propriedades instaladas com a assinatura de código

A assinatura de código adiciona as seguintes propriedades.

Solução de problemas e acesso a logs

Acesse vários logs para solucionar problemas e identificar os motivos da falha.

Propriedades instaladas com a assinatura de código

A assinatura de código adiciona as seguintes propriedades.

Propriedade	Tipo	Descrição
com.glide.codesigning.expanded.tracking.enabled	verdadeiro | falso	Quando verdadeiro, o tamanho da validação da meta-stack aumenta para tópicos ecc_queue listados na propriedade **com.glide.codesigning.expanded_tracking.topic.list**. **Importante:** A segurança elevada é necessária para modificar esta propriedade.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Propriedade	Tipo	Descrição
com.glide.codesigning.expanded.tracking.level	Inteiro	Níveis de validação de assinatura de código quando a assinatura de código estiver habilitada. O valor padrão é 3. **Importante:** A segurança elevada é necessária para modificar esta propriedade.
com.glide.codesigning.expanded_tracking.topic_list	Cadeia de caracteres	Lista separada por vírgulas de tópicos que estarão sujeitos ao aumento do rastreamento da meta-stack. **Importante:** A segurança elevada é necessária para modificar esta propriedade.
com.glide.codesigning.tracking.agent.exclusion_list	Cadeia de caracteres	Lista separada por vírgula de agentes ecc_queue para os quais a assinatura de código deve ser ignorada
com.glide.codesigning.tracking.debug	verdadeiro | falso	Quando verdadeiro, o registro em log de depuração do rastreador de assinatura de código está habilitado.
com.glide.codesigning.tracking.enabled	verdadeiro | falso	Quando verdadeiro, habilita o rastreamento de chamadas de assinatura de código. **Importante:** A segurança elevada é necessária para modificar esta propriedade.
com.glide.codesigning.tracking.logging.enabled	verdadeiro | falso	Quando verdadeiro, habilita o registro em log para o rastreamento de assinatura de código.
com.glide.codesigning.tracking.unsupported_script_tracking.enabled	verdadeiro | falso	Quando verdadeiro, os registros ecc_queue inseridos por meio de scripts não suportados (se detectados) não são autenticados. **Importante:** A segurança elevada é necessária para modificar esta propriedade.
com.glide.codesigning.tracking.validation.fail_first	verdadeiro | falso	Quando verdadeiro, a verificação de assinatura de código falha na primeira falha de validação do script em vez de verificar todos os scripts. **Importante:** A segurança elevada é necessária para modificar esta propriedade.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Propriedade	Tipo	Descrição
com.glide.event_handler.code_signing.tracking	Cadeia de caracteres	Define o manipulador de eventos que ajuda a garantir que os clientes que habilitarem recentemente a assinatura de código sejam configurados para serem o mais seguros possível. **Importante:** A segurança elevada é necessária para modificar esta propriedade.
com.glide.web_service_outbound.impl.v2.codesigning.tracking	verdadeiro | falso	Quando verdadeiro, habilita o rastreamento de assinatura de código SOAPMessageV2 **Importante:** A segurança elevada é necessária para modificar esta propriedade.
com.snc.csf.servicenow_root_of_trust.disabled	verdadeiro | falso	Se o recurso Raiz de confiança está ativo. O valor padrão é `falso`, o que significa que os certificados de compilação ServiceNow são confiáveis. **Importante:** Esta propriedade só pode ser alterada usando um trabalho agendado assinado de um usuário com as funções de administrador, administrador de segurança e gerente do KMF. Para obter detalhes sobre como mudar sua Raiz de confiança, consulte Mudar a configuração de Raiz de confiança.
com.snc.kmf.signature.validation.optin	verdadeiro | falso	Quando verdadeiro, habilita a assinatura de código na sua instância. **Importante:** Esta propriedade só pode ser alterada por meio de uma solicitação para Suporte e atendimento ao cliente. Para obter mais informações, consulte KB1205749
glide.jdbcprobeloader.tracking	verdadeiro | falso	Ativa ou desativa a assinatura de código para fontes de dados JDBC.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Propriedade	Tipo	Descrição
		Importante: A segurança elevada é necessária para modificar esta propriedade.
glide.rest.codesigning.tracking	verdadeiro | falso	Quando verdadeiro, habilita o rastreamento de assinatura de código RESTMessageV2. **Importante:** A segurança elevada é necessária para modificar esta propriedade.

Funções instaladas com a Assinatura de código

A Assinatura de código inclui as seguintes funções.

Administrador de assinatura de código [codesigning_admin]

Use a função de administrador de assinatura de código para atribuir as funções codesigning_manager e codesigning_auditor a outros usuários.

Contém funções

Lista de funções contidas na função.

Nenhum.

Grupos

Lista de grupos aos quais esta função está atribuída por padrão.

Nenhum.

Considerações especiais

Evite conceder uma função de administrador quando houver mais funções especializadas disponíveis.

Gerente de assinatura de código [codesigning_manager]

Use a função de gerente de assinatura de código para criar e atualizar a configuração de assinaturas e criar e executar trabalhos de assinatura de código.

Contém funções

Lista de funções contidas na função.

Nenhum.

Grupos

Lista de grupos aos quais esta função está atribuída por padrão.

Nenhum.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Considerações especiais

Nenhum.

Auditor de assinatura de código [codesigning_auditor]

Use a função de auditor de assinatura de código para exibir configurações e trabalhos de assinatura. A função de auditor não tem acesso de criação ou gravação para ativos de assinatura de código.

Contém funções

Lista de funções contidas na função.

Nenhum.

Grupos

Lista de grupos aos quais esta função está atribuída por padrão.

Nenhum.

Considerações especiais

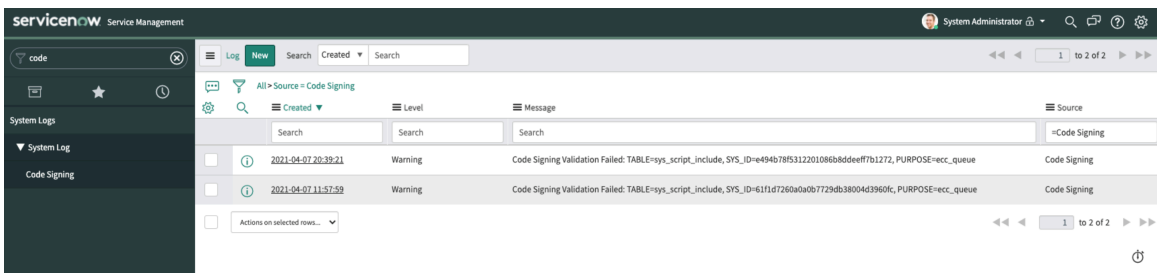
Nenhum.

Solução de problemas e acesso a logs

Acesse vários logs para solucionar problemas e identificar os motivos da falha.

Logs de assinatura de código

Se algum dos registros de fila do ECC não estiver assinado pela API do rastreador de assinatura de código , as mensagens não assinadas e os detalhes necessários serão exibidos no módulo de Assinatura de código. Navegue até **Logs do sistema** > **Log do sistema** > **Assinatura de código** para acessar a lista de registros que não são confiáveis.



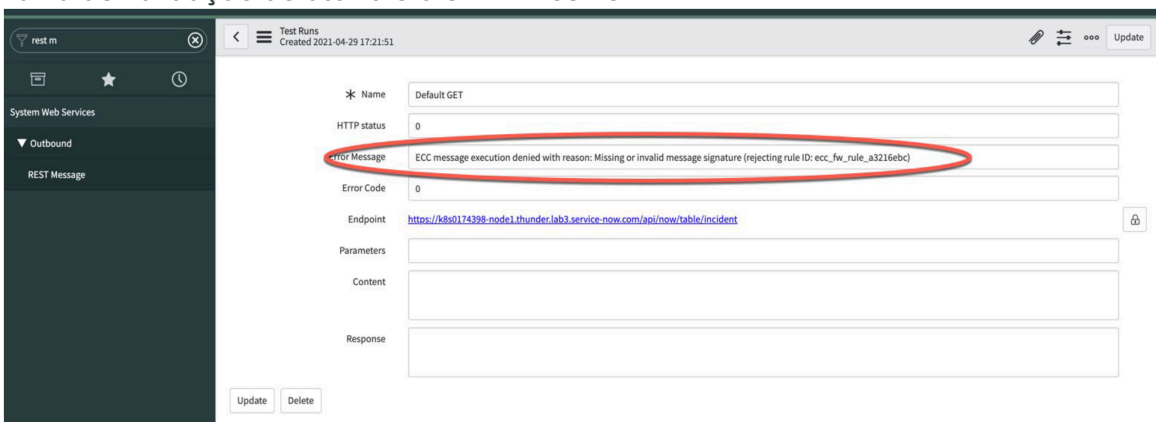
Para os logs de nó de depuração adicionais, habilite *com.glide.codesigning.tracking.debug* e configure seu valor para `verdadeiro`.

Falha na validação de assinatura de mensagem REST em MID Server

Acesse a mensagem de erro relacionada à falha de validação de assinatura, navegando até **Serviços Web do sistema** > **Saída** > **Mensagem REST** e abrindo o registro de mensagem REST necessário.

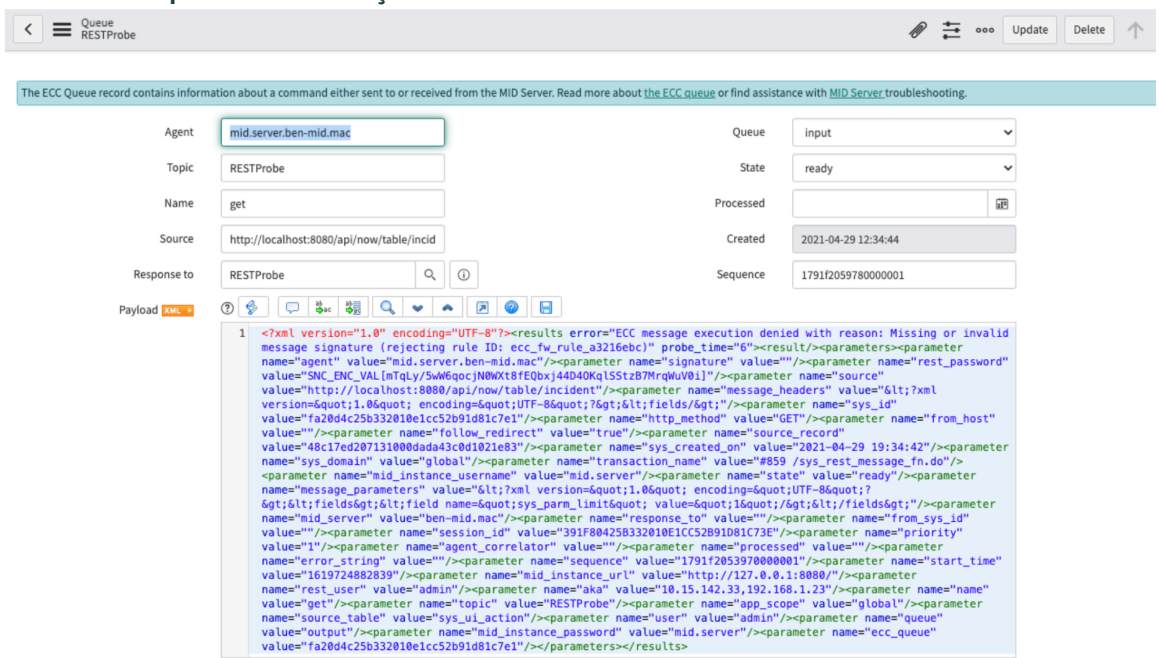
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Falha de validação de assinatura em MID Server

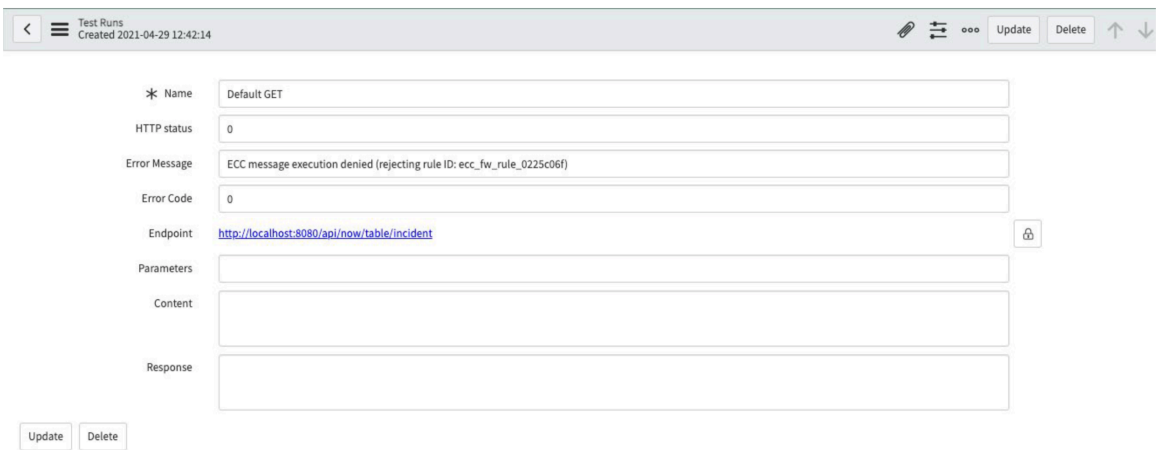


Nota: As mensagens de erro relacionadas às rejeições de firewall do ECC começam com a `execução de mensagem do ECC negada`.

Fila do ECC quando a validação da assinatura falha no MID Server



Mensagem de erro quando a mensagem do ECC é bloqueada pela regra do usuário

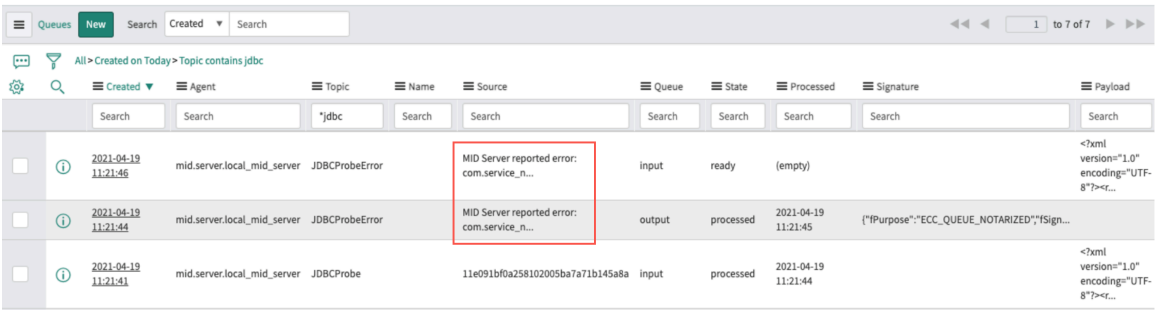


© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Probe JDBC

Quando uma fonte de dados JDBC com uma assinatura ausente ou inválida for executada em um MID Server, será exibida uma mensagem de erro com os detalhes necessários.

A **origem** também exibe os detalhes da mensagem de erro.



MID Server logs

Para habilitar o log do firewall do ECC detalhado, aumente o nível de log configurando o valor do parâmetro de configuração MID Server, *`mid.log.level`*, como `TRACE`. Os logs detalhados fornecem informações sobre:

- Regras que o MID Server carregou do arquivo de configuração de inicialização.
- Rastreamento de execução granular de regras.
- Regra específica devido à qual uma mensagem do ECC deve ser aceita ou rejeitada.

Nota: Se `boot-config.xml` for inválido, o MID Server falhará em iniciar e os detalhes de falha serão registrados nos logs do agente MID.

Varredura antivírus

Use Varredura antivírus para ajudar a proteger sua instância contra infecções de vírus que podem ser introduzidas por anexos de arquivo aos registros do sistema, como incidentes, problemas e histórias.

Explore a varredura antivírus

Configure a proteção antivírus

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Conheça o valor da Varredura antivírus.

Entenda como configurar a proteção antivírus.

Resolva Arquivos infectados

Saiba o que fazer com arquivos infectados.

Referência de Varredura antivírus

Conheça os Atributos do Dicionário para a Varredura antivírus.

Explorar a Varredura antivírus

Use Varredura antivírus para ajudar a proteger sua instância contra infecções de vírus que podem ser introduzidas por anexos de arquivo aos registros do sistema, como incidentes, problemas e histórias.

Varredura antivírus verifica anexos de arquivo armazenados na tabela de anexos [sys_attachment] para ajudar a proteger os usuários contra o carregamento e o download de arquivos infectados. Todos os tipos de documentos compatíveis com a plataforma são verificados pela Varredura Antivírus.

O plug-in Proteção antivírus (com.glide.snap) está ativado e habilitado por padrão em sua instância. Como administrador, é possível desativar e reativar o recurso Varredura antivírus em sua instância no comutador de uma alternância, definir opções de configuração e revisar a atividade de antivírus na instância.

Nota:

- O Varredura antivírus também está disponível para clientes na GCC (Government Community Cloud) e no ambiente comercial. Os usuários devem definir a propriedade (com.glide.snap.fed_enable_scan) como Verdadeiro para começar a usar o recurso.
- Os protocolos de comunicação HTTP e HTTPS são suportados.
- Arquivos criptografados pelo Edge são excluídos desta verificação.
- As definições de antivírus são atualizadas todos os dias.
- Qualquer arquivo com mais de 100 MB não é verificado.

Verificação de e-mails e anexos

Os e-mails de entrada são verificados quanto a vírus pelo sistema filtros de e-mail, não pela Varredura antivírus.

Por padrão, somente anexos vinculados a tabelas zz_yylive_profile são verificados. Para verificar outras tabelas que têm o tipo de coluna **file_attachment**, crie a propriedade do sistema `com.glide.snap.scan.zz_yytables` e insira o nome da tabela.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Se os nomes das tabelas forem zz_yyincident e zz_yycase, o valor da propriedade deverá ser *zz_yyincident,zz_yycase*.

Depois que essa propriedade for definida, os anexos das tabelas zz_yyincident e zz_yycase serão verificados.

Cenários de verificação

Analise esses cenários de carregamento e download para entender como o sistema identifica as possíveis ameaças à segurança de arquivos anexados aos seus registros.

Cenário 1 - Carregar um arquivo

1. Sem saber, o usuário carrega um arquivo infectado em um registro.
2. O sistema verifica o arquivo e o deixa em quarentena.
3. O arquivo aparece na janela Anexos, onde fica marcado como indisponível.
4. O usuário seleciona o arquivo e esta mensagem de erro é exibida: `O arquivo Infected_testing.txt não passou na verificação de segurança. Remova o arquivo do registro INC0000059 e tente novamente.`
5. O sistema envia uma notificação por e-mail ao usuário e ao administrador do antivírus.
6. O usuário fecha a janela Anexos e retorna ao registro. O arquivo infectado é exibido no cabeçalho como indisponível. Exemplo, `infected_testing123.txtZ [unavailable]`.

Cenário 2 - Baixar um arquivo

1. O usuário abre um registro para baixar um arquivo anexado a ele.
2. Sem saber que o arquivo está infectado, o usuário o seleciona para download.
3. O sistema verifica o arquivo, deixa-o em quarentena e exibe uma mensagem semelhante a `O arquivo infectado_testing123.txt não passou na verificação de segurança e não pode ser baixado.`
4. O usuário fecha a mensagem e a tela é atualizada mostrando que o arquivo está indisponível.
5. O sistema envia uma notificação por e-mail ao usuário e ao administrador do antivírus.

Cenário 3 - Baixar um arquivo ZIP

1. Um usuário abre um registro e baixa um arquivo ZIP anexado a ele.
2. O sistema verifica os arquivos ZIP individualmente.
3. Um arquivo não passa na verificação de segurança e fica marcado como indisponível. Os arquivos restantes são compactados e baixados com sucesso.
4. O usuário abre o arquivo ZIP e vê um arquivo "error.txt" além do arquivo baixado com sucesso. Este arquivo contém uma mensagem de erro que especifica qual arquivo não passou na verificação e, portanto, não foi incluído no ZIP.
5. O usuário abre o registro novamente e vê que o arquivo indisponível foi movido para a seção **Possíveis riscos de segurança**, na janela Anexos, e não pode ser baixado.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configuração do Varredura antivírus

Configure Varredura antivírus em sua instância e no nível de tabela.

Antes de Iniciar
Função necessária: antivirus_admin ou administrador

Por Que e Quando Desempenhar Esta Tarefa
Varredura antivírus fica ativo por padrão em sua instância, onde verifica automaticamente os anexos para identificar todos os arquivos que estão infectados por vírus. Configure o recurso garantindo que a verificação esteja habilitada em sua instância e identificando todas as tabelas que deseja excluir da verificação.

Procedimento

1. Navegue até **Todos** > **Antivírus** > **Configuração**.
2. Conforme configura o recurso, considere o seguinte.

Opção	Descrição
Habilitar varredura antivírus	A varredura antivírus fica ativa e habilitada na instância por padrão, sua alternância é definida para a posição Ligada e aparece na cor verde. **Nota:** Para definir a propriedade como `falsa`, entre em contato com o suporte ao cliente.
Permitir que anexos sejam baixados quando o scanner do Antivírus não estiver disponível	Se esta opção estiver definida na posição Ligada, a varredura antivírus será ignorada se o scanner chegar ao tempo limite e não for possível obter uma resposta. Nesta situação, o download do arquivo continua sem concluir a verificação. Se a opção estiver definida como desativada, o download do arquivo será proibido até que a verificação seja concluída com êxito.
Lista de Tabelas Excluídas	Todos os anexos de arquivo associados a uma tabela nesta lista são excluídos da varredura antivírus. Prossiga para a Etapa 4 se quiser definir as tabelas que o sistema exclui da verificação.

3. Selecione **Salvar**.
4. Exclua as tabelas da verificação do Antivírus adicionando-as à **Lista de tabelas excluídas**.
   a. Navegue até **Definição do sistema→ Dicionário**.
   b. Pesquise a tabela que deseja excluir da verificação e selecione a tabela com o Tipo definido como coleção.
   c. Na guia **Atributos**, selecione **Novo**.
   d. Adicione `Exclude_from_antivirus_scan` no campo Atributos e insira `Verdadeiro` no campo **Valor**.
   e. Selecione **Enviar**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resultados
O Varredura antivírus está habilitado na sua instância e a **Lista de tabelas excluídas** na página Configuração do Antivírus é preenchida com todas as tabelas que você excluiu da verificação.

Revisar arquivos em quarentena

Revise os anexos de arquivo em quarentena e execute ações adicionais necessárias.

Antes de Iniciar
Função necessária: antivirus_admin ou administrador

Por Que e Quando Desempenhar Esta Tarefa
Monitore suas entradas de arquivo em quarentena na página Quarentena do Antivírus em intervalos regulares para executar qualquer uma das ações a seguir.

Procedimento

1. Navegue até **Todos** > **Antivírus** > **Quarentena**.
2. Marque a caixa de seleção ao lado de cada entrada em quarentena na qual deseja executar uma ação disponível.
3. Selecione o menu suspenso **Ações nas linhas selecionadas** na faixa para escolher a ação a ser realizada na entrada da linha selecionada em quarentena.

Ação	Descrição
Excluir	Selecione esta ação para excluir o arquivo em quarentena se ele não for mais necessário para os usuários.
Restaurar	Selecione esta ação para restaurar o arquivo com base na avaliação do status ou na solicitação do usuário. No entanto, verifique o arquivo com o produto antivírus de terceiros antes de restaurá-lo para atenuar quaisquer ameaças de vírus. Depois de restaurado, o arquivo fica disponível para download para o usuário.
Baixar	Selecione esta ação para baixar o arquivo para o seu sistema local para verificação e análise adicionais.

Resultados
O sistema solicita confirmação e executa a ação selecionada de acordo com sua entrada.

Informações relacionadas

Central de segurança da instância

Métricas de antivírus

Analisar a atividade do antivírus

Analise o registro em log de Atividades do Antivírus que rastreia todas as atividades que ocorrem em arquivos potencialmente infectados a partir do ponto em que são descobertos e colocados em quarentena.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: antivirus_admin ou administrador

Por Que e Quando Desempenhar Esta Tarefa
Este log funciona como um relatório que captura a atividade do antivírus, como descoberta, exclusão e outros possíveis eventos de arquivo em quarentena.

Procedimento
1. Navegue até **Todos** > **Antivírus** > **Atividade**.
2. Analise o registro em log de arquivos em quarentena.
   É possível exibir as ações realizadas na coluna Evento para cada arquivo em quarentena.

O que Fazer Depois
Determine quais registros deseja excluir, restaurar, baixar ou manter no log. Consulte Analisar arquivos em quarentena

Conhecer os atributos do Dicionário para Varredura antivírus

Os atributos do dicionário alteram o comportamento da tabela ou do elemento que o registro do dicionário descreve. Como administrador, é possível definir os valores dos atributos do dicionário para modificar o comportamento da configuração padrão da Varredura Antivírus.

Atributos do dicionário para Varredura antivírus

Nome	valor	Elemento de destino	Descrição
Exclude_from_antivirus_scan	verdadeiro/falso	qualquer tabela	Se verdadeiro, os anexos de arquivo na tabela serão excluídos da verificação do antivírus. Veja Configuração do Varredura antivírus
Supress_antivirus_email_notification	verdadeiro/falso	qualquer tabela	Se verdadeiro, para de enviar notificações por e-mail geradas pela plataforma quando um arquivo potencialmente infectado for identificado.
Suppress_antivirus_ui_notification	verdadeiro/falso	qualquer tabela	Se verdadeiro, vai parar as notificações de IU geradas pela plataforma quando um arquivo potencialmente infectado for identificado.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Informações relacionadas

Como alterar tabelas e campos usando atributos de dicionário

Limpador de HTML

Remova o código indesejado e proteja-se contra problemas de segurança, como ataques de script entre sites, limpando a marcação HTML nos campos HTML e nos campos HTML traduzidos.

Explore o limpador de HTML

Saiba como o limpador de HTML funciona.

Configure o limpador de HTML

Configure o limpador de HTML.

Ative o limpador de HTML

Saiba como habilitar o limpador de HTML.

Explorar o limpador de HTML

Remova o código indesejado e proteja-se contra problemas de segurança, como ataques de script entre sites, limpando a marcação HTML nos campos HTML e nos campos HTML traduzidos.

Use a limpeza de HTML para garantir que o conteúdo HTML em sua instância não contenha conteúdo potencialmente prejudicial. A limpeza de HTML funciona removendo marcadores HTML que podem ser usados para comprometer sua instância, como marcadores `<script>`, `<link>` ou `<embed>` que podem ser usados para executar scripts indesejados em sua instância ou direcionar seus usuários para conteúdo indesejado. Os marcadores seguros que controlam a formatação do seu conteúdo são preservadas. Como administrador, você pode personalizar o conteúdo removido ou preservado. Você também pode controlar se a limpeza se aplica a todo o conteúdo ou apenas aos campos especificados.

O limpador de HTML funciona verificando se há marcação que você queira manter preservada na lista de inclusões internas. O limpador fornece a inclusão de script

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

HTMLSanitizerConfig que os administradores podem usar para modificar a lista de inclusões interna. Também podem ser adicionados itens à lista de exclusões para remover a marcação HTML. Os conteúdos da lista de exclusões substituem a lista de inclusões.

Os seguintes tipos de itens podem ser adicionados às listas de inclusão e exclusão:

- Atributos globais
- Quaisquer elementos HTML

Nota: Por padrão, atributos de URL como `href` e `src` são compatíveis somente com estes protocolos:

- `http`
- `https`
- `mailto`
- `dados`

Por exemplo:

```
<a href="https://community.servicenow.com/community">ServiceNow
 Community</a>
```

Nota: Para aprender mais sobre a propriedade *glide.html.sanitize_all_fields* que controla o uso do limpador de HTML, consulte Limpador de HTML nas Configurações de proteção de segurança de instância.

Configurar urlAttributes e os protocolos

Você pode configurar o urlAttributes e seus protocolos na inclusão de script **HTMLSanitizer**. Por exemplo:

```
HTML_WHITELIST : {
urlAttributes: { "protocols" : [ "file", "notes" ] },
                 -  -
                 -  -
        }
```

Como `anotações` está na lista de inclusões neste exemplo, este URL não foi limpo:

```
<a title="Lotus"
 href="Notes://
ABC/X575C90019DE33/ABC594DCB76D86EB4925653E0011C4C1/ZZ90B7E2D33964749257E
EA003456FD">Lotus</a></p>
```

Lista de inclusões padrão

Nota: A lista de inclusões padrão é uma lista do sistema e não pode ser acessada por usuários na instância.

```
BUILTIN_HTML_WHITELIST :{

    globalAttributes:{ attribute:["id","class","lang","title","style"],

                                  attributeValuePattern:{}},

    label:{ attribute:["for"]},
```

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

```
    font:{ attribute:["color","face","size"]},

    a:{ attribute:["href","nohref","name","shape"]},

 img:{ attribute:["src","name","alt","border","hspace","vspace","align","
height","width"},

 table:{ attribute:["border","cellpadding","cellspacing","bgcolor","backg
round","align","no resize","height","width","summary","frame","rules"]},

 th:
{ attribute:["background","bgcolor","abbr","axis","headers","scope","nowr
ap","height","width","align","valign","char
 off","char","colspan","rowspan"]},

 td:
{ attribute:["background","bgcolor","abbr","axis","headers","scope","nowr
ap","height","width","align","valign","char
 off","char","colspan","rowspan"]},

    tr:{ attribute:["background","height","width","align","valign","char
 off","char"]},

    thead:{attribute:["align","valign","char off","char"]},

    tbody:{attribute:["align","valign","char off","char"]},

    tfoot:{attribute:["align","valign","char off","char"]},

    colgroup:{attribute:["align","valign","char
 off","char","span","width"]},

    col:{attribute:["align","valign","char off","char","span","width"]},

    p:{attribute:["align"]},

    style:{attributeValuePattern:{"type":"text/css"}}

    canvas:{ attribute:["height","width"]},

    details:{ attribute:["open"]},

    summary:{ attribute:["open","valign","char off","char"]},

    button:{ attribute:["disabled","accesskey","type"]},

    form:{},

 input:{ attribute:["size","maxlength","checked","alt","src","type","disa
bled","readonly","accesskey","border","usemap"]},
```

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

```
   select:{ attribute:["disabled","multiple","size"]},

textarea:{ attribute:["rows","cols","disabled","readonly","accesskey"]},
   option:{ attribute:["disabled","label","selected"]},
   div:{ attribute:["align"]},
   ol:{ attribute:["start","type","square"]},
   ul:{ attribute:["type","square","itemscope","itemtype","itemref"]},
   li:{ attribute:["value","fb__id","itemprop"]},

span:{ attribute:["color","size","data-mce-bogus","itemprop","face"]},
   br:{ attribute:["clear"]},
   h3:{ attribute:["itemprop"]},
   html:{ attribute:["xmlns","lang","xml:lang"]},
   link:{ attribute:["rel","type","href","charset"]},
   meta:{ attribute:["name","content","scheme","charset","http-equiv"]},
   pre:{ attribute:["xml:space"]},
   noscript:{},    h1:{},    h2:{},      h4:{},    h5:{},    h6:{},
   i:{},    b:{},    u:{},    strong:{},    em:{},    small:{},
big:{},
   pre:{},    code:{},    cite:{},    samp:{},    sub:{},    sup:{},
   strike:{},   center:{},  blockquote:{},    hr:{},      map:{},
   dd:{},    dt:{},    dl:{},  fieldset:{},    legend:{}, figure:{},
tt:{},
   body:{},   caption:{},   head:{},   title:{},  shape:{},},
```

Configurar o limpador de HTML

Você deve modificar uma inclusão de script para fazer mudanças de configuração no limpador de HTML.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Navegue até **Todos** > **Definição do sistema** > **Inclusões de script**.
2. Abra **HTMLSanitizerConfig**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Para adicionar itens à lista de exclusões, use a classe "HTML_BLACKLIST".

   Para adicionar itens à lista de inclusões, use a classe "HTML_WHITELIST".

   Use este formato:

```
HTML_XXXXLIST :{
        globalAttributes :{

            attribute:[attribute-name1,...],

 attributeValuePattern:{ attribute-name2:attribute-value-regex-pattern,
...}

        },<html-element-name>:{// Same as Above},----}
```

   - *globalAttributes* contém itens de atributo ou attributeValuePattern que são aplicáveis globalmente a todos os elementos HTML.
   - *attribute* é uma lista de atributos separados por vírgulas.
   - *attributeValuePattern* é um dicionário de atributos para pares atributo-valor-regex-padrão. "Atributo-valor-regex-padrão" é uma expressão regular que deve corresponder ao valor do atributo.

Example:
Considere o seguinte exemplo:

```
HTML_WHITELIST:{
        globalAttributes:{
            attribute:["id","name"],},
        img:{
            attribute:["style","align"],
            attributeValuePattern:{src:".*jpeg"}},
        iframe:{},}
```

Ele adiciona os seguintes itens à lista de inclusões:

- O ID e o nome dos atributos globais. Essa é uma lista de cadeias de caracteres que podem ser aplicadas globalmente a todos os elementos.
- O elemento "img" em que os atributos são estilizados e alinhados.
- O elemento "img" em que o atributo de origem da imagem é um arquivo com a extensão .jpeg. Este é um exemplo de um padrão de expressão regular que corresponde a um valor de atributo.
- O elemento "iframe".

Habilitar o limpador de HTML

O limpador de HTML fornece uma propriedade para habilitar ou desabilitar o limpador para todos os campos HTML no sistema.

Antes de Iniciar
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa
Por padrão, a propriedade é definida como verdadeira para novas instâncias.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. No filtro de navegação, insira `sys_properties.list`.
2. Defina as propriedades *`glide.html.sanitize_all_fields`* e *`glide.translated_html.sanitize_all_fields`* como **verdadeiras**.

> **Nota:** Para aprender mais sobre essa propriedade, consulte Limpador de HTML nas Configurações de proteção de segurança de instância.

Trouble?

Se as propriedades não existirem na tabela Propriedades do sistema, você poderá adicioná-las.

Habilitar a limpeza em campos individuais

Você pode usar atributos de campo para habilitar ou desabilitar o limpador em campos individuais.

Antes de Iniciar
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa
Primeiramente, você precisa definir a propriedade do limpador como falsa e, em seguida, habilitar o limpador por campo para qualquer formulário.

Procedimento

1. Navegue até a tabela "sys_properties" e defina *`glide.html.sanitize_all_fields`* como **falso**.
   Ela desabilita o limpador para todos os campos HTML no sistema.
2. Navegue até o formulário que contém o campo HTML.
3. Clique com o botão direito do mouse no rótulo do campo HTML e selecione **Configurar dicionário**.
   O formulário de entrada de dicionário é aberto para o campo HTML.
4. Insira um dos seguintes no campo Atributos:
   - Para desabilitar a limpeza, insira `html_sanitize=false`
   - Para habilitar a limpeza, insira `html_sanitize=true`
5. Clique em **Atualizar**.
6. Para habilitar o limpador de HTML para campos HTML traduzidos, defina a propriedade *`glide.translated_html.sanitize_all_fields`* como **verdadeira**.

Habilitar o registro em log do limpador de HTML

Quando o limpador de HTML remove elementos ou atributos, eles são adicionados ao log do sistema.

Antes de Iniciar
Função necessária: admin

Por Que e Quando Desempenhar Esta Tarefa
Você pode avaliar esses elementos limpos adicionando "/syslog_list.do?sysparm_query=source%3DHTMLSanitizer" ao URL da sua instância.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Avalie esses elementos limpos adicionando `/syslog_list.do?sysparm_query=source%3DHTMLSanitizer` ao URL da sua instância.
2. Para habilitar ou desabilitar o registro em log, adicione a propriedade `glide.html_sanitize.discarded_log.enable` às propriedades do sistema e defina o valor como **verdadeiro** (habilitado) ou **falso** (desabilitado).
   Essa propriedade será definida como **verdadeira** por padrão.

Auditoria

Rastreie mudanças de registro em tabelas habilitadas para auditoria. Por padrão, o sistema rastreia mudanças nas tabelas de incidentes, mudanças e problemas, entre outras.

Explorar

Conheça os recursos e valores comerciais da auditoria.

Configurar

Entenda como configurar a auditoria.

Exibir

Revise as tabelas de Auditoria do sistema e Mudança de relacionamento de auditoria.

Referência

Saiba mais sobre os conjuntos de históricos.

Explorar a auditoria

Rastreie mudanças de registro em tabelas habilitadas para auditoria. Por padrão, o sistema rastreia mudanças nas tabelas de incidentes, mudanças e problemas, entre outras.

A habilitação da auditoria rastreia a criação, a atualização e a exclusão de todos os registros na tabela. Se deseja auditar campos individuais em uma tabela, é possível ocultar os campos que não deseja rastrear usando um atributo de dicionário.

As informações de auditoria são mantidas nestas tabelas:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- A tabela Auditoria.
- A Conhecer os conjuntos de históricos tabela.

Aviso: Auditar tabelas do sistema que recebem uma grande quantidade de tráfego, tal como Contextos do fluxo de trabalho [wf_context] ou Alertas de gestão de eventos [em_alert], pode afetar o desempenho. Por esse motivo, não é possível auditar a tabela em_alert por inteiro. Em vez disso, audite os campos de interesse selecionados. Defina *audit=true* na tabela em_alert e nos campos selecionados. Tente auditar o menor número possível de campos.

Auditoria de tabelas primárias e secundárias

As tabelas não derivam os sinalizadores de auditoria das tabelas auditadas primárias ou secundárias.

- Por exemplo, se você habilitar a auditoria para a tabela Itens de configuração [cmdb_ci], somente os ICs armazenados nessa tabela base serão auditados.
- Da mesma forma, se você habilitar a auditoria para a tabela Computadores [cmdb_ci_computer], somente os registros de IC de computador serão auditados, incluindo quaisquer campos na tabela Computadores [cmdb_ci_computer] que forem derivados da tabela Itens de configuração [cmdb_ci].

Tabelas do sistema de auditoria

Por padrão, o sistema não audita a exclusão de um registro das tabelas do sistema. Para auditar uma tabela do sistema, adicione-a à lista de tabelas na *glide.ui.audit_deleted_tables* lista de propriedades.

Auditoria de exclusões de um formulário ou lista

Por padrão, o sistema audita exclusões de registros individuais de um formulário. Para evitar auditoria, defina o atributo de dicionário da tabela *no_audit_delete*.

O sistema audita exclusões de uma lista quando a **auditoria** é selecionada no dicionário de tabela, e a tabela não está listada na propriedade *glide.db.audit.ignore.delete*.

Nota: Por padrão, a propriedade *glide.db.audit.ignore.delete* não está presente na tabela Propriedade do sistema [sys_properties]. Para mudar a propriedade e seus valores associados, primeiro você deve adicioná-la manualmente. No entanto, quando adicionada manualmente, ela substitui os seguintes valores padrão:

```
glide.db.audit.ignore.delete =
sys_mutex,sys_db_cache,sys_lucene_block,sys_lucene_file,sys_lucene_directory,sys_use
cmdb_ci_windows_service, cmdb_sam_sw_install, cmdb_software_instance,
cmdb_sam_sw_usage, sam_sw_counter_detail
```

Para saber mais sobre a adição de propriedades do sistema, consulte Adicionar uma propriedade do sistema.

Por padrão, as exclusões de auditoria são habilitadas se o registro é excluído das visualizações do formulário e das exibições de lista ou por um script/trabalho agendado.

Informações auditadas

A auditoria rastreia as seguintes mudanças de registro:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Identificador de registro exclusivo (sys_id) do registro que mudou
- Campo que mudou
- Novo valor do campo
- Antigo valor do campo
- Número de vezes que este registro e campo foram atualizados
- Data e hora em que a mudança ocorreu
- Usuário que fez a mudança
- Motivo da mudança (se houver algum motivo associado à mudança)
- ID do ponto de verificação interno do registro, se o registro tiver várias versões.

Informações isentas de auditoria

Algumas atualizações não são auditadas, apesar de habilitar a auditoria em uma tabela. É por isso que você pode ver 132 atualizações no histórico de um registro, mas apenas sete auditadas.

A auditoria exclui as seguintes informações:

- Atualizações feitas por um upgrade.
- Atualizações são feitas por meio de conjuntos para importação.
- Registros em tabelas primárias ou secundárias.
- Campos com o atributo de dicionário no_audit.
- Tabelas do sistema não são listadas na lista de propriedades *glide.ui.audit_deleted_tables*.
- Campos que começam com sys_ prefix (campos do sistema), exceto as colunas sys_class_name e sys_domain_id.
- As Páginas de IU às vezes podem acionar atualizações para um registro sem criar um log de auditoria.
- Sempre que um monitor de inatividade toca um registro. Isso evita que você possivelmente veja centenas de atualizações listadas em relação a um incidente, com o ruído minando os dados úteis.
- Mudanças manuais para Performance Analytics pontuações.

Auditoria de uma tabela

Para obter instruções sobre como auditar uma tabela, consulte Configurar auditoria para uma tabela.

Por padrão, o sistema rastreia todos os campos em uma tabela auditada. É possível auditar um subconjunto de campos em uma tabela de uma das duas maneiras:

- É possível habilitar a auditoria para a tabela inteira e excluir os campos que não deseja incluir. Isso é apropriado quando você deseja auditar a maioria dos campos, mas não todos, e é conhecido como uma lista de exclusões. Para obter mais informações, consulte Excluir um campo de ser auditado (listagem de exclusões).
- É possível habilitar a auditoria para a tabela, mas somente para os campos especificados. Isso é apropriado quando você deseja auditar apenas um pequeno número de campos da tabela e isso é conhecido como uma lista de inclusões. Para obter informações sobre como incluir um campo usando a lista de inclusões, consulte Incluir um campo de tabela na auditoria (lista de inclusões).

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Registros de auditoria não canceláveis

Reduza as chances de os registros de auditoria não serem registrados quando uma transação for cancelada com a nova configuração padrão.

As auditorias foram definidas para criar um registro imediatamente na mesma transação com as operações de gravação do registro de destino. Se o registro de destino for excluído, a auditoria ainda será criada e mantida no módulo **Exclusão de auditoria de teste NCA**.

Nota: O processo aprimorado de auditoria fica habilitado por padrão. Se a propriedade `glide.db.audit.lacy` estiver definida como `Verdadeira`, o processo aprimorado de auditoria será desabilitado.

Antes da versão Xanadu, quando uma transação era cancelada, determinadas operações auditáveis não eram registradas. Isso porque a plataforma executava algumas operações entre a mudança de registro e era cancelada antes da criação da auditoria. Mas, agora, as auditorias são criadas imediatamente após o registro ser alterado, reduzindo as chances de uma transação cancelada anular a operação antes que a auditoria seja registrada.

As auditorias são registradas no mesmo thread da transação. As auditorias anteriores eram criadas em um thread em segundo plano. Esta mudança redefine o valor padrão da propriedade `glide.db.audit.lazi` de Verdadeiro para Falso. Em geral, essa propriedade não é definida na tabela Propriedades, pois a maioria das instâncias começa usando o novo valor e comportamento padrão. Em algumas instâncias, essa propriedade pode já estar presente e definida como Verdadeira, ou seja, essas instâncias não poderão usar a mudança para auditar o comportamento.

Nota: É recomendável excluir essa propriedade para aproveitar a atualização.

Configurar auditoria para uma tabela

É possível habilitar a auditoria da tabela para rastrear mudanças para todos ou alguns dos campos da tabela.

Antes de Iniciar

Função necessária: administrador

Nota: Por natureza, os campos criptografados não são auditados. Este comportamento não é configurável.

Procedimento

1. Navegue até **Todos** > **Definição do sistema** > **Dicionário**.
   O sistema exibe a lista de entradas do dicionário. A lista inclui uma linha para cada tabela, bem como uma linha para cada coluna (campo) na tabela.
2. Na lista de entradas do dicionário, localize a linha correspondente à tabela que você deseja auditar, por exemplo `cmdb_ci_computer`.
   É possível distinguir a linha da própria tabela – versus uma linha para uma coluna na tabela – encontrando a linha com o nome de tabela correto, uma entrada vazia para o nome **Coluna** e um **Tipo** de **Coleção**.
3. Selecione a entrada do dicionário para a tabela.
   O sistema exibe o formulário de entrada do dicionário.
4. Marque a caixa de seleção **Auditoria**.
5. Selecione **Atualizar**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O que Fazer Depois

Se deseja auditar apenas alguns campos na tabela Habilitar auditoria da lista de inclusão para uma tabela. Se você desejar auditar a maioria dos campos, mas quiser excluir alguns, consulte Excluir um campo de ser auditado (listagem de exclusões).

Habilitar auditoria da lista de inclusão para uma tabela

Habilite uma tabela para auditar somente os campos que você designar explicitamente. Isso é útil quando você deseja auditar apenas um pequeno número de campos em uma tabela auditada.

Antes de Iniciar

Função necessária: administrador
A tabela deve ser habilitada para auditoria.

Procedimento

1. Navegue até **Todos** > **Definição do sistema** > **Dicionário**.
   O sistema exibe a lista de entradas do dicionário. A lista inclui uma linha para cada tabela, bem como uma linha para cada coluna (campo) na tabela.
2. Se necessário, personalize a exibição da lista para mostrar a coluna **Atributos**.
3. Na lista de entradas do dicionário, localize a linha correspondente à tabela que você deseja auditar, por exemplo `cmdb_ci_computer`.
   É possível distinguir a linha para a própria tabela – em comparação a uma linha para uma coluna na tabela – encontrando a linha com o nome de tabela correto, uma entrada vazia para o nome Coluna e um tipo de *`collection`*.
4. No campo **Atributos** para essa linha, insira *`audit_type=whitelist`*.

O que Fazer Depois

Designe quais campos você deseja auditar nesta tabela.

Excluir um campo de ser auditado (listagem de exclusões)

Impeça que o Now Platform rastreie o subconjunto de campos em uma tabela auditada excluindo esses campos de uma auditoria.

Antes de Iniciar

Função necessária: administrador
Para excluir um campo em uma tabela sendo auditada, primeiro você deve habilitar a auditoria para essa tabela.

Por Que e Quando Desempenhar Esta Tarefa

Adicione um conjunto de campos a uma lista de exclusões quando quiser auditar a maioria dos campos em uma tabela auditável. Se deseja auditar apenas alguns campos, siga o procedimento de listagem de inclusão em vez disso.

> **Nota:** Desabilitar a auditoria em campos baseados em diário pode afetar a funcionalidade de recursos, como o Formatador de atividades. Para obter mais informações, consulte KB0743142.

Procedimento

1. Navegue até **Todos** > **Definição do sistema** > **Dicionário**.
2. Se necessário, personalize a exibição da lista para mostrar a coluna **Atributos**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Navegue até a linha correspondente à tabela e ao campo (coluna) que deseja excluir da auditoria.
4. Na coluna **Atributos** para essa linha, insira `no_audit`.

Incluir um campo de tabela na auditoria (lista de inclusões)

Rastreie um subconjunto de campos em uma tabela auditada adicionando esses campos a uma lista de inclusões.

Antes de Iniciar

Função necessária: administrador

Para adicionar campos em uma tabela a uma lista de inclusões, primeiro você deve habilitar a auditoria para essa tabela e habilitar a auditoria de lista de inclusões para essa tabela.

Por Que e Quando Desempenhar Esta Tarefa

Adicione um conjunto de campos a uma lista de inclusões quando desejar auditar apenas um pequeno número de campos da tabela auditada. Se precisar auditar a maioria dos campos e excluir apenas alguns, siga o procedimento da lista de exclusões em vez disso.

Procedimento

1. Navegue até **Todos** > **Definição do sistema** > **Dicionário**.
2. Se necessário, personalize a exibição de lista para mostrar a coluna **Atributos**.
3. Navegue até a tabela e o campo (coluna) desejado para a lista de inclusões.
4. No campo **Atributos**, insira *`audit=true`*.

Habilitar auditoria para uma tabela de sistema

As exclusões de tabelas com um prefixo sys_ não são auditadas por padrão. Para rastrear exclusões dessas tabelas, adicione o nome da tabela à propriedade *`glide.ui.audit_deleted_tables`*. Habilitar o plug-in Restaurar registros excluídos adiciona vários valores padrão a esta propriedade.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Navegue até **Todos** > **Propriedades do sistema** > **Propriedades de IU**.
2. Localize a **Lista de tabelas do sistema (iniciando com "sys_", separado por vírgula) que terá a** propriedade de excluir auditado.
3. Adicionar ou remover nomes de tabelas. Os nomes da tabela devem ser separados por vírgulas, sem espaços.
4. Clique em **Salvar**.

> **Nota:** Para obter mais informações sobre auditoria, consulte Entendendo a tabela de auditoria do sistema.

Visualizar tabelas de auditoria do sistema e de mudança de relacionamento de auditoria

O Now Platform rastreia as inserções e atualizações para registros auditados nas tabelas Auditoria do sistema (sys_audit) e Mudança de auditoria do sistema (sys_audit_relation).

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O Now Platform rastreia tabelas de auditoria. Para rastrear tabelas, marque a caixa de seleção **Auditoria** no registro do dicionário para definir o valor como verdadeiro. Por padrão, ele não audita registros de tabelas do sistema, como tabelas de conjuntos para atualização.

Nota: Para evitar problemas de desempenho e loops infinitos, o sistema ignora qualquer regra de negócios ou fluxo de trabalho acionado por inserções na tabela Auditoria do sistema.

Colunas da tabela de auditoria do sistema

As seguintes colunas aparecem nos registros da tabela sys_audit:

Campo	Descrição
Nome da tabela	Tabela à qual se destina o registro de auditoria (por exemplo, "`incidente`")
Nome do campo	Coluna na tabela para a qual o registro de auditoria se destina (por exemplo, "`assigned_to`")
Chave do documento	Sys_id (identificador de registro exclusivo) para o registro de origem associado ao registro de auditoria.
Usuário	Nome do usuário que criou a mudança. **Nota:** Alguns processos automatizados usam o sistema ou o usuário convidado para aplicar e rastrear mudanças nos registros. Para obter mais informações, consulte Usuários do sistema e convidados.
Valor antigo	O valor antigo da mudança do campo representado por este registro sys_audit. • Campos de referência: valor sys_id exclusivo do registro alterado. • Campos de data e hora: valor em Coordinated Universal Time (UTC) conforme armazenado no banco de dados.
Novo valor	Novo valor da mudança do campo representado por este registro sys_audit. • Campos de referência: valor sys_id exclusivo do registro alterado. • Campos de data e hora: valor em Coordinated Universal Time (UTC) conforme armazenado no banco de dados.

Como funciona a tabela Mudança de relacionamento de auditoria (sys_audit_relation)

A tabela Auditoria do sistema [sys_audit] rastreia mudanças nos campos de referência em tabelas que são sinalizadas para auditoria. Esta atividade inclui entradas de campo de diário e conjuntos de históricos. A tabela Mudança de relacionamento de auditoria [sys_audit_relation] rastreia as mudanças de relacionamento entre os registros da tabela sys_audit e as tabelas de origem das quais os registros auditados se originam. Ela também rastreia quando um registro pode ter sido excluído.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

-
- Sempre que você audita qualquer registro em uma tabela, um relacionamento é criado entre as várias tabelas de origem para o armazenamento que registra os dados. Essas informações de relacionamento são salvas nas tabelas sys_history_set, sys_history_line e sys_journal.
- Se você excluir um campo que está relacionado a um registro de tabela auditado, a tabela sys_audit_relation registrará a exclusão. Em outras palavras, sempre que você alterar um registro auditado, ele primeiro excluirá os elementos anteriores e, em seguida, criará um relacionamento na tabela sys_audit_relation com novos IDs de documento.

Conhecer os conjuntos de históricos

O sistema gera automaticamente registros de Conjunto de históricos conforme necessário na tabela de Auditoria quando um usuário cria um registro ou exibe seu histórico.

Se um registro estiver em uma tabela auditada, seu conjunto de históricos será gerado quando o registro for inserido ou quando um usuário exibir o registro.

Nota: Não use conjuntos de históricos para gerar relatórios.

Vários campos de informações são capturados no registro de Conjunto de históricos, mostrado na exibição de lista.

Campos de Registro de Exibição de Lista

Campo	Valor de entrada
ID	ID do documento para o registro cujo histórico está sendo registrado.
Tabela	Tabela para o registro cujo histórico está sendo registrado.
Tempo de carregamento	Quantidade de tempo necessária para gerar o conjunto de históricos.

Campos de registro de histórico de auditoria

Campo	Valor de entrada
Rótulo	O rótulo do campo que foi alterado.
Antigo	Valor antes da mudança.
Novo	Valor após a mudança.
Tipo	Indica se a entrada é para um campo normal, um registro de e-mail ou um registro de mudança de relacionamento.
Número de upgrade	O número de vezes que este campo foi alterado. Um valor de -1 indica quando o registro foi criado ou excluído.
Hora de atualização	Data e hora da mudança

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campos de registro de histórico de auditoria

Campo	Valor de entrada
	Nota: A hora de atualização das linhas de histórico geradas automaticamente não corresponde à hora de criação ou de atualização de um registro em uma situação de processamento específica. Quando você exibe um conjunto de históricos de um registro pela primeira vez, um conjunto inicial de registros de linha de histórico é gerado automaticamente. Como as mudanças de arquivo em um upgrade não são auditadas, essa incompatibilidade de data ocorre quando: • Você exibe um conjunto de históricos após ser feita uma mudança em um registro, mas • Antes que outra mudança seja feita nele em um upgrade futuro.
Nome de usuário	Nome do usuário que criou a mudança.

Conjuntos de históricos em uma exibição de calendário

Depois que os Conjuntos de históricos ficam ativos, a opção de menu de contexto do Histórico é preenchida usando informações do conjunto de históricos, em vez da tabela `sys_audit`. Da perspectiva do usuário, os mesmos dados históricos ficam disponíveis na mesma interface do usuário, mas a forma como as informações são armazenadas é diferente.

Como a exibição de Histórico inclui uma exibição de calendário, mas não usa a interface de lista normal para filtrar e interagir com os registros de histórico, ela permite:

- Pesquisar e filtrar dados históricos.
- Exportar dados.

Exibição de conjuntos de históricos

Há duas maneiras de exibir o histórico definido, acessíveis por meio do **Histórico** de ação do Menu de Contexto.

Diferenças entre auditoria e conjuntos de históricos

As tabelas Auditoria [sys_audit], Conjuntos de históricos [sys_history_set] e Histórico [sys_history_line] armazenam os mesmos dados, mas servem a diferentes propósitos e gerenciam os dados de forma diferente.

Tabela Auditoria [sys_audit]

A tabela Auditoria [sys_audit] fica onde o sistema armazena informações históricas para todos os registros. Esses registros devem ser mantidos indefinidamente para que os administradores possam sempre rastrear o histórico de registros auditados. Conforme o número de registros de auditoria aumenta ao longo do tempo, se torna mais ineficiente consultar diretamente a tabela de auditoria para obter informações de histórico. É muito mais eficiente executar consultas somente nos registros de subconjunto menor dos quais você realmente deseja exibir informações históricas.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela Conjunto de históricos [sys_history_set]

A tabela Conjunto de históricos [sys_history_set] identifica quais registros específicos de uma tabela auditada têm informações de histórico. A tabela Histórico [sys_history_line] armazena as mudanças reais nos valores de campos que ocorreram.

- O sistema gera automaticamente os registros de Conjunto de históricos e Histórico conforme necessário a partir da tabela Auditoria quando um usuário cria um registro ou solicita seu histórico.
- Em vez de conter um histórico completo de todas as mudanças no sistema, os registros de Conjunto de históricos e Histórico contêm apenas um subconjunto recente de informações históricas para registros em que os usuários criaram ou solicitaram essas informações.
- Além dos dados de auditoria, os conjuntos de históricos também incluem informações definidas durante a inserção do registro, incluindo entradas de campo de diário. As entradas de campo de diário que você cria antes da criação de um registro são tratadas da mesma maneira que as entradas de diário criadas no momento da criação do registro. Essas entradas de diário aparecem em conjuntos de históricos que possuem a mesma hora de criação e dados sobre quem criou que o registro associado em si.

O sistema limita os registros Conjunto de históricos e Histórico por:

- Fazer com que o limpador de tabela exclua os registros Conjunto de históricos que não foram atualizados em 30 dias.
- Usar a rotação de tabela para girar entre quatro tabelas de histórico a cada sete dias. O sistema descarta registros de Histórico com mais de 28 dias.

Se alguém precisar de informações de histórico novamente em uma data posterior, o sistema pode gerá-las novamente a partir de registros de origem de auditoria.

Depois que o sistema gera registros de Conjunto de históricos, a opção de menu de contexto **Histórico** usará o Conjunto de históricos em vez de registros de Auditoria. Da perspectiva do usuário, os mesmos dados históricos ficam disponíveis na mesma interface do usuário, mas a maneira como as informações são armazenadas é diferente.

Controlar o acesso ao histórico

É possível conceder a uma função acesso para exibir o histórico de auditoria, definindo uma propriedade do sistema.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Navegue até **Todos** > **Propriedades do sistema** > **Sistema**.
2. Selecionar a propriedade *glide.history.role* na tabela.
3. Em *List of roles (comma-separated) that can access the history of a record*, selecione as funções do usuário que deseja para acessar o histórico.
4. Selecione **Salvar**.

Resultados

Quaisquer mudanças em um campo serão omitidas, se um usuário sem acesso de leitura exibir o histórico de um registro.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mudar o número de entradas do histórico

Por padrão, o histórico exibe no máximo 250 entradas de histórico, mas é possível mudar este valor.

Antes de Iniciar

Função necessária: administrador

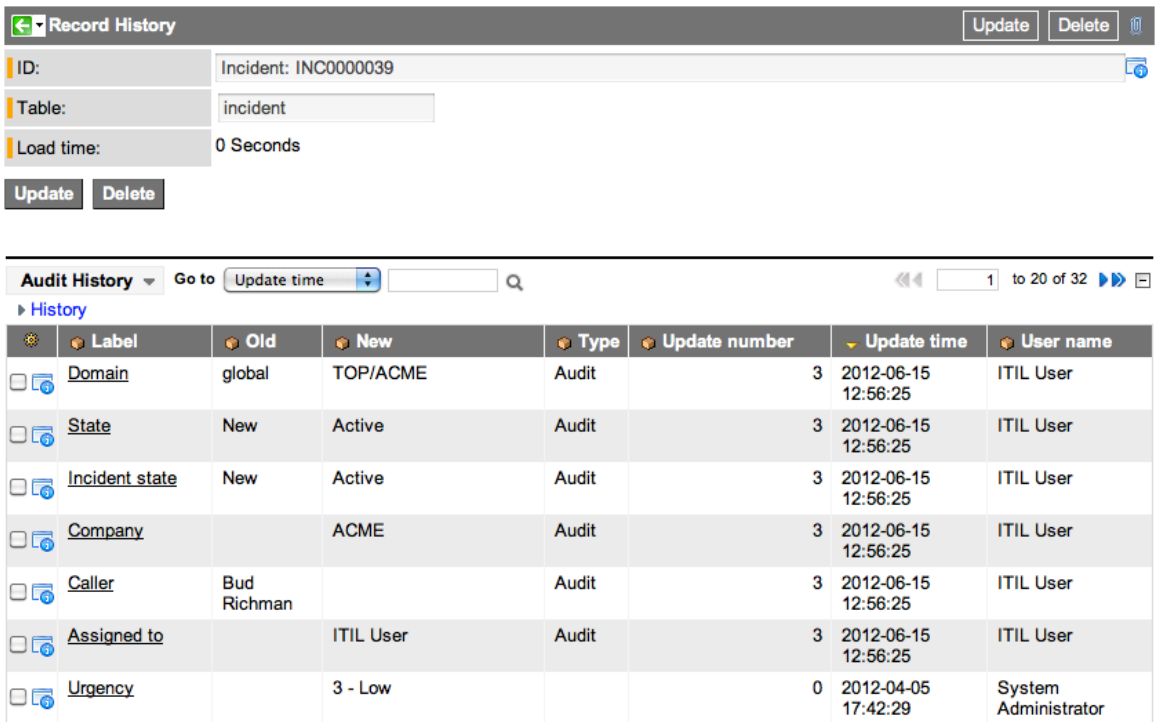
Procedimento

1. Navegue até **Todos** > **Propriedades do sistema** > **Sistema**.
2. Selecione a propriedade *glide.history.max_entries*.
3. Defina o valor *Maximum number of field entries displayed in record history, default is 250* com um novo número máximo de entradas a serem exibidas.

Lista de históricos

A lista de históricos exibe cada mudança como sua própria linha na lista de mudanças.

Exibir Lista de históricos

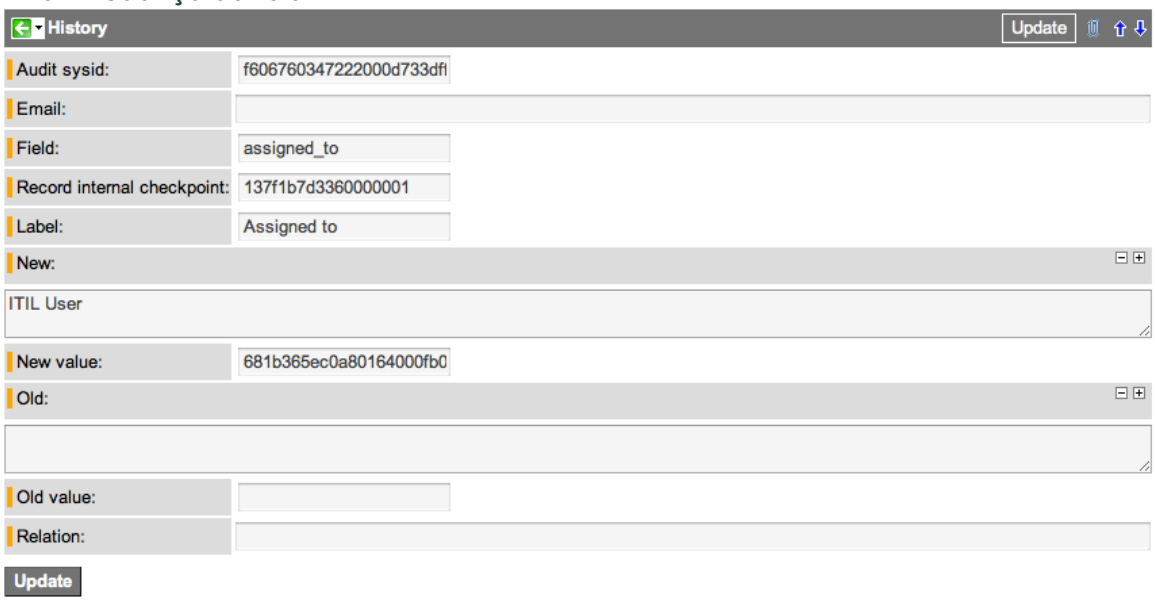


Label	Old	New	Type	Update number	Update time	User name
Domain	global	TOP/ACME	Audit	3	2012-06-15 12:56:25	ITIL User
State	New	Active	Audit	3	2012-06-15 12:56:25	ITIL User
Incident state	New	Active	Audit	3	2012-06-15 12:56:25	ITIL User
Company		ACME	Audit	3	2012-06-15 12:56:25	ITIL User
Caller	Bud Richman		Audit	3	2012-06-15 12:56:25	ITIL User
Assigned to		ITIL User	Audit	3	2012-06-15 12:56:25	ITIL User
Urgency		3 - Low		0	2012-04-05 17:42:29	System Administrator

Clique em um item de linha para exibir detalhes adicionais sobre a mudança.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exibir mudança da lista



Requisitos

Para exibir uma lista de históricos, os seguintes requisitos devem ser atendidos.

Auditoria

A auditoria da tabela deve estar habilitada para exibir uma lista de históricos.

ACLs

Por padrão, a opção de histórico *Lista* está disponível apenas para usuários com a função do usuário administrador. Para habilitar esta opção para não administradores, crie uma regra de ACL personalizada concedendo acesso de leitura para a tabela Histórico de registro [sys_history_set].

Funções

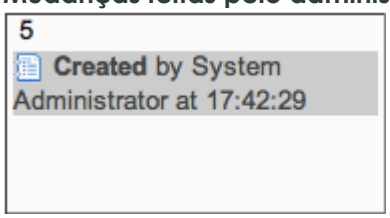
Pelo menos uma das funções que o usuário tem deve ser incluída na *glide.history.role* propriedade, que inclui a função itil por padrão.

Calendário de histórico

O calendário de histórico mostra os dias em que o registro foi alterado, quem fez a mudança e quando.

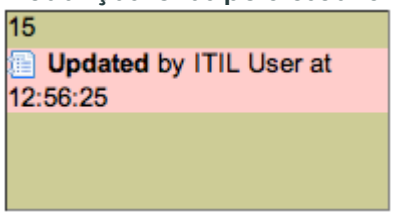
O Calendário de histórico é classificado por número de atualização. Cada usuário é atribuído a uma cor para que seja possível saber rapidamente quantas vezes um registro foi alterado por um usuário específico. Por exemplo:

Mudanças feitas pelo administrador do sistema



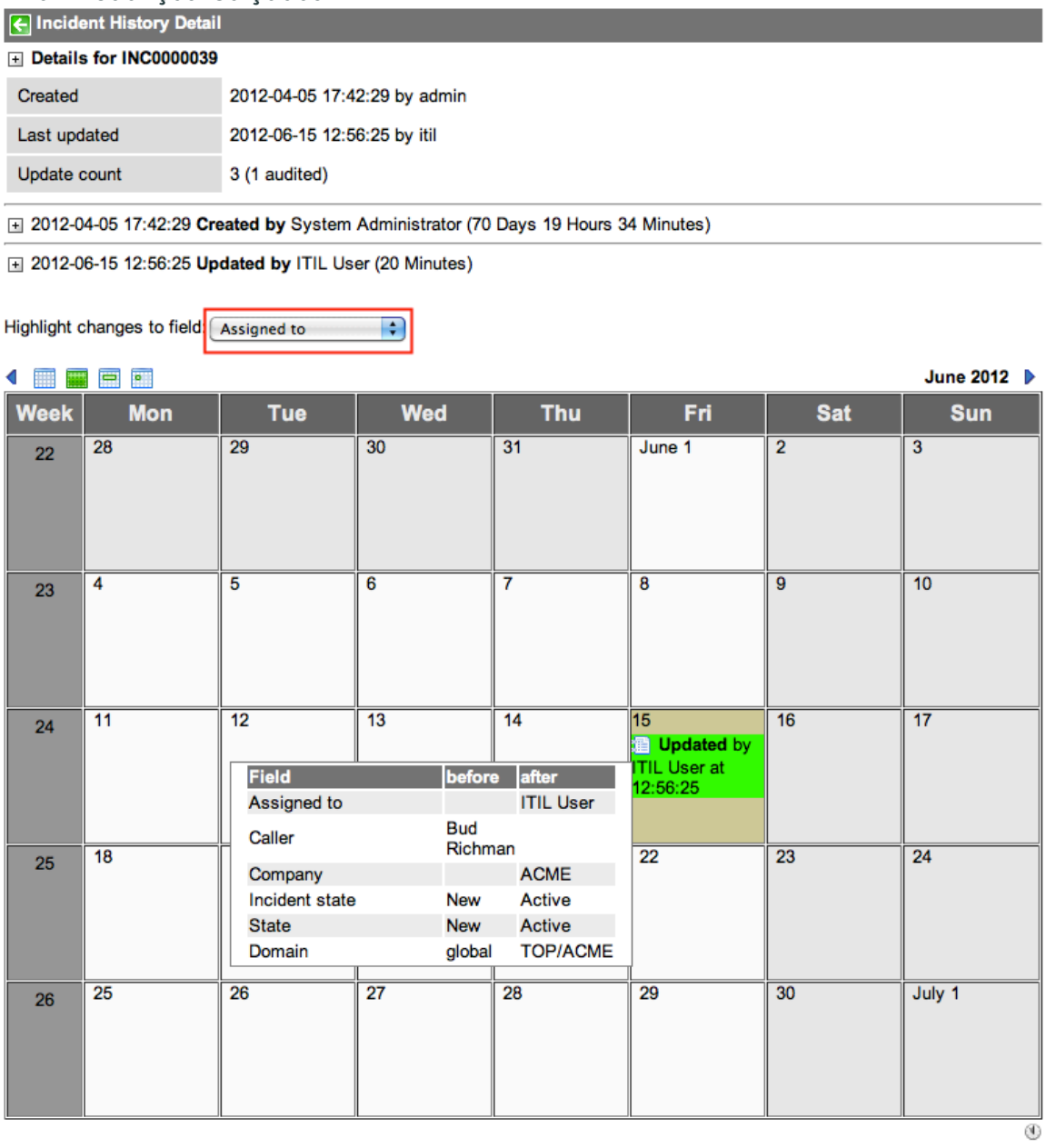
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mudanças feitas pelo usuário ITIL



Para realçar mudanças em um campo específico, marque o campo na caixa de seleção **Realçar mudanças no campo**. Escolher um campo nesta caixa de seleção muda o calendário para realçar as horas em que esse campo foi alterado. Passe o mouse sobre o texto de uma das mudanças realçadas para ver a mudança no valor.

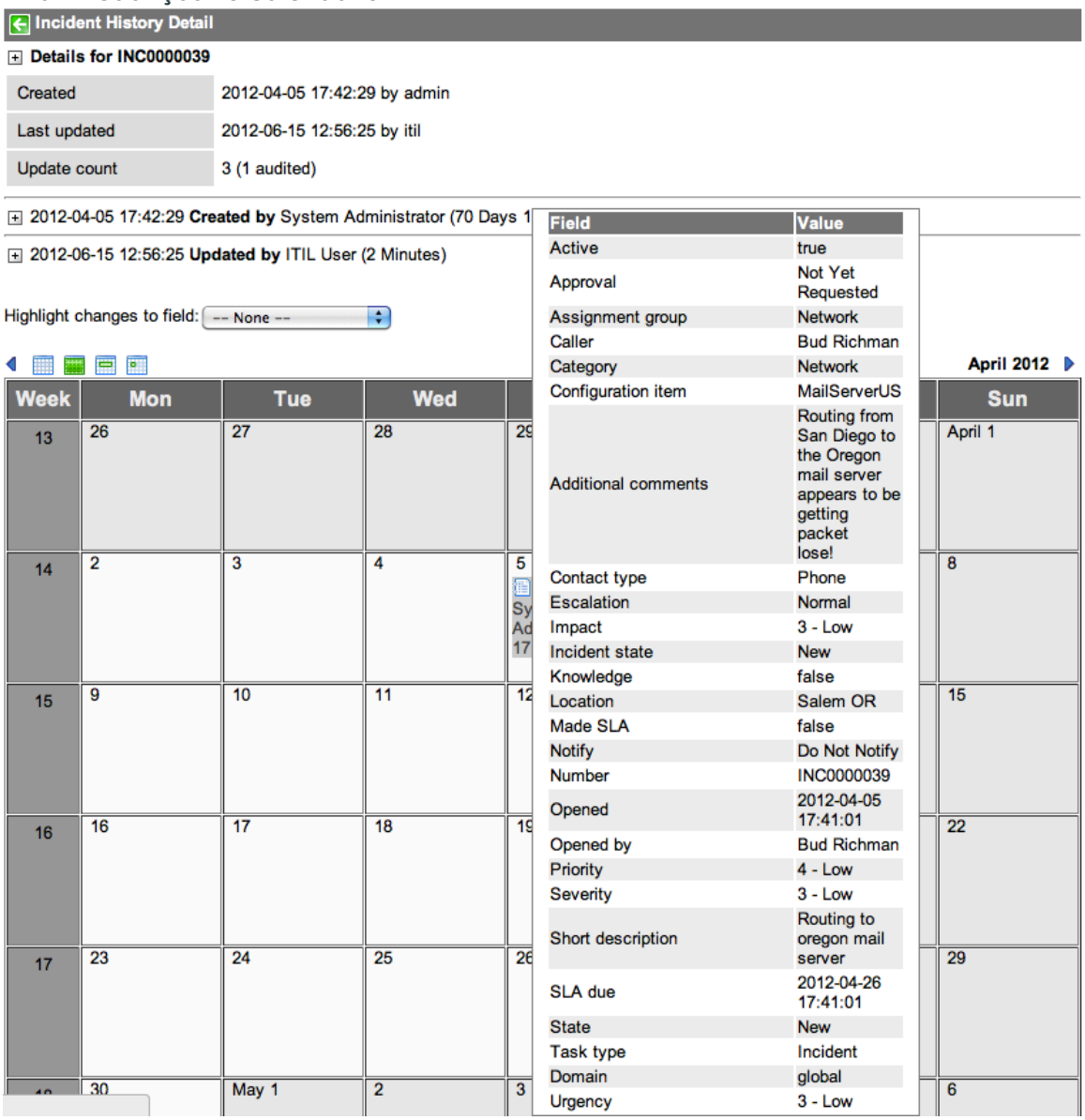
Exibir mudanças realçadas



Se você passar o mouse sobre o ícone em uma entrada, um pop-up exibirá todas as mudanças de valor. Essas são as mesmas informações exibidas na parte superior do formulário.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exibir mudanças no calendário



É possível clicar no número do dia para obter uma exibição das mudanças desse dia. Também é possível clicar no número da semana à esquerda para obter a exibição da semana. É possível rolar para e de mês a mês para ver as mudanças.

Linha do tempo do Histórico

É possível exibir uma linha de tempo de mudanças para um CI e para seus registros relacionados, relacionamentos, linhas de base e mudanças propostas para CI. As linhas de tempo estão disponíveis para ICs na tabela Item de configuração [cmdb_ci] ou em um descendente desta tabela, se a auditoria estiver habilitada para as tabelas.

Função necessária: a ACL para esta exibição é baseada nas funções definidas na propriedade do sistema *glide.history.role*, que por padrão é definida como `itil`. Além disso, o usuário deve ter acesso de leitura para a tabela Conjunto de históricos [sys_history_set], que por padrão é concedido como administrador.

É possível abrir uma linha do tempo ao exibir o histórico de um IC. É possível especificar o período de tempo, o intervalo de tempo e as propriedades que são exibidas na linha do tempo. É possível exibir o que mudou em um conjunto de mudanças específico ou exibir o CI inteiro para solucionar melhor os problemas. Também é possível exibir uma linha do

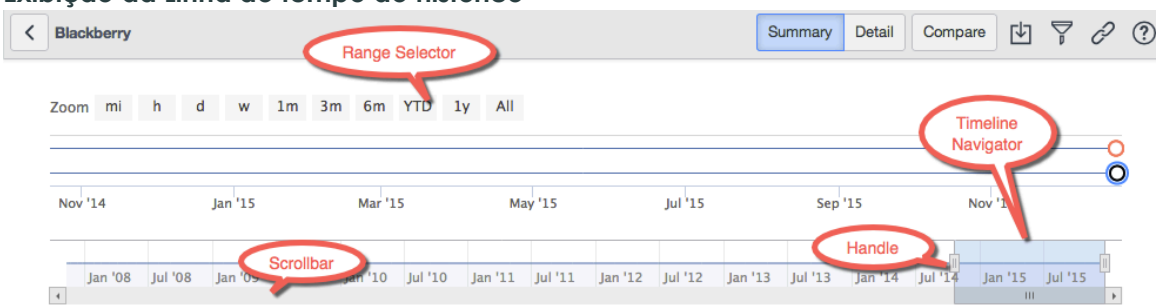
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

tempo de mudanças para os registros relacionados do IC e exportar e comparar snapshots do IC em qualquer momento.

As mudanças de IC são representadas por bolhas em diferentes formas e cores ao longo da linha do tempo. A forma de cada bolha representa um tipo diferente de mudança e a cor de cada bolha especifica se a mudança é válida ou inválida. As linhas de base de IC são representadas por círculos pretos sobre os quais você pode passar o mouse para exibir mais detalhes. Clique no ícone **?** para exibir a forma da bolha e as definições de cor e apontar para uma bolha para exibir detalhes sobre o conjunto de mudanças.

Uma mudança em um relacionamento é considerada válida somente se tiver sido aplicada por meio da gestão de mudanças. Se a mudança tiver sido aplicada por meio da estrutura de mudanças propostas, ela será válida. Para obter etapas de validação adicionais, consulte Criação ou edição de um script de validação planejado .

Exibição da Linha do tempo do histórico



Bolhas da Linha do tempo

Nota: Mudanças propostas que não possuem uma data de início planejada são colocadas em pontos de tempo futuros.

Navegador da linha do tempo

Use as alças em ambas as extremidades do navegador da linha do tempo para estender ou encurtar o período de tempo mostrado.

É possível rolar para um período de tempo diferente clicando na parte inferior do navegador da linha do tempo e então arrastando o navegador para a esquerda ou direita.

Zoom

Por padrão, a linha do tempo do último mês é mostrada. Ao lado do rótulo **Zoom** acima da linha do tempo, é possível selecionar outro intervalo de tempo. É possível selecionar intervalos de um minuto até o período inteiro de dados.

Se houver muitas mudanças do IC durante o período de tempo, as bolhas exibidas podem ficar muito cheias. É possível ampliar ou reduzir para espalhar as bolhas em qualquer um dos métodos:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Altere o intervalo de tempo na linha do tempo. Conforme reduz o intervalo de tempo, você aumenta o zoom e, conforme aumenta o intervalo de tempo, você reduz o zoom.
- Selecione a seção da linha do tempo que deseja ampliar.

Filtro de propriedade

É possível filtrar as bolhas exibidas. Por padrão, todas as bolhas são exibidas, representando mudanças em todas as propriedades do IC. É possível limitar a exibição para mostrar somente as bolhas nas quais as propriedades selecionadas mudaram e excluir as bolhas nas quais somente as propriedades não selecionadas mudaram.

As exibições **Detalhe** e **Resumo** realçam as propriedades em seu escopo de filtro que mudaram. As propriedades alteradas são realçadas em azul claro.

Na exibição **Resumo**, é possível optar por incluir todas as propriedades do IC ou somente as propriedades que foram alteradas. Se você optar por exibir todas as propriedades na exibição de resumo, as propriedades alteradas serão listadas antes das propriedades inalteradas.

Exibição de resumo

A exibição **Resumo** mostra snapshots dos ICs representados por cada bolha.. Cada snapshot exibe as mudanças nos campos e relacionamentos do IC de acordo com o conjunto de mudanças. Ele exibe valores antigos e novos antes e depois da mudança e todos os relacionamentos que foram adicionados ou excluídos.

Use os botões **>** e **<** em ambos os lados da exibição do snapshot para rolar pelos registros de conjunto de mudanças anteriores e seguintes em ordem cronológica.

Exibição de detalhe

A exibição **Detalhe** mostra snapshots de CI que correspondem às bolhas. Cada snapshot inclui os campos que estão dentro do escopo do filtro de propriedade, exibindo as propriedades que foram alteradas com um plano de fundo azul claro. Clique em uma bolha para exibir seu snapshot correspondente do CI. Os dados exibidos são somente leitura.

Use os botões **>** e **<** em ambos os lados para rolar pelos registros de conjunto de mudanças anteriores e seguintes em ordem cronológica.

Exibir linha do tempo de mudanças nos registros relacionados

Na linha do tempo de mudanças de um registro de CI, você também pode exibir uma linha do tempo de mudanças para os registros relacionados ao CI.

Antes de Iniciar

Função necessária: administrador

- Tabela de destino: o registro de CI deve estar na tabela Item de configuração [cmdb_ci] ou ser um descendente desta tabela.
- Auditoria: deve estar habilitada para a tabela que contém o CI.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Abra a linha do tempo do CI.
2. Selecione o ícone **Registros relacionados** e selecione registros relacionados na **Lista de registros relacionados** a serem exibidos.
   Clique no ícone Registros relacionados novamente para exibir a linha do tempo dos registros relacionados.

Resultados

A linha do tempo de mudanças nos registros relacionados do CI é exibida logo acima da linha do tempo do CI. Se você desmarcar todos os registros relacionados, a linha do tempo dos registros relacionados ficará oculta.

O que Fazer Depois

Passe o mouse sobre uma bolha de mudança na linha do tempo de registros relacionados para exibir detalhes sobre a mudança, como data e número de propriedades alteradas. Conforme muda o intervalo de tempo em foco, ou aumenta ou diminui o zoom, isso afeta a linha do tempo do CI e a linha do tempo dos registros relacionados simultaneamente.

Exportar um snapshot de um CI

É possível exportar um snapshot de um IC de sua linha do tempo.

Antes de Iniciar

O IC deve estar na tabela Item de configuração [cmdb_ci] ou em um descendente desta tabela. A auditoria deve estar habilitada para a tabela que contém o CI.
Função necessária: administrador.

Por Que e Quando Desempenhar Esta Tarefa

É possível exportar um snapshot do IC para um formato XML, PDF (Portal) ou PDF (Paisagem).

Procedimento

1. Abra a linha do tempo do IC.
2. Selecione a bolha que representa o tempo para o qual deseja exportar um snapshot do IC.
3. Clique no ícone de exportação ( ).
4. Selecione o formato de arquivo a ser usado para a exportação.
   É possível baixar o arquivo para o seu sistema para exibição.

Comparar snapshots do CI

É possível comparar as propriedades e os relacionamentos de um CI em dois pontos diferentes em sua linha do tempo.

Antes de Iniciar

O IC deve estar na tabela Item de configuração [cmdb_ci] ou em um descendente desta tabela. A auditoria deve estar habilitada para a tabela que contém o CI.
Função necessária: administrador.

Procedimento

1. Abra a linha do tempo do CI.
2. Clique em **Comparar**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Selecione uma data de **Início** e uma data de **Término**.
4. Clique em **Comparar**.

Rastreando mudanças para campos de referência

Os administradores podem rastrear mudanças nos valores de exibição do campo de referência.

Como os campos de referência armazenam apenas um valor de ID, o sistema normalmente só pode auditar mudanças quando o valor de ID muda. Por padrão, o sistema não audita mudanças quando o valor de exibição de um campo de referência muda.

Considere a seguinte situação. Um usuário muda seu nome de Jane Smith para Jane Miller. Como o nome de usuário é o valor de exibição da tabela Usuário, qualquer referência anterior a Jane Smith se refere, em vez disso, a Jane Miller. Se o administrador apenas atualizar o nome do registro do usuário existente, os registros de auditoria e histórico exibirão somente o novo nome Jane Miller. Por padrão, o sistema não fornece uma maneira de distinguir entre as mudanças feitas com o nome de usuário original e as feitas com o novo nome de usuário.

Se sua política de auditoria exigir o rastreamento de mudanças de nome de usuário, você poderá:

- Criar um novo registro de usuário para o novo nome e desativar o registro de usuário anterior. O sistema preserva registros de auditoria para o antigo nome de usuário e cria registros de auditoria futuros com o novo nome de usuário.
- Crie campos personalizados e uma regra de negócios para salvar o nome anterior e a data da mudança de nome. O sistema pode usar essas informações para construir os nomes apropriados em registros de auditoria e de histórico.

Acompanhamento de inserções

Por padrão, o sistema não cria registros de Auditoria para inserções porque, em uma instância típica, as inserções podem representar mais de 80% do tamanho da tabela de Auditoria.

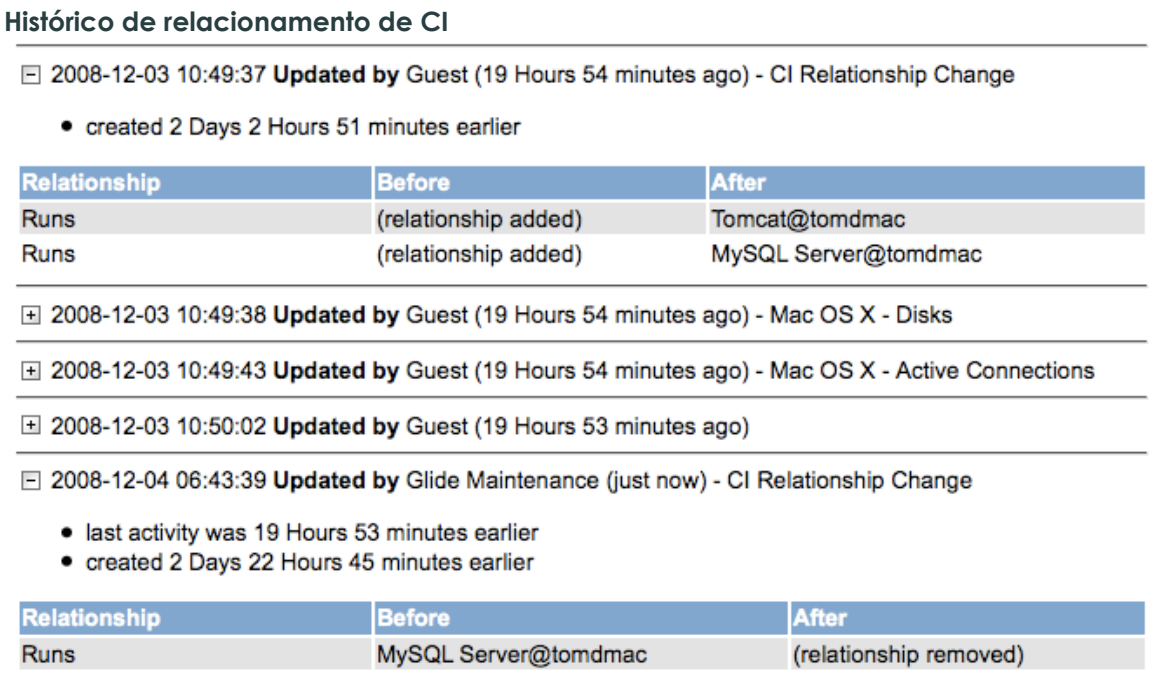
Não rastrear as inserções permite melhor desempenho e uma tabela de auditoria muito menor. Os administradores podem habilitar a auditoria de inserções definindo a *`glide.sys.audit_inserts`* propriedade para *verdadeira*.

Rastreamento dos relacionamentos de IC

As mudanças em um relacionamento de IC (relações de IC, relações de IC/Usuário ou Relações de IC/Grupo) aparecem no histórico dos itens em ambos os lados do relacionamento alterado independentemente de a mudança ter sido manual ou um resultado de Descoberta.

Por exemplo, se o computador alfa tem uma relação usada pelo IC com o computador beta, então o histórico para alfa tem um registro de quando o relacionamento com beta foi estabelecido, e da mesma forma, o histórico para beta tem um registro de quando o relacionamento com alfa foi estabelecido. Este exemplo ilustra o histórico exibido quando algumas relações de CI são estabelecidas e, em seguida, uma das relações é removida:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



O marcador criado indica a data em que o CI, o usuário ou o grupo foi criado. O último marcador de atividade se refere à quando os relacionamentos foram alterados. Se não deseja mostrar o histórico de relacionamento de CI para qualquer ou todos os tipos de relacionamento de CI, é possível desativá-lo desabilitando a auditoria nas tabelas de relacionamento CI (relacionamento de CI [`cmdb_rel_ci`], Tipo de relacionamento de CI/Usuário [`cmdb_rel_user_type`] ou Relacionamento de grupo [`cmdb_rel_group`]).

Configurações de Alta Segurança

As Configurações de alta segurança se referem a várias opções de segurança disponíveis em sua instância.

Explore as Configurações de alta segurança

Conheça os recursos e valores comerciais da Configurações alta segurança.

Ative as Configurações de alta segurança

Ative as Configurações de alta segurança.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Defina as Configurações de alta segurança

Entenda como definir as Configurações de alta segurança.

Explorar configurações de alta segurança

As Configurações de alta segurança se referem a várias opções de segurança disponíveis em sua instância.

O módulo Configurações de alta segurança é ativado com o plug-in High Security Settings, que está ativo por padrão em novas instâncias. Se as Configurações de alta segurança não estiverem ativas em sua instância, consulte Como solicitar a ativação das Configurações de alta segurança. Para saber mais sobre este plug-in, consulte Plug-in High Security nas Configurações de proteção de segurança da instância. Propriedades para estes tipos de configurações de alta segurança estão disponíveis:

- Valores de propriedade padrão: para fortalecer a segurança em sua plataforma, centralizando todas as configurações de segurança críticas em um local para gestão e auditoria.
- Propriedade de negação padrão: fornece uma propriedade de gerenciador de segurança para controlar o comportamento de segurança padrão para acesso à tabela.
- Função de administrador de segurança: fornece uma função para impedir a modificação das principais configurações e recursos de segurança. A função de administrador de segurança não é herdada pela função de administrador e deve ser atribuída explicitamente.
- Privilégios elevados: permite que usuários com a função de administrador de segurança operem no contexto de um usuário normal e elevem para função de segurança superior quando necessário.
- Controles de acesso à propriedade: permite que os administradores de segurança definam as funções necessárias para ler e gravar propriedades.
- Logs do sistema: são somente leitura.
- Regras de controle de acesso: controle quais dados os usuários podem acessar e como eles podem acessá-los.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

- As configurações de alta segurança também ativam automaticamente o plug-in de segurança contextual, se ainda não estiver ativo. Além disso, as configurações de segurança da plataforma - Alta fornecem configurações e recursos no contexto de aumentar a segurança da sua instância.
- O conteúdo das Configurações de proteção da segurança da instância contém descrições detalhadas e valores de conformidade para as propriedades do sistema relacionadas à segurança e plug-ins em Now Platform. Para saber mais sobre cada uma dessas propriedades, consulte Configurações de proteção de segurança da instância.
- Para saber mais sobre cada uma dessas propriedades, consulte Configurações de proteção de segurança da instância.

Existem duas maneiras de definir ou alterar as propriedades de Configurações de alta segurança.

- Navegue até a **Segurança do sistema** > **High Security Settings**.

  As opções na página Propriedades de alta segurança são **Sim** ou **Não**.

- Navegue até **sys_properties.list** e pesquise a propriedade que você deseja definir ou mudar.

  As opções na tabela Propriedades do sistema [sys_properties.list] são **verdadeiras** ou **falsas**.

Controle de acesso à propriedade

Duas colunas adicionais são criadas na tabela Propriedades [sys_properties] quando as configurações de alta segurança estão ativas:

- **read_roles**: uma lista separada por vírgulas de nomes de função que têm permissão para ler todos os campos desta propriedade.
- **write_roles**: uma lista separada por vírgulas de nomes de função que têm permissão para gravar/modificar todos os campos dessa propriedade.

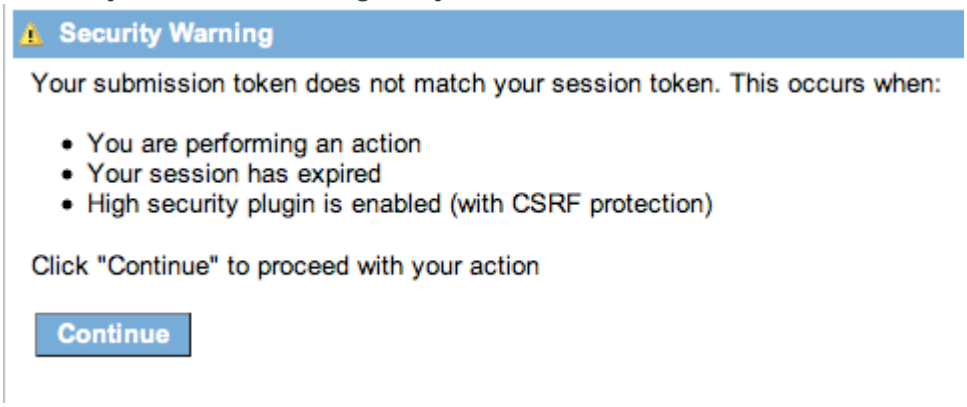
As propriedades listadas na tabela Propriedades têm **read_roles** de administrador e **write_roles** de security_admin. Usuários com a função de administrador podem exibir e ler os valores da propriedade, mas devem ser elevados à função security_admin para modificá-los.

Notificações

A ativação de configurações de alta segurança também ativa mensagens de aviso de segurança. A seguir está um exemplo de uma mensagem que aparece após uma aprovação.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Notificação de Aviso de Segurança



Propriedades de Configurações de alta segurança

Propriedade	Descrição	Valor Padrão	Configurações de proteção de segurança da instância
glide.ui.escape_text	Valores XML de escape no nível do analisador para a interface do usuário. Impede ataques de script entre sites refletidos e armazenados. Esta propriedade não é aplicável no portal de serviços. **Nota:** Essa propriedade é definida como **true** por padrão em Vancouver e versões posteriores, e não pode ser alterada pelos administradores. Para um caso de uso em que a propriedade precise ser alterada, entre em contato com o suporte ao cliente.	Sim	Escapar do XML
glide.ui.escape_all_script	Força todas as expressões no Jelly JavaScript `<script`	Sim em novas instâncias	Escapar do Jelly

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Propriedade	Descrição	Valor Padrão	Configurações de proteção de segurança da instância
	`type="text/javascript">` tags a serem escapadas por padrão. Impõe o escape somente se o atributo de tipo no marcador `<script>` estiver em branco ou se o valor for `text/javascript`, `text/ecmascript`, `application/javascript`, `application/ecmascript` ou `application/x-javascript`.		
glide.ui.rotate_sessions	Rotaciona os identificadores de sessão HTTP para reduzir vulnerabilidades de segurança. Consulte: http://www.owasp.org/index.php/Session_Management#	Sim **Nota:** Se você estiver usando o plug-in SAML 2.0 para autenticação de Single Sign-on, defina esta propriedade como Não. Caso contrário, isso interferirá no compartilhamento de informações da sessão que ocorre entre a instância e o Provedor de Identidade.	Rotação de identificadores de sessão HTTP fiers .
glide.ui.secure_cookies	Habilitar cookies de sessão segura: habilite a segurança de cookie adicional. Se **sim**, a validação estrita de cookie da sessão é imposta.	Sim	Cookies de sessão segura
glide.security.password_reset.uri	Para Redefinição de senha móvel, o URL para o qual		Nenhum

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Propriedade	Descrição	Valor Padrão	Configurações de proteção de segurança da instância
	o usuário é levado quando clica no botão **Esqueceu a senha?**.		
glide.security.strict.updates	Verifica novamente a segurança em transações de entrada durante o envio do formulário (sempre são verificados os direitos na geração do formulário). **Nota:** Essa propriedade é definida como **true** por padrão em Vancouver e versões posteriores, e não pode ser alterada pelos administradores. Para um caso de uso em que a propriedade precise ser alterada, entre em contato com o suporte ao cliente.	Sim	Verifique duas vezes as transações de entrada
glide.security.strict.actions	Verifique as condições nas ações de IU antes da execução. Normalmente, as condições são verificadas somente durante a renderização do formulário.	Sim	Verifique a ação de IU antes da execução
glide.security.use_csrf_token	Habilite o uso de um token seguro para identificar e validar solicitações de entrada. Este	Sim	Token anti-CSRF

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Propriedade	Descrição	Valor Padrão	Configurações de proteção de segurança da instância
	token é usado para impedir ataques de falsificação de solicitação entre sites.		
glide.ui.escape_html_list_field	Escapa o HTML para campos HTML em uma exibição de lista.	Sim	Escapar do HTML
glide.html.escape_script	Escapa marcadores JavaScript em campos HTML.	Sim	Escapar do JavaScript
glide.ui.forgetme	Remove a caixa de seleção **Lembrar-me** da página de login.	Sim	Remover Lembrar-me
glide.smtp.auth	Autentique com o servidor SMTP pelas propriedades de nome de usuário e senha. **Nota:** Essa propriedade foi descontinuada.	Sim	
glide.script.use.sandbox	Execute scripts gerados pelo cliente (condições AJAXEvaluate e consulta) dentro de uma área restrita de direitos reduzidos. Se **Sim**, somente as regras de negócio e inclusões de script com a caixa de seleção **Cliente chamável** selecionada para **Sim** ficarão disponíveis e algumas chamadas de API de back-end serão desabilitadas. Para obter mais informações,	Sim	Área restrita de scripts gerados pelo cliente

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Propriedade	Descrição	Valor Padrão	Configurações de proteção de segurança da instância
	consulte Configurar propriedade da área restrita de script.		
glide.soap.strict_security	Imponha segurança estrita nas solicitações SOAP de entrada. Exige que as solicitações SOAP de entrada passem pelo gerenciador de segurança para acessar tabelas e campos, bem como verifica usuários SOAP no que diz respeito às funções corretas para usar o serviço Web.	Sim	Segurança estrita de solicitação SOAP
glide.basicauth.required.wsdl	Exige autorização para solicitações WSDL de entrada. **Nota:** Caso opte por não exigir autorização para as solicitações WSDL de entrada, você deve modificar as regras de Controle de acesso (ACL) para permitir que os usuários convidados acessem o conteúdo WSDL.	Sim	Autorização de solicitação de WSDL
glide.basicauth.required.csv	Exige autorização básica para solicitações de CSV de entrada .	Sim	Autorização de solicitação de CSV

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Propriedade	Descrição	Valor Padrão	Configurações de proteção de segurança da instância
glide.basicauth.required.excel	Exige autorização básica para solicitações de entrada do Excel.	Sim	Autorização de solicitação de Excel
glide.basicauth.required.importprocessor	Exige autorização básica para solicitações de importação de entrada.	Sim	Autorização de solicitação de importação
glide.basicauth.required.pdf	Exige autorização básica para solicitações de PDF de entrada.	Sim	Autorização de solicitação de PDF
glide.basicauth.required.rss	Exige autorização básica para solicitações RSS de entrada.	Sim	Autorização de solicitação de RSS
glide.basicauth.required.scriptedprocessor	Exige autorização básica para solicitações de script de entrada.	Sim	Autorização de solicitação de script
glide.basicauth.required.soap	Exija autorização básica para solicitações SOAP de entrada.	Sim	Autenticação básica: solicitações SOAP
glide.basicauth.required.unl	Exige autorização básica para solicitações de descarregamento de entrada.	Sim	Autorização de solicitação de descarregamento
glide.basicauth.required.xml	Exige autorização básica para solicitações XML recebidas.	Sim	Autorização de solicitação de XML
glide.basicauth.required.xsd	Exige autorização básica para solicitações XSD recebidas.	Sim	Autorização de solicitação de XSD

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Propriedade	Descrição	Valor Padrão	Configurações de proteção de segurança da instância
glide.cms.catalog_uri_relative	Aplica links relativos do parâmetro URI em "/ess/catalog.do". Em caso **afirmativo**, somente URLs relativos serão permitidos por meio da página /ess/catalog.do usando o parâmetro *uri*. Se **não**, todos os URLs são permitidos, o que pode permitir vinculação a conteúdo externo não autorizado.	Sim	Impor links relativos
glide.set_x_frame_options	Habilita essa propriedade para definir o cabeçalho de resposta X-Frame-Options como SAMEORIGIN para todas as páginas de IU. O cabeçalho de resposta HTTP X-Frame-Options pode ser usado para indicar se um navegador deve ter permissão para renderizar uma página em <frame> ou <iframe>. Os sites podem usar esta propriedade para evitar ataques de clickjacking, garantindo que seu conteúdo não seja incorporado em outros sites. https://developer.mozilla.org/en/the_x-frame-options_response_header	Sim	X-Frame-Options: SAMEORIGIN
glide.ui.attachment.download_mime_types	Uma lista de tipos de mime de anexo separados por vírgula que não são	`texto/html, imagem/svg, imagem/svg + xml`	Forçar o download de tipos MIME

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Propriedade	Descrição	Valor Padrão	Configurações de proteção de segurança da instância
	renderizados em linha no navegador. Impede ataques de script entre sites. Por exemplo, `text/html` força os arquivos HTML a serem baixados para o cliente como anexos, em vez de exibidos em linha no navegador.		
glide.security.groupby_acl_check	Quando essa propriedade é habilitada, as verificações de ACL para as operações GroupBy são realizadas para os nomes do grupo com base nos dados reais dos grupos.	Sim	Nenhum
glide.security.diag_txns_acl	Se **Sim**, somente o usuário administrador ou os usuários com endereços IP permitidos poderão acessar `stats.do`, `threads.do` e `replication.do`.	Não	Monitoramento de desempenho (ACL)
glide.ui.security.codetag.allow_script	Permite que o HTML incorporado (usando marcadores [code]) contenha marcadores JavaScript.	Não	Permitir código HTML incorporado

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Propriedade	Descrição	Valor Padrão	Configurações de proteção de segurança da instância
	Nota: Essa propriedade é definida como **true** por padrão em Vancouver e versões posteriores, e não pode ser alterada pelos administradores. Para um caso de uso em que a propriedade precise ser alterada, entre em contato com o suporte ao cliente.		
glide.script.allow.ajaxevaluate	Habilita o processador AJAXEvaluate. A chamada de API *AJAXEvaluate* permite que o cliente envie e execute scripts arbitrários no servidor.	Não	Habilitar AJAXEvaluate
glide.login.autocomplete	Permite que navegadores usem o preenchimento automático em campos de senha de formulários de login.	Não	Preenchimento automático do campo de senha

As propriedades a seguir são definidas na tabela sys_properties, mas não estão visíveis na página Configurações de alta segurança.

Propriedade	Descrição	Valor padrão	Configurações de proteção de segurança da instância
com.glide.communications.httpclient.verify_hostname	Verifique o nome do host e a cadeia de certificados apresentados pelos hosts SSL remotos. Protege	verdadeiro	Nenhum

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Propriedade	Descrição	Valor padrão	Configurações de proteção de segurança da instância
	contra ataques de intermediários (MITM). Para obter mais detalhes, consulte Configurar spoke do Kubernetes spoke. **Nota:** Esta propriedade substitui a propriedade "com.glide.communications.trustmanager_trust_all".		
glide.basicauth.required.schema	Requer autenticação básica para solicitações de esquema de tabela de entrada.	verdadeiro	Nenhum
glide.security.csrf_previous.allow	Permite o uso de um token expirado seguro para identificar e validar solicitações de entrada. Este token é usado para impedir ataques de falsificação de solicitação entre sites.	falso	Nenhum
glide.security.csrf_previous.time_limit	Tempo em segundos para um token seguro expirar. Permite controlar o período de tempo em que o token CSRF anterior é válido. Quando a sessão do usuário expira, o token de segurança expira com ela, a menos que a propriedade *glide.security.csrf_previous.allow* esteja habilitada e esteja dentro do intervalo de tempo descrito por esta	86400 **Nota:** Valor em segundos. Equivalente a 1 dia.	Nenhum

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Propriedade	Descrição	Valor padrão	Configurações de proteção de segurança da instância
	propriedade. Esse token é usado para impedir ataques de falsificação de solicitação entre sites.		
glide.security.csrf.strict_validation.mode	Aplica a validação estrita em tokens CSRF para que os usuários não reenviem uma solicitação se o token CSRF não corresponder.	falso	Validação estrita de CSRF
com.glide.security.check_unsanitized_html	Aplica o comportamento de sanitização de campos "translated_html" à nível global para atribuições de campo.	impor	Nenhum

Configurar propriedade da área restrita de script

Habilita a propriedade de área restrita de script (*glide.script.use.sandbox*) para executar scripts gerados pelo cliente dentro de uma área restrita que tenha direitos restritos.

Existem dois casos dentro do sistema que permitem que o cliente envie scripts para o servidor para avaliação.

- Filtros e/ou consultas: é lícito enviar um filtro para o servidor como: `assign_to=javascript:getMyGroups()`.
- API do sistema: a chamada de API *AJAXEvaluate* permite que o cliente execute scripts arbitrários no servidor e receba uma resposta.

Se você habilitar a propriedade de área restrita de script (*glide.script.use.sandbox*), o script que está sendo avaliado por meio de um desses dois pontos de entrada é executado em uma área restrita de direitos reduzidos com as seguintes características:

- Somente as regras de negócios marcadas como **cliente chamável** estão disponíveis na área restrita.
- Somente as inclusões de script marcadas como **cliente chamável** estão disponíveis na área restrita.
- Certas chamadas de API (em grande parte, mas não totalmente limitadas àquelas que lidam com acesso direto ao banco de dados) não são permitidas.
- Os dados não podem ser inseridos, atualizados ou excluídos da área restrita. Quaisquer chamadas para *current.update()*, por exemplo, são ignoradas.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Para aprender mais sobre essa propriedade, consulte Área restrita de scripts gerados pelo cliente nas Configurações de proteção de segurança de instância.

Esses métodos não são permitidos em scripts gerados pelo cliente quando a área restrita de script está habilitada.

Métodos restritos

Classe	Método
GlideRecord	• `deleteMultiple()` • `deleteRecord()` • `getRowCount()` • `insert()` • `update()` • `updateMultiple()`
GlideSystem (gs)	• `addErrorMessage()` • `addInfoMessage()` • `addMessage()` • `eventQueue()` • `flushMessages()` • `getEscapedProperty()` • `getProperty()` • `log()` • `logError()` • `logWarning()` • `setProperty()` • `setRedirect()` • `setReturn()` • `workflowFlush()`
ScopedGlideRecord	• `deleteMultiple()` • `deleteRecord()` • `insert()` • `update()` • `updateMultiple()`
ScopedGlideSystem (gs)	• `addErrorMessage()` • `addInfoMessage()` • `debug()`

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Métodos restritos

Classe	Método
	• `eventQueue()` • `executeNow()` • `getProperty()` • `getSessionToken()` • `info()` • `setRedirect()`
GlideDate GlideDateTime GlideTime	• `add()` • `addDays()` • `addDaysLocalTime()` • `addDaysUTC()` • `addMonthsLocalTime()` • `addMonths()` • `addSeconds()` • `addWeeks()` • `addYears()` • `compareTo()` • `getByFormat()` • `getDate()` • `getDayOfWeek()` • `getDayOfWeekUTC` • `getDayOfWeekLocalTime()` • `getDayOfMonth()` • `getDayOfMonthLocalTime()` • `getDayOfMonthNoTZ()` • `getDayOfWeek()` • `getDayOfWeekLocalTime()` • `getDayOfWeekUTC()` • `getHourOfDayLocalTime()` • `getHourOfDayUTC()` • `getDaysInMonth()` • `getDaysInMonthUTC()` • `getDaysInMonthLocalTime()` • `getDisplayValueInternal()` • `getDisplayValue()` • `getHourLocalTime()`

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Métodos restritos

Classe	Método
	• `getLocalDate()` • `getLocalTime()` • `getMinutesLocalTime()` • `getMinutesUTC()` • `getMonthLocalTime()` • `getMonthNoTZ()` • `getMonthUTC()` • `getNumericValue()` • `getSeconds()` • `getTime()` • `getTZOffset()` • `getValue()` • `getYear()` • `getUserTimeZone()` • `getWeekOfYearLocalTime()` • `getWeekOfYearUTC()` • `getYearUTC()` • `getYearLocalTime()` • `isDST()` • `onOrAfter()` • `onOrBefore()` • `setDayOfMonthUTC()` • `setDisplayValue()` • `setMonth()` • `setNumericValue()` • `setTZ()` • `setValue()` • `setValueUTC()` • `subtract()` • `toString()`
GlideSchedule	• `add()` • `isInSchedule()` • `Load()` • `whenNext()`

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Os métodos GlideSystem (gs) *log()*, *logError()* e *logWarning()* podem ser habilitados com a área restrita de script definindo a propriedade do sistema *glide.security.sandbox_no_logging* como `falsa`.

Se você executar o sistema sem a área restrita de script ativada, nenhuma dessas restrições se aplicará.

Nota: Essa propriedade é ativada por padrão quando você ativa o plug-in Configurações de alta segurança. Não ative essa propriedade fora do plug-in.

Propriedade	Padrão
Executa scripts gerados pelo cliente (condições *AJAXEvaluate* e consulta) dentro de uma "área restrita" de direitos reduzidos. Se habilitada, somente as regras de negócio e inclusões de script com a caixa de seleção **Cliente chamável** selecionada para "verdadeiro" ficarão disponíveis e algumas chamadas de API de back-end serão desabilitadas.	Habilitado (área restrita em uso).

Ativar configurações de alta segurança

O plug-in "High Security Settings" está ativo por padrão em todas as novas instâncias. Se não estiver ativo em sua instância, você pode solicitar o plug-in.

Antes de Iniciar
Função necessária: nenhuma

Antes de ativar o plug-in "High Security Settings" em uma instância existente:

1. Analise as seguintes informações para entender o novo comportamento:
   - Regras da lista de controle de acesso
   - Configurações de Alta Segurança
   - Propriedade de negação padrão
2. Habilite o plug-in em uma instância de não produção. Um clone de produção recente é preferível.
3. Teste a funcionalidade revisada, especialmente as ACLs adicionadas e a funcionalidade de negação padrão. Continue testando até que o sistema funcione conforme o esperado. Se os usuários não puderem acessar os recursos esperados, verifique se eles têm funções e regras de ACL apropriadas para que o acesso seja concedido.
4. Crie conjuntos de atualizações de todas as mudanças necessárias para que você possa aplicá-las à produção.

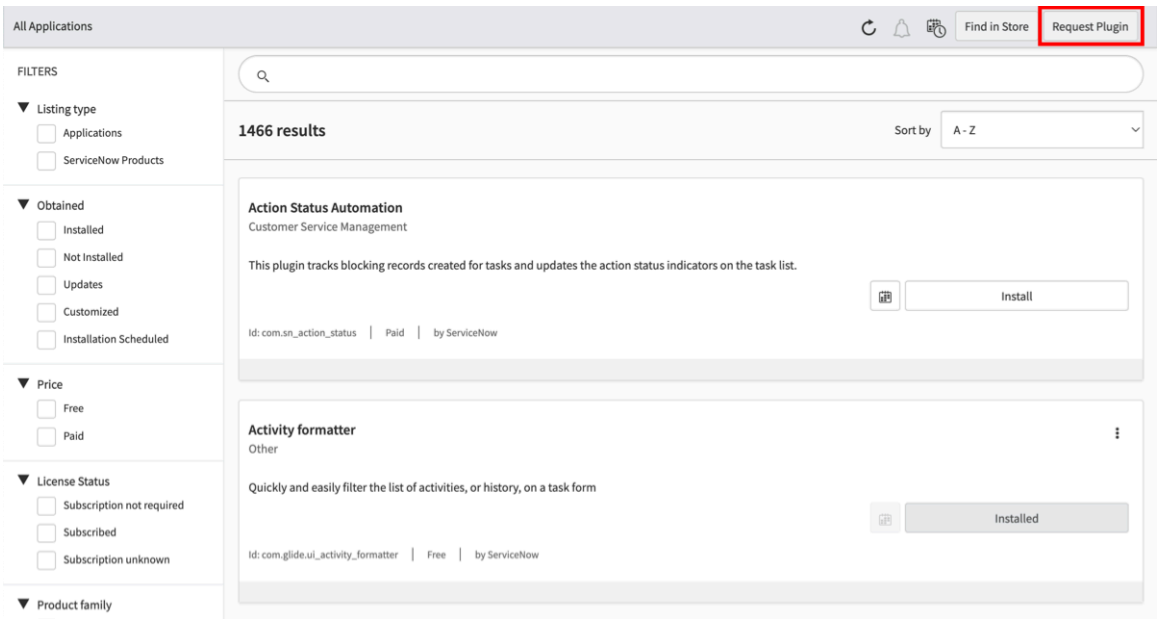
Nota: Para saber mais sobre este plug-in, consulte Plug-in High Security nas Configurações de proteção de segurança da instância.

Função necessária: administrador

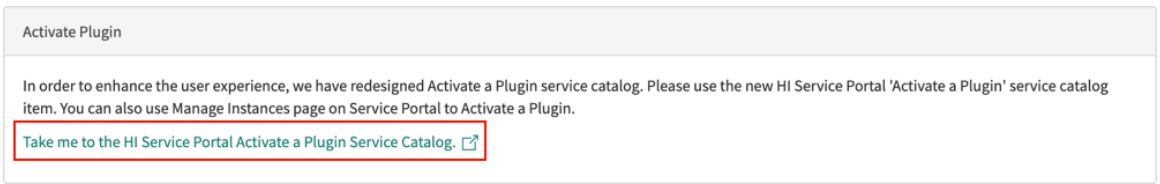
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegue até **Todas** > **Aplicações do sistema** > **Todas os aplicações disponíveis** > **Todas**.
2. Na página Todas as Aplicações, selecione **Solicitar plug-in** para abrir o formulário **Ativar plug-in** em Now Support.



3. No Now Support, selecione o link para acessar o Now Support Portal de serviços Catálogo de serviços.



4. Selecione sua instância.
5. Selecione **Ações > Ativar plug-in**.
6. No formulário **Ativar plug-in**, forneça as seguintes informações.

Formulário Ativar plug-in

Campo	Descrição
Qual é a sua instância de destino	Instância na qual o plug-in será ativado.
Qual plug-in você deseja ativar	Nome do plug-in a ser ativado.

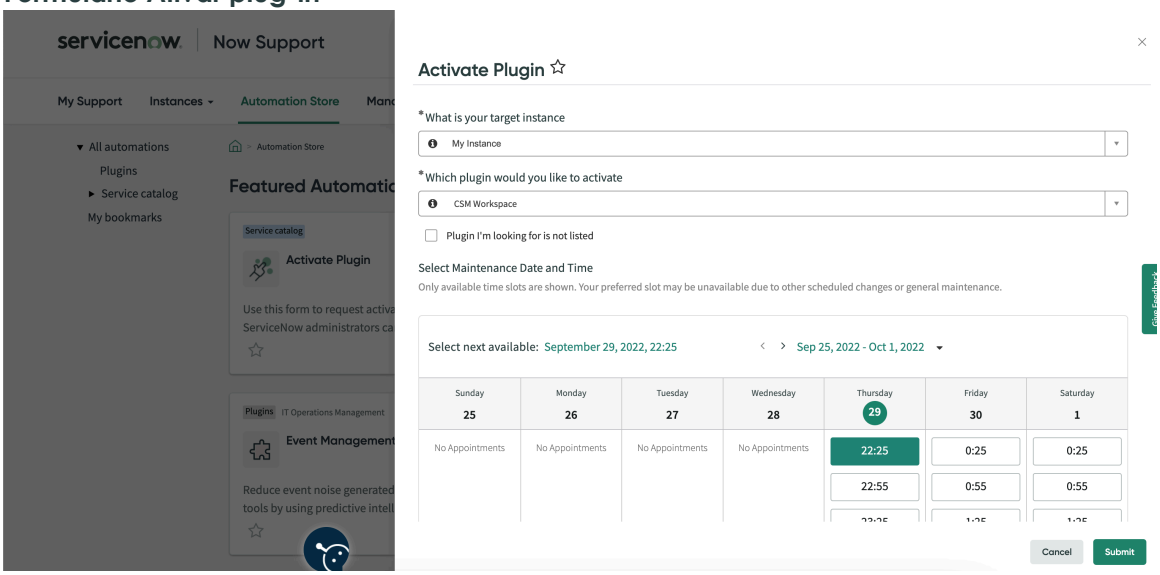
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: Se o sistema não listar o plug-in desejado ou se você estiver ativando o plug-in em uma instância do OEM ou no local, marque a caixa de seleção O **plug-in que estou procurando não está listado** e insira o nome do plug-in.
Selecionar data e hora de manutenção	A data e a hora para ativar o plug-in. **Nota:** Os plug-ins são ativados em dois lotes, uma pela manhã e outra à noite, em todos os dias úteis no fuso horário do Pacífico dos EUA. Se o plug-in deve ser ativado em um momento específico, insira a solicitação no campo **Motivo/ Comentários**.

Example

Por exemplo, consulte o formulário a seguir para ativar o plug-in Espaço de trabalho CSM em uma instância chamada Minha instância.

Formulário Ativar plug-in



7. Selecione **Enviar**.
   Para obter detalhes adicionais sobre como solicitar um plug-in, consulte Solicitar um plug-in no artigo do Catálogo de serviços [KB0751715] em Now Support Base de conhecimento.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Rede virtual privada (VPN)

Use uma VPN (virtual private network, rede virtual privada) para integrar sua instância com fontes de dados externas na Internet.

Explorar Conheça os recursos e os valores comerciais da rede virtual privada.	Ativar Ative a rede virtual privada.
Configurar Entenda como configurar uma rede virtual privada.	

Explorar rede virtual privada (VPN)

Use uma VPN (virtual private network, rede virtual privada) para integrar sua instância com fontes de dados externas na Internet.

Minhas informações de IP

Ao configurar uma integração que usa um protocolo criptografado, como o protocolo LDAP (Lightweight Directory Access Protocol, Protocolo de acesso a diretório leve) ou HTTPS, usar a Internet como mecanismo de transporte é uma prática recomendada.

No entanto, pode haver requisitos de arquitetura de segurança ou de rede que determinem o uso de uma conexão de Rede Privada Virtual (VPN) IPSEC (Internet Protocol Security, Segurança de protocolo de internet) site a site entre os datacenters e suas redes de negócios. A VPN oferece suporte à comunicação criptografada necessária entre a instância e a rede.

Conexões de VPN

A infraestrutura de VPN da ServiceNow usa pares de ASA (adaptive security appliance, dispositivo de segurança adaptativo) Cisco que servem como pontos de terminação de VPN.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A VPN entre a instância e sua rede utiliza o hardware de rede existente para oferecer suporte a comunicações. Não é necessário instalar nenhuma peça de hardware. Como cada cliente tem uma configuração exclusiva, a instância tem uma solução VPN flexível. A instância construiu túneis para Checkpoint, Juniper, Nortel e outros dispositivos compatíveis com VPN IPSEC.

As conexões de VPN entre a instância e sua rede são criadas para oferecer suporte ao fluxo criptografado de tráfego em sua rede. Frequentemente, as integrações que usam a VPN não têm criptografia como parte do protocolo subjacente. Por exemplo, LDAP na VPN versus LDAPS na Internet e HTTP na VPN versus HTTPS na Internet.

A rede não permite que nenhuma integração de entrada para a ServiceNow ou tráfego de usuário final para a ServiceNow atravesse uma conexão VPN. Essa comunicação restrita inclui o acesso do usuário final à plataforma, a administração da plataforma, as integrações de serviços da Web e outras integrações que são configuradas para usar um MID Server. Todas essas comunicações de entrada com a instância devem ser realizadas pela Internet usando HTTPS. Esta configuração fornece um canal de comunicação criptografado. O canal de criptografia, junto com o controle de acesso IP, atende aos requisitos de segurança para este fluxo de tráfego.

Endereços para comunicação VPN

Para evitar conflito ou sobreposição com redes internas da ServiceNow ou com outros esquemas de endereço IP interno em sua rede, todo o tráfego em túnel no domínio de criptografia deve usar endereços não RFC-1918 em ambos os lados do túnel.

ServiceNow fornece um único endereço IP para a origem das consultas em sua rede. Você deve fornecer endereços de NAT (Network Address Translation, conversão de endereço de rede) não RFC-1918 para cada host que está se integrando à sua instância. Esses endereços públicos precisam pertencer à sua organização. Endereços de terceiros não podem ser usados dentro de túneis. Além disso, o domínio de criptografia não deve conter o endereço IP do par da VPN.

Túneis redundantes

Existem duas maneiras de criar redundância para seus túneis:

- Usar o mesmo domínio de criptografia por trás de seus pares. Este é o método preferencial.
- Usar um domínio de criptografia diferente atrás de cada par.

Com o primeiro método, você precisa fornecer o mesmo endereço de NAT atrás de cada um dos seus pares para criar um caminho de conexão usando esse endereço para o seu servidor. O caminho para o servidor pode ser a mesma máquina física ou um espelho que fornece serviços idênticos. Com este método, sua instância usaria o mesmo endereço IP para se conectar aos seus servidores, independentemente de o túnel primário ou secundário estar ativo. Se você tiver mais de um servidor, siga este mesmo esquema para os servidores adicionais. Este método fornece mais transparência para os usuários e é recomendado.

O segundo método requer configuração em sua instância para fornecer a redundância. Quando o túnel é usado para LDAP, por exemplo, você pode fornecer servidores LDAP redundantes em sua instância. Observe que este método requer que a conexão com o primeiro servidor LDAP configurado atinja o tempo limite antes que a instância tente se conectar ao servidor secundário. Por causa deste atraso de tempo adicional, esta solução só deve ser implementada se a primeira opção estiver inatingível. Observe também que nem todos os serviços podem ser configurados de forma redundante em sua instância. Se você estiver usando um túnel VPN para algo diferente de LDAP e a redundância for

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

necessária, verifique se sua configuração pode oferecer suporte a vários endereços ou consulte a primeira opção acima.

Alternativas ao uso de uma VPN

Essas alternativas fornecem uma maneira mais simples de conectar sua instância aos recursos nos datacenters da ServiceNow e fornecer melhor criptografia. Além disso, você pode evitar problemas que o tempo de inatividade da VPN possa causar, como tornar sua instância indisponível para os usuários se houver um problema com o túnel VPN.

Single Sign-on e MID Server

Considere usar uma combinação de Single Sign-On (SSO) para autenticação e o MID Server para sincronização de dados do usuário, em vez de usar uma VPN para conectar o servidor LDAP à sua instância. Para integrações diferentes do LDAP, considere o uso de criptografia baseada em certificado.

Você pode usar o ouvinte LDAP em um MID Server para sincronizar sua tabela de usuário quase em tempo real.

A vantagem dessa abordagem é que não há falhas no firewall, rotas, túneis de VPN ou outras configurações de rede especiais para configurar e manter. A solução SSO/MID-Server é o método mais flexível, seguro e econômico para obter a integração LDAP completa.

LDAP sobre SSL

Outra alternativa ao uso de um túnel VPN é configurar o LDAP sobre SSL (LDAPS) diretamente pela Internet. Você pode configurar um controlador de domínio somente de leitura e bloquear a instância em seu DMZ usando somente os endereços de fonte da instância e as portas de destino de sua escolha. Como as portas do LDAP são configuráveis em sua instância, você pode executar uma PAT (port address translation, tradução de endereço de porta), se desejar. Com o LDAPS, você controla o certificado que é carregado por meio de um canal criptografado para a instância, (consulte Carregamento de certificados para uma instância). Os pacotes não podem ser criptografados ou descriptografados sem o certificado.

A vantagem desta abordagem é que ela fornece um mecanismo de criptografia e descriptografia mais forte. Uma VPN só pode criptografar e descriptografar o tráfego entre os dois pares na Internet com uma chave pré-compartilhada coordenada, semelhante a uma senha. O LDAPS fornece um caminho criptografado mais longo, de ponta a ponta, na camada da aplicação e com um certificado que é muito mais complexo do que uma chave pré-compartilhada que o túnel IPSec usa.

Configuração de VPN

A partir do momento em que uma solicitação de VPN é enviada, normalmente leva uma semana ou menos para concluir a compilação da VPN. Para oferecer suporte aos requisitos de redundância da sua instância e da sua organização, um mínimo de duas e um máximo de quatro VPNs são provisionadas (do site ativo para o seu site ativo ou do site ativo para o seu site de DR e assim por diante).

É uma prática recomendada que o domínio de criptografia seja o mais específico possível. O ideal é que o domínio de criptografia inclua somente os hosts específicos necessários para as integrações. Um domínio de criptografia grande pode criar oportunidades para discrepâncias de roteamento (VPN versus Internet).

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para criar a VPN, a instância faz o seguinte:

1. Fornece o par VPN e os endereços do host de cada datacenter.
2. Cria a conectividade de VPN necessária de dois datacenters em sua rede. Para oferecer suporte aos requisitos de redundância e DR (disaster recovery, recuperação de desastre), as VPNs podem ser provisionadas de dois datacenters em duas redes.

A instância não é compatível com a criação de vários túneis VPN em uma rede de cliente para fins de conexão com várias regiões geográficas ou subsidiárias. Você deve executar qualquer roteamento entre sites, distribuição de tráfego ou modelagem de tráfego em sua própria rede interna, em vez de ter vários túneis VPN.

Ativar um serviço VPN

Para todas as solicitações de VPN, incluindo provisionamento, modificações ou perguntas gerais, use o formulário Solicitação de VPN do Catálogo de serviços.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Navegue até https://support.servicenow.com/now?draw=case.
2. Selecione a guia **Armazenamento de automação**.
3. Use a árvore à esquerda para navegar até **Todas as automações** > **Catálogo de serviços** > **Infraestrutura em nuvem**.
4. Selecione **Solicitações de VPN**
5. Selecione o tipo de solicitação de VPN apropriado.
6. Responda às perguntas.
   As perguntas variam de acordo com o tipo de solicitação selecionado.
7. Clique em **Enviar**.

Resultados

Depois que sua solicitação for enviada, a ServiceNow trabalhará com seus engenheiros de rede para testar e validar se a VPN está passando o tráfego com êxito. Para garantir que suas perguntas sejam respondidas em tempo hábil, resolva as perguntas relacionadas à VPN durante este processo.

Configurar um endereço para comunicação VPN

Para evitar conflito ou sobreposição com redes internas da ServiceNow ou com outros esquemas de endereço IP interno do cliente, a instância exige que todo o tráfego em túnel no domínio de criptografia use endereços não RFC-1918 em ambos os lados do túnel.

Antes de Iniciar

Função necessária: admin

Por Que e Quando Desempenhar Esta Tarefa

A instância fornece um único endereço IP para a origem das consultas em sua rede.

Procedimento

Forneça endereços de NAT (Network Address Translation, conversão de endereço de rede) não RFC-1918 para cada host que está se integrando à instância.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

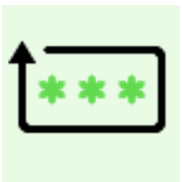
Privacidade da plataforma

A privacidade permite mascarar a data confidencial na instância.

Privacidade de dados

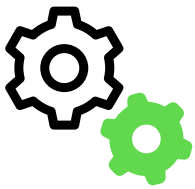
Use a Privacidade de dados para classificar dados confidenciais e remover informações de identificação pessoal (PII - personally identifiable information) dos dados do usuário em uma instância de produção e para tornar os dados anônimos em instâncias de não produção.

Descoberta de dados



Use a descoberta de dados para identificar dados confidenciais em uma instância a fim de classificar, proteger ou reportar.

Classificação de dados



Agrupe dados por tipo, usando classificações de dados predefinidas ou definidas por usuário. Se você tiver uma função de auditor ou administrador de classificação de dados atribuída, será possível administrar diferentes classes de dados ou analisar visualmente o estado atual de diferentes tipos de dados na instância.

Anonimização de dados

A anonimização de dados oferece uma maneira de transformar facilmente os dados para que eles não sejam identificáveis e estejam mais em conformidade com as regulamentações da privacidade de dados.

Privacidade de dados

Use a Privacidade de dados para classificar dados confidenciais e remover informações de identificação pessoal (PII - personally identifiable information) dos dados do usuário em uma

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

instância de produção e para tornar os dados anônimos em instâncias de não produção. Depois de tornados anônimos, os dados do usuário não são mais considerados informações privadas regulamentadas.

Explore Privacidade de dados

Saiba mais sobre a Privacidade de dados.

Configurar a Privacidade de dados

Saiba como configurar a Privacidade de dados.

Funções na Privacidade de dados

Veja os detalhes sobre as funções na Privacidade de dados.

Recursos avançados de Privacidade de dados

Saiba mais sobre os recursos avançados de Privacidade de dados.

Explorando a privacidade de dados

Use a Privacidade de dados para classificar dados confidenciais e remover informações de identificação pessoal (PII - personally identifiable information) dos dados do usuário em uma instância de produção e para tornar os dados anônimos em instâncias de não produção. Depois de tornados anônimos, os dados do usuário não são mais considerados informações privadas regulamentadas.

Explica a importância da privacidade de dados e as etapas que as empresas podem executar para proteger informações confidenciais por meio de classificação e anonimização. Usando a aplicação de armazenamento de privacidade de dados, fornecemos uma visão geral do painel principal e dos recursos.

Os desenvolvedores devem trabalhar com dados em instâncias de não produção para garantir que suas implementações estejam funcionando conforme o esperado. Embora a importação de dados de sua instância de produção seja uma maneira útil de simular a produção, ela apresenta um risco à segurança. Os administradores podem usar o Data Privacy para fornecer aos desenvolvedores dados que não contenham informações privadas para trabalhar com segurança em um ambiente de não produção.

Classificação de dados

Identifique e classifique seus dados confidenciais de acordo com critérios predefinidos determinados pelo nível de confidencialidade dos tipos de dados em sua instância. Os níveis de confidencialidade dos dados ajudam a determinar como cada tipo de dados

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

classificados deve ser tratado. Existem várias classes predefinidas fornecidas com a Privacidade de dados de nível de base. Use a seção de classificação da Privacidade de dados para rotular e agrupar dados em sua instância. Adicione classes, exiba a estrutura de classes de dados e classifique os dados. Agrupe dados por tipo, usando classificações de dados predefinidas ou definidas por usuário.

Explica como classificar dados usando a aplicação de armazenamento de privacidade de dados.

Anonimização de dados de usuário

Como administrador, você define se todas as informações de todos os usuários ou de um subconjunto de usuários devem ser anônimas. Quando anônimos, os dados dos registros de usuário selecionados são substituídos por valores aleatórios ou valores definidos por você. Ao substituir os valores, a estrutura de dados pode ser preservada usando diversas técnicas.

Explica como anonimizar dados usando a aplicação de armazenamento de privacidade de dados.

Opções da Privacidade de dados

- Privacidade de dados (Clássico): primeiro, use o aplicativo de classificação de dados para agrupar os dados por tipo, usando classificações de dados pré-definidas ou definidas por usuário. Em seguida, crie técnicas e trabalhos da Privacidade de dados para anonimizar PII.
- Privacidade de dados (Aplicação da Store): classifique e anonimize seus dados de dentro do aplicativo da Privacidade de dados.

Considerações

- Somente dados classificados podem ser anônimos. Para obter mais informações sobre classes e classificação de dados, consulte Classificação de dados (Classic) ou Classificação de dados a aplicação da Store.
- PII em logs e outros dados de auditoria não são anônimos.
- Somente dados estruturados podem ser anônimos. Dados não estruturados, como Campos de diário, comentários, anexos e outros campos em que o texto parcial pode representar PII não são anônimos. Para obter mais informações, consulte Tipos de campos compatíveis para anonimização.
- As integrações com sistemas de conexão única (SSO - Single Sign-on) podem sincronizar novamente as informações do usuário de sua fonte de sistemas verdadeiros. Não há nenhum mecanismo para garantir a permanência da desidentificação de dados do sys_user. Para obter informações sobre administração de usuário e sys_users, consulte Administração de usuário.

Domain separation e Privacidade de dados

Domain separation não é compatível com Privacidade de dados. O Domain Separation permite separar dados, processos e tarefas administrativas em agrupamentos lógicos chamados de domínios. Você pode controlar vários aspectos dessa separação, incluindo quais usuários podem ver e acessar os dados.

Nível de suporte: Sem suporte

- O campo de domínio pode existir em tabelas de dados, mas não há lógica de negócios para gerenciar os dados.
- Este nível não é considerado separado por domínio.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para obter mais informações sobre os níveis de suporte, consulte Suporte de aplicação para separação de domínio.

Informações relacionadas

Domain Separation para provedores de serviço

Tipos de campos compatíveis para anonimização

Verifique quais tipos de campo são compatíveis ao anonimizar os dados.

Nota: Nem todos os tipos de campo que foram classificados estão disponíveis para anonimização.

Alguns tipos de campo de alto risco estão desativados por padrão, conforme detalhado na tabela. Para obter mais informações sobre campos, consulte Tipos de campo.

Tipos de campos compatíveis para anonimização

Tipo de campo	Disponível por padrão
áudio	Não
condição	Não
condition_string	Não
moeda	Sim
decimal	Sim
due_date	Sim
variável	Sim
glide_date	Sim
glide_date_time	Sim
glide_duration	Não
glide_time	Sim
html	Não
ícone	Não
inteiro	Sim
ip_addr	Não
ip_address	Não
registro	Sim
journal_input	Sim
journal_list	Sim
longint	Sim
name_values	Não
percent_complete	Não
phone_number_e164	Sim

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tipo de campo	Disponível por padrão
preço	Sim
cadeia de caracteres	Sim
string_full_utf8	Sim
translated_html	Não
translated_text	Não
url	Não
user_image	Não
vídeo	Não
wiki_text	Não

Funções da Privacidade de dados

a Privacidade de dados adiciona essas funções.

Administrador da Privacidade de dados

As funções de administrador da Privacidade de dados são uma função de administrador usada para criar técnicas e políticas da Privacidade de dados.

Administrador da Privacidade de dados [data_privacy_admin]

Contém as funções

Nenhum

Atribuído a grupos

Nenhum

Assinatura

Não

Elevado

Sim

Considerações

Evite atribuir esta função a seus usuários quando houver mais funções direcionadas disponíveis.

Para atribuir a função "Administrador de privacidade de dados", eleve o usuário à função de administrador de segurança para adicionar a função.

Auditor da Privacidade de dados

O auditor da Privacidade de dados é uma função somente leitura usada para exibir registros da Privacidade de dados.

Auditor da Privacidade de dados [data_privacy_auditor]

Contém as funções

Nenhum

Atribuído a grupos

Nenhum

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Assinatura

Não

Elevado

Não

Considerações

Nenhum

Processador de clone da Privacidade de dados

Usuários com a função de processador de clone da Privacidade de dados podem criar e executar trabalhos de classe de dados da Privacidade de dados.

Processador de clone da Privacidade de dados [data_privacy_clone_processor]

Contém as funções

Nenhum

Atribuído a grupos

Nenhum

Assinatura

Não

Elevado

Sim

Considerações

Nenhum

Processador da Privacidade de dados

Usuários com a função de processador da Privacidade de dados criam e executam trabalhos de classe de dados da Privacidade de dados na tabela [sys_user] de usuário.

Processador da Privacidade de dados [data_privacy_processor]

Contém as funções

Nenhum

Atribuído a grupos

Nenhum

Assinatura

Não

Elevado

Sim

Considerações

Nenhum

Privacidade de dados (Clássico)

a Privacidade de dados (Clássico) está disponível como uma versão de família. As últimas atualizações de família foram divulgadas no lançamento de Tóquio.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Como ativar a Privacidade de dados (Clássico)

Você pode ativar o plug-in privacidade de dados (com.glide.data_privacy) para Segurança da plataforma se tiver a função de administrador. A aplicação inclui dados de demonstração e instala aplicações e plug-ins relacionados ServiceNow® Store se eles ainda não estiverem instalados.

Antes de Iniciar

A privacidade de dados requer uma assinatura separada do restante do Now Platform.

Para adquirir uma assinatura, entre em contato com o seu gerente de contas ServiceNow. Quando você compra uma assinatura, determinados plug-ins são ativados automaticamente. Se um plug-in pago não for ativado automaticamente, você poderá ativá-lo manualmente na lista Todas as aplicações em sua instância.

Nota: Antes de adquirir uma assinatura, você pode avaliar a Privacidade de dados (Clássico) e a Descoberta de dados por um período de avaliação de 30 dias. Após o vencimento da avaliação, não será mais possível descobrir dados ou executar trabalhos de anonimização em sem uma licença.

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

Os itens a seguir são instalados com a privacidade de dados:

- Plug-ins
- Funções
- Tabelas

Para obter mais informações, consulte Instalado com a Privacidade de dados (Clássico).

Procedimento

1. Navegue até **Todos** > **Aplicações do sistema** > **Todas as aplicações disponíveis** > **Todas**.
2. Encontre o plug-in privacidade de dados (com.glide.data_privacy) usando os critérios de filtro e a barra de pesquisa.

   Pesquise o plug-in pelo nome ou ID. Se não conseguir encontrar um plug-in, talvez seja necessário solicitá-lo ao pessoal ServiceNow.
3. Selecione **Instalar** para iniciar o processo de instalação.

   Nota: Quando a separação de domínio e o administrador delegado estão habilitados em uma instância, o usuário administrativo deve estar no domínio **global.** Caso contrário, será exibido o seguinte erro: `A instalação da aplicação não está disponível porque há outra operação em execução: ativação de plug-in para <plugin name>.`

   Você verá uma mensagem após a conclusão da instalação.

Instalado com a Privacidade de dados (Clássico)

Saiba mais sobre os componentes instalados com o plug-in privacidade de dados (com.glide.data_privacy).

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabelas instaladas

Tabela	Descrição
Trabalho Federado de Privacidade de Dados [dp_federated_job]	Trabalhos federados para a privacidade de dados
Trabalho de Privacidade de Dados [dp_job]	Trabalhos de privacidade de dados
Trabalho de Privacidade de dados [dp_job_summary]	Resumo de trabalhos de privacidade de dados
Técnica de Privacidade de dados [dp_technique]	Técnicas de privacidade de dados
Link de referência primária [dp_primary_reference]	Links de referência primária
Técnica de campo classificado de privacidade [dp_field_technique]	Técnicas de campo classificado de privacidade de dados
Configuração de privacidade [dp_configuration]	Configuração de privacidade de dados
Configuração de técnica de privacidade [dp_technique_with_params]	Técnicas de privacidade de dados
Parâmetro de técnica de privacidade [dp_technique_with_parameter]	Técnicas de privacidade de dados com parâmetros
Valor do parâmetro de técnica de privacidade [dp_technique_with_parameter_value]	Valores de parâmetro usados nas técnicas de privacidade de dados com parâmetros.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configuração da Privacidade de dados (Clássico)

Aprenda a criar técnicas e políticas para privacidade de dados e a criar e executar trabalhos dele.

Técnicas de privacidade de dados

Técnicas de privacidade de dados são opções que você seleciona para determinar como seus dados são anonimizados Você deve criar uma técnica de privacidade de dados para fazer referência no trabalho dele. Consulte Como criar um configuração de técnica da Privacidade de dados para associar uma técnica de privacidade a uma **configuração de técnica de privacidade** associada.

Políticas de privacidade de dados

Configure uma política de privacidade de dados para especificar quais técnicas dele são usadas ao anonimizar seus dados. Consulte Como criar um política da Privacidade de dados para obter detalhes.

Trabalhos de privacidade de dados

Os trabalhos de privacidade de dados usam todos esses componentes para anonimizar seus dados. Para obter mais informações sobre esses trabalhos, consulte Configuração de um trabalho da Privacidade de dados.

Como criar um configuração de técnica da Privacidade de dados

Crie uma configuração de técnica da Privacidade de dados para personalizar como ele anonimiza seus dados.

Antes de Iniciar

Função necessária: data_privacy_admin e administrador

Procedimento

1. Eleve para a função **data_privacy_admin**.
   Para obter detalhes sobre a elevação de função, consulte Elevar para uma função privilegiada.
2. Navegue até **Segurança do sistema** > **Privacidade de dados** > **Configuração de técnica de privacidade**.
3. Clique em **Novo**.
4. No campo **Nome**, insira um nome para a configuração de técnica de privacidade.
5. No campo **Técnica de privacidade**, selecione uma técnica de privacidade.

Técnicas da Privacidade de dados

Técnica	Descrição
Nenhuma ação	Esta técnica é um espaço reservado. Ela não modifica os campos quando selecionada.
Substituição aleatória	Esta técnica troca valores por valores gerados aleatoriamente. Dados de cadeia de caracteres e números podem usar esta técnica.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Técnica	Descrição
Substituição seletiva	Esta técnica faz uma substituição seletiva de dados de cadeia de caracteres. Todos os caracteres entre os índices inicial e final da entrada são substituídos pelo caractere escolhido. Você pode especificar caracteres a serem excluídos do mascaramento: ◦ start_index: a técnica mascara os dados que começam no caractere especificado. Se deixado em branco, o mascaramento começará com o primeiro caractere. ◦ end_index: a técnica mascara os dados desde o início da cadeia de caracteres até o caractere especificado. Se deixado em branco, o mascaramento terminará com o último caractere. ◦ exclude_char: define um caractere a ser excluído do mascaramento. ◦ replacement_char: define um caractere usado para mascaramento. Se nenhum for fornecido, serão usados asteriscos (*) por padrão.
Substituição estática	Esta técnica troca valores por valores estáticos. Dados de Cadeia de caracteres, Número e Data podem usar esta técnica: ◦ date_time_value: substitui os valores de data por esta data. Use o formato aaaa-MM-dd HH:mm:ss. ◦ date_value: substitui os valores de data por esta data. Use o formato aaaa-MM-dd. ◦ number_value: substitui os valores de número por este número. ◦ string_value: substitua os valores de cadeia de caracteres por este texto.
Remover	Esta técnica remove valores, substituindo-os por valores vazios (nulos).

Nota: O valor com suporte anterior **Substituir** foi descontinuado e foi renomeado como **Substituir-Descontinuado** e não deve ser usado.

6. Clique com o botão direito do mouse no cabeçalho e, em seguida, em **Salvar** no menu de contexto.
   Depois que o registro é salvo, a lista **Valores com parâmetros de privacidade** é exibida.
7. Use os registros na lista **Valores com parâmetros de privacidade** para personalizar a configuração de técnica da Privacidade de dados.
   Os valores com parâmetros disponíveis dependem de qual técnica de privacidade você selecionou. Não há valores com parâmetros para as técnicas **Nenhuma ação** e **Remover**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Valores com parâmetros de privacidade para Substituição seletiva

Valor do parâmetro de técnica de privacidade	Descrição	Valor-padrão
char_to_replace	Caractere a ser usado ao substituir valores usando uma substituição seletiva.	*
end_index	A técnica mascara os dados desde o início da cadeia de caracteres até o caractere especificado. Se deixado vazio, o mascaramento terminará com o último caractere.	(Vazio)
exclude_char	Caractere para ignorar o mascaramento. Somente um único caractere pode ser usado neste valor. Se mais de um for inserido, o primeiro caractere será usado.	(Vazio)
start_index	A técnica mascara os dados que começam no caractere especificado.	1

Valores parametrizados de privacidade para substituir

Valor do parâmetro de técnica de privacidade	Descrição	Valor-padrão
date_time_value	Substitui os valores de data e hora por esta data. Use o formato aaaa-MM-dd HH:mm:ss.	1988-11-11 10:10:10
date_value	Substitui os valores de data por esta data. Use o formato aaaa-MM-dd.	1988-11-11
number_value	Substitua os valores de Número por este número.	1234567
preserve_data_length	Defina como **verdadeiro** para preservar o tamanho dos dados. Os dados desidentificados terão o mesmo comprimento que os dados originais.	verdadeiro
string_value	Substitua os Valores de cadeia de caracteres por este texto.	TEXT123
use_random_generated_value	Defina como **verdadeiro** para substituir os dados por valores gerados	falso

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Valor do parâmetro de técnica de privacidade	Descrição	Valor-padrão
	aleatoriamente. Somente dados de cadeia de caracteres e números podem ser substituídos por valores aleatórios. Esta opção substitui os valores estáticos.	

8. Clique em **Salvar**.

Como criar um política da Privacidade de dados

Configure uma política da Privacidade de dados para especificar quais técnicas dele são usadas ao anonimizar seus dados.

Antes de Iniciar

A configuração da Privacidade de dados define tabelas, sys_user e outros, além de colunas para o desidentificado dependendo do caso de uso e especifica tipos parametrizados das técnicas a serem usadas durante a desidentificação de dados.

Nota: Para concluir uma configuração de privacidade, você deve primeiro configurar uma configuração de técnica da Privacidade de dados. Para obter mais informações, consulte Como criar um configuração de técnica da Privacidade de dados.

Função necessária: data_privacy_admin e administrador

Procedimento

1. Eleve para a função **data_privacy_admin**.
   Para obter detalhes sobre a elevação de função, consulte Elevar para uma função privilegiada.
2. Navegue até **Segurança do sistema** > **Privacidade de dados (Clássico)** > **Configuração de política de privacidade**.
3. Selecione **Novo**.
4. No campo **Nome**, insira um nome para a configuração de política de privacidade.
5. No campo **Classe de dados**, selecione a classe de dados a ser usada com esta política.
   As políticas da Privacidade de dados só podem ser aplicadas a dados classificados. Para obter mais informações sobre classificação de dados, consulte Classificação de dados.
   Depois de selecionar uma classe de dados, as listas de **Técnicas de campo de privacidade** e **Links de referência primária de privacidade** são exibidas no formulário.
6. Opcional: Selecione **Aplicar a todos os dados da classe** para aplicar a anonimização a todos os dados na classe de dados escolhida.
   Se você não selecionar este campo, os usuários do processador da Privacidade de dados poderão escolher quais usuários serão anonimizados ao criar trabalhos da Privacidade de dados. Se você selecionar este campo, essa opção não estará disponível.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- **Aplicar ao clonar**: esta opção se torna disponível. Quando selecionada, a configuração de privacidade é executada durante o clone da Privacidade de dados.
- **Pedido de aplicação**: um trabalho da Privacidade de dados para Configuração de pós-clonagem com um pedido de aplicação mais alto pode iniciar antes de outro trabalho com pedido mais baixo.

> **Importante:** Evite criar várias políticas da Privacidade de dados com o mesmo Pedido de aplicação, pois o pedido de processamento resultante para aqueles com o mesmo pedido será inconsistente.

7. Opcional: Selecione **Compatível com rollback** para habilitar a capacidade de desanonimizar os dados de um trabalho da Privacidade de dados.
   Para obter mais informações, consulte Execute o rollback de um trabalho de privacidade de dados.
   Depois de selecionar **Compatível com rollback**, ao criar um trabalho da Privacidade de dados, a opção de reverter o trabalho se torna disponível.
8. Selecione a guia **Técnicas de campo classificadas de privacidade** para exibir a lista **Técnicas de campo classificadas de privacidade**.
9. Selecione uma entrada no campo **Tabela** para abrir o campo **Configuração da técnica de privacidade** para cada entrada da lista.
   A lista **Técnicas de campo classificadas de privacidade** exibe todos os dados a serem anonimizados na classe de dados selecionada. Para cada uma dessas entradas, você deve selecionar uma técnica de privacidade a ser aplicada.
10. Selecione uma **Configuração de técnica de privacidade** a ser aplicada.

> **Importante:** Se você não estiver anonimizando uma entrada, selecione a técnica **Não fazer nada** em vez de deixar a entrada em branco. Políticas com valores em branco no campo **Configuração da técnica de privacidade** não podem ser executadas quando usadas em trabalhos da Privacidade de dados.

11. Selecione **Enviar** ou **Salvar** para salvar o registro.

O que Fazer Depois

Configuração de um trabalho da Privacidade de dados.

Configuração de um trabalho da Privacidade de dados

Configure um trabalho da Privacidade de dados na instância de produção para usar dados anonimizados na instância de não produção para trabalhos de classe de dados e de usuário.

Antes de Iniciar

O trabalho da privacidade de dados é compatível com dois casos de uso de desidentificação:

- Dados confidenciais de sys_users específicos
- Dados confidenciais de uma classe de dados específica.

Função necessária: data_privacy_processor e administrador

Procedimento

1. Eleve para a função **data_privacy_processor**.
   Para obter detalhes sobre a elevação de função, consulte Elevar para uma função privilegiada.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

2. Navegue até **Segurança do sistema** > **Privacidade de dados** > **Trabalho da Privacidade de dados**.
3. Na lista Trabalhos da Privacidade de dados, clique em **Novo**.
4. No formulário, preencha os campos.

Campos de Trabalho da privacidade de dados

Campo	Descrição
Nome	Nome do trabalho.
Descrição	Descrição do trabalho.
Configuração de privacidade	A configuração de política de privacidade a ser usada para este trabalho. Para obter detalhes sobre as configurações de política de privacidade, consulte Como criar um política da Privacidade de dados.
Usuários	Selecione os usuários ou grupo de usuários a serem anonimizados nesta tarefa. Até 1.000 usuários de um grupo podem ser processados. **Nota:** Este campo é exibido somente quando a condição de política de privacidade selecionada requer uma seleção de registros do usuário.
Simulação	Execute o trabalho como um teste. Nenhum registro é afetado ao executar este trabalho. Os resultados são exibidos no campo **Resumo** como se o trabalho tivesse sido executado. **Nota:** A **simulação** deve ser desativada ao configurar um trabalho da Privacidade de dados com rollback. Consulte Execute o rollback de um trabalho de privacidade de dados para obter detalhes.
Estado	Estado do trabalho da Privacidade de dados: ◦ **Pronto para programar**: estado-padrão para novos trabalhos. ◦ **Rollback em andamento**: o trabalho foi definido para reverter a anonimização. ◦ **Rollback concluído**: o rollback do trabalho de anonimização foi concluído com sucesso. Um campo somente leitura.
Contagem de registro estimada	O número estimado de registros que este trabalho afeta. Um campo somente leitura.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Resumo	Um campo somente leitura que exibe os resultados do trabalho quando você o executa.
Início da janela de tempo	O início da janela de tempo para executar este trabalho. O trabalho será executado após a hora inserida neste campo. Um valor de tempo válido está em Tempo universal coordenado com base em uma notação de tempo de 24 horas.
Fim da janela de tempo	O fim da janela de tempo para executar este trabalho. O trabalho é executado antes da hora inserida neste campo. Se o trabalho ainda não tiver sido concluído, ele será pausado e retomado no próximo início da janela de tempo. A hora de término deve ser posterior à hora de início. Um valor de tempo válido está em Tempo universal coordenado com base em uma notação de tempo de 24 horas.

5. Clique com o botão direito do mouse no cabeçalho do formulário e selecione **Salvar** no menu de contexto.
   Depois de salvar o registro, os botões **Programar trabalho** e **Excluir trabalho** são exibidos.
6. Clique em **Programar trabalho** para executar seu trabalho.
   O trabalho é executado entre as horas selecionadas nos campos **Início da janela de tempo** e **Término da janela de tempo**. Se o trabalho não tiver sido concluído durante a janela de tempo de início e término, o trabalho continuará no próximo início da janela de tempo.

   Nota: Um trabalho só poderá ser executado uma vez, mesmo se a **Simulação** estiver selecionada. Para executar o mesmo trabalho novamente, crie um trabalho da Privacidade de dados usando os mesmos valores de campos.

7. Opcional: Escolha uma das opções a seguir:
   - **Cancelar trabalho**: cancela o trabalho da Privacidade de dados.
   - **Pausar**: pausará o trabalho e a gravação de rollback se o rollback tiver sido selecionado. Uma mensagem de aviso será exibida após um período de expiração de três dias para contextos de rollback. Consulte Execute o rollback de um trabalho de privacidade de dados para obter detalhes.
   - **Retomar**: reinicia um trabalho pausado. O rollback não é compatível com trabalhos retomados se pausados. Cancele o trabalho e crie um trabalho da privacidade de dados. A gravação usa um contexto de rollback não expirado.

Rollback de trabalho da Privacidade de dados

As mudanças do banco de dados são capturadas para ações como trabalhos e scripts para que as mudanças possam ser revertidas. Rollback de um trabalho da Privacidade de dados para quando o erro humano anonimiza inadvertidamente as informações incorretas do usuário. O rollback desanonimiza os dados do trabalho da Privacidade de dados.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Visão geral

- O rollback é limitado a alguns dias de acordo com a duração de expiração configurada do RollbackContext do novo RollbackType *REDACT*. Após a expiração do RollbackContext associado a um trabalho da Privacidade de dados, a função de rollback não estará mais disponível para esse trabalho.
  - Um contexto de rollback da desanonimização é salvo por três dias por padrão.
  - O tempo de expiração padrão pode ser definido como um valor superior a um pelo administrador da Privacidade de dados no **RollbackContext** do novo **RollbackType** *REDACT*. Defina o valor na propriedade do sistema Glide *glide.rollback.expiration_days_redact*. Consulte Reverter e excluir recuperação.

    Para saber mais sobre como adicionar ou criar uma propriedade do sistema, consulte Adicionar uma propriedade do sistema.

    para obter mais informações.
- O rollback está disponível para trabalhos da Privacidade de dados que estão em estado Concluído, Cancelado ou Erro.
- Para cada trabalho bem-sucedido de desanonimização sys_user configurado com uma política da Privacidade de dados compatível com o rollback ativado, um contexto de rollback é criado. Pode haver no máximo um contexto de rollback por trabalho da Privacidade de dados.

Execute o rollback de um trabalho de privacidade de dados

Execute o rollback de um trabalho de privacidade de dados em sua instância de não produção que usa dados anonimizados de sua instância de produção para um estado anterior à desidentificação de uma classe de dados ou trabalho do usuário.

Antes de Iniciar

Função necessária: data_privacy_admin ou data_privacy_processor, e administrador

Procedimento

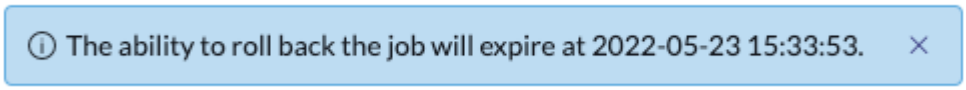
1. Eleve para a função **data_privacy_processor** ou **data_privacy_admin**.
   Para obter detalhes sobre a elevação de função, consulte Elevar para uma função privilegiada.
2. Navegue até **Todos** > **Segurança do sistema** > **Privacidade de dados** > **Trabalho de privacidade de dados**.

   Nota: Com antecedência, uma configuração de política de privacidade de dados compatível com o rollback deve ser criada. Como criar um política da Privacidade de dados.

3. Crie um trabalho de privacidade de dados e selecione uma configuração de privacidade compatível com o rollback.
   Consulte Configuração de um trabalho da Privacidade de dados.
4. Programação do trabalho para anonimização de dados.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Depois que o trabalho for executado, os dados serão anonimizados para a configuração selecionada.
- Uma mensagem é exibida no trabalho informando a hora de expiração. Dentro do período de expiração, você tem a capacidade executar o rollback do trabalho.



5. Eleve para a função **data_privacy_processor**.
6. Abra o trabalho de privacidade de dados a ser revertido.
7. Selecione **Rollback** para desanonimizar os dados.

Clone da privacidade de dados

Conforme os dados do cliente são clonados de uma instância de origem para uma instância de destino, normalmente da produção para a não produção, os dados confidenciais são desidentificados na instância de destino.

Um administrador da Privacidade de dados configura as políticas de pós-clonagem. Depois que o script de pós-clonagem for concluído na instância de destino, os usuários verão os dados desidentificados e não terão acesso aos dados originais. Os administradores da Privacidade de dados podem configurar políticas de desidentificação a serem aplicadas à instância de destino durante a clonagem para garantir que a instância de destino não tenha dados confidenciais originais. Uma ordem é especificada para a política relativa a outras políticas a serem executadas.

Nota: A clonagem da Privacidade de dados está disponível em instâncias auto-hospedadas.

O clone da Privacidade de dados tem os seguintes atributos adicionais:

- O plug-in de Privacidade de dados cria o script de pós-clonagem a ser executado na instância de destino.
- Os trabalhos de privacidade de dados criados para a configuração PostClone poderão ser executados em paralelo se não envolverem as mesmas tabelas.
- Um trabalho de privacidade de dados para Configuração PostClone com um Pedido de aplicação superior poderá iniciar antes de outro trabalho de ordem inferior se o trabalho com o pedido superior não envolver qualquer tabela relacionada a outro trabalho de pedido inferior.
- Com o plug-in de Privacidade de dados, as tabelas de privacidade de dados por padrão estão no conjunto de tabelas Clonar preservadores de dados.
- Uma tentativa de adicionar uma tabela de privacidade de dados (dp_ [table]) para clonar tabelas de exclusão receberá um aviso de que essa tabela não deve ser excluída.

Configuração da solicitação de clone da Privacidade de dados

A integração do clone da Privacidade de dados é configurada usando um script PostClone para criar e executar trabalhos da Privacidade de dados para políticas configuradas no destino. Depois de executar o script, os usuários verão os dados não identificados e não terão acesso aos dados originais.

Antes de Iniciar

Função necessária: data_privacy_clone_processor, data_privacy_admin e administrador

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Ative o plug-in Privacidade de dados (com.glide.data_privacy) na instância de origem.
   O plug-in só pode ser instalado por Suporte e atendimento ao cliente.
   O script PostClone da Privacidade de dados está instalado.
2. Eleve para a função **data_privacy_admin**.
   Para obter detalhes sobre a elevação de função, consulte Elevar para uma função privilegiada.
3. Navegue até **Segurança do sistema** > **Privacidade de dados** > **Configuração de política de privacidade**.
4. Criação de uma configuração de política de privacidade
   Selecione **Aplicar a todos na classe de dados** e **Aplicar ao clonar**. Para obter mais informações, consulte Como criar um política da Privacidade de dados.
5. Faça back-up das configurações da Privacidade de dados.
6. Como administrador da Privacidade de dados, envie uma solicitação de clone.

Resultados

O script PostClone da privacidade de dados é executado na instância de destino e o script PostClone cria um registro de trabalho federado da privacidade de dados na instância de destino. O trabalho federado cria e executa um trabalho da privacidade de dados para cada política pós-clonagem, na Ordem da aplicação, na instância de destino.A origem do backup é clonada para a instância de destino. O script PostClone da privacidade de dados cria e executa trabalhos da privacidade de dados para políticas configuradas na instância de destino.

O processador de clone da privacidade de dados elevado pode fazer logon na instância de destino e monitorar o estado do trabalho federado de pós-clonagem em dp_federated_job.list e dp_job.list.

Privacidade de dados

A aplicação da store de Privacidade de dados é um upgrade do Next Experience para classificação de dados e privacidade de dados com aparência e usabilidade modernas. A aplicação da store de Privacidade de dados é compatível com Utah e posteriores.

A privacidade de dados é composto por vários componentes, Visão geral, Classificação e Anonimização.

Visão geral

Use a seção Visão geral como ponto de partida para gerenciar seus dados e a conformidade da privacidade de dados. Consulte Visão geral da privacidade de dados para obter detalhes.

Classificação

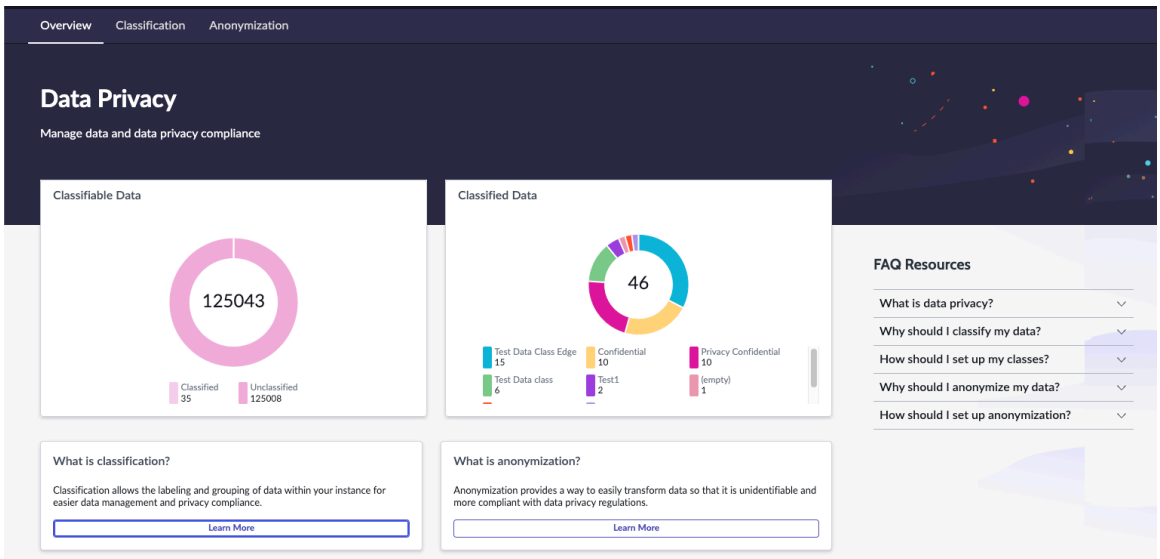
Classificação de dados é o processo de organizar dados em categorias que facilitam a recuperação, classificação e armazenamento para uso futuro. Usar um sistema de classificação ajuda a enfocar os requisitos da política de confidencialidade e segurança. Classifique os dados a serem usados para anonimização. Para obter informações sobre classes de dados e classificação, consulte Classificação de dados.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Visão geral da privacidade de dados

A página inicial da Visão geral é um ponto de partida para gerenciar seus dados e a conformidade da privacidade de dados.

O painel Visão geral relata o estado atual das classificações de dados e trabalhos de anonimização na instância. Você pode exibir seus dados com o painel Visão geral para ver quantos dados podem ser classificados, as classes de dados disponíveis, a quantidade de dados em cada classe e um status geral dos trabalhos de anonimização. Os dados classificados são divididos em diferentes categorias. Selecionar uma subcategoria em qualquer gráfico adicionará ou removerá a categoria do gráfico geral e ajustará as contagens.



Dados classificáveis

Exibe o número total de registros de dados na instância que podem ser classificados. O número é dividido entre o número total de dados classificados e o total de dados não classificados. Isso fornece aos administradores uma exibição rápida de oportunidades de classificação em potencial.

Dados classificados

Exibe o número total de registros de dados na instância que foram classificados. O número é dividido entre o número total de dados classificados para cada classe de dados atribuída. Isso fornece uma compreensão rápida de quantos dados foram classificados em cada área.

Trabalhos de anonimização

Exibe trabalhos de privacidade de dados que estão em processo de trabalhos concluídos em sua instância de não produção para trabalhos de classe de dados e usuário.

Saiba mais

As seções **Saiba mais** fornecem uma visão rápida do entendimento da classificação e da anonimização, bem como uma maneira fácil de iniciar o processo.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Recursos de perguntas frequentes

Acesse recursos de aprendizado do produto sobre classificação ou anonimização para obter informações adicionais sobre como começar a proteger sua instância com a privacidade de dados.

Ativação da privacidade de dados

A Privacidade de dados inclui a classificação de dados e a anonimização e é instalada a partir de ServiceNow Store.

Antes de Iniciar

Para usar a anonimização de dados, a Privacidade de dados (Clássico) deve primeiro ser ativada com o direito ServiceNow Vault. Consulte Como ativar a Privacidade de dados (Clássico) para obter informações adicionais.

Função necessária: administrador

Procedimento

1. Navegue até **Todas** > **Aplicações do sistema** > **Todas os aplicações disponíveis** > **Todas** > **Privacidade de dados**.
2. Encontre a aplicação usando os filtros e a barra de pesquisa.

   Você pode pesquisar a aplicação pelo nome ou ID. Se não conseguir encontrar uma aplicação, pode ser necessário solicitá-la na ServiceNow Store.

   Acesse o site ServiceNow Store para ver todos os aplicativos disponíveis e obter informações sobre como enviar solicitações para a loja. Para obter informações sobre notas de versão cumulativa para todos os aplicativos liberados, consulte as ServiceNow Store notas de versão do histórico de versão.
3. Escolha uma versão na lista e selecione **Instalar**.

   Na caixa de diálogo Instalar exibida, todas as dependências instaladas junto com a aplicação são listadas.
4. Se for solicitado, siga os links para ServiceNow Store e obtenha direitos adicionais para dependências.
5. Opcional: Se os dados de demonstração estiverem disponíveis e você quiser instalá-los, marque a caixa de seleção **Carregar dados de demonstração**.

   (Optional) Os dados de demonstração compreendem registros de amostra que descrevem os recursos da aplicação para casos de uso comuns. Carregue os dados de demonstração ao instalar a aplicação pela primeira vez em uma instância de desenvolvimento ou teste.

   > **Importante:** Se você não carregar os dados de demonstração durante a instalação, eles não estarão disponíveis para serem carregados mais tarde.
6. Selecione **Instalar**.

Classificação de dados

Agrupe dados por tipo, usando classificações de dados predefinidas ou definidas por usuário. Se você tiver uma função de auditor ou administrador de classificação de dados

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

atribuída, será possível administrar diferentes classes de dados ou analisar visualmente o estado atual de diferentes tipos de dados na instância.

Data Classification habilita suporte para:

- Visibilidade nos tipos de dados hospedados em instâncias Now Platform.
- Conformidade com as leis de privacidade e cumprimento dos requisitos de regulamentação para indústrias como serviços financeiros e fabricação de dispositivos médicos.

Classificações de dados

A classificação de dados é um processo independente no qual você aplica manualmente as classificações de dados nas entradas de dicionário existentes em qualquer tabela. Consulte Tabelas Dicionário de dados para obter informações adicionais.

- Classifique os dados conforme achar apropriado para o seu negócio e poderá alterar as classes de dados disponíveis conforme necessário.
- Ao classificar dados, é possível usar as classificações de dados predefinidas ou criar suas próprias. Embora o uso de classificações de dados predefinidas seja opcional, é aconselhável fazê-lo como ponto de partida. Essas classificações de dados predefinidas são incluídas nos dados de demonstração que você pode instalar na instância.
- Se você criar suas próprias classificações de dados, também poderá projetar um sistema hierárquico em camadas com classificações de dados primários e secundários.

Nota: Data Classification suporta a separação de domínio e a própria tabela data_classification tem processo separado. Consulte Domain Separation e Data Classification para obter informações adicionais.

Casos de uso

A GDPR (General Data Protection Regulation) é uma regulamentação da União Europeia cujo propósito é fornecer aos indivíduos controle sobre seus próprios dados pessoais. É possível usar classificações de dados, como informações de identificação pessoal, para identificar onde os dados pessoais estão sendo armazenados em sua instância. Ao aplicar os mecanismos de segurança apropriados para proteger esses dados pessoais contra vazamento, a sua organização satisfaz os requisitos da GDPR.

Se você armazenar as informações do cliente no Now Platform, use o código de classificação das informações de identificação pessoal (PII) onde for necessário para rastrear os dados sujeitos à regulamentação pelas leis de privacidade local.

É possível aplicar uma classificação de dados Restritos a colunas da tabela de funcionários que armazenam informações confidenciais de funcionário como número do seguro social (SSN). Os administradores e auditores então podem usar o painel Visão geral para confirmar que você designou as classificações de dados atribuídos às colunas corretas. Eles também podem exibir detalhes de classificação para tipos restritos de informações.

Criação de classificações de dados

Crie suas próprias classificações de dados definidas pelo usuário na tabela [data_classification] que você pode atribuir a colunas específicas em tabelas específicas. Crie novas classes de dados para iniciar o processo de classificação.

Antes de Iniciar
Função necessária: data_classification_admin, administrador

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegue até **Tudo** > **Segurança do sistema** > **Privacidade de dados** > **Classificação**.
2. Selecionar **+ Adicionar classe de dados**.

   Nota: Existem várias classes de dados incluídas com o sistema de base.

3. Preencha os campos no formulário.

Campo	Descrição
Nome da classe	Nome da classificação de dados.
Classificação primária	Nome da classificação de dados primária à qual esta classificação de dados está subordinada. Deixe o campo em branco se esta classificação de dados não for uma classificação de dados secundária para primária.
Descrição	Descrição da classificação de dados.

4. Clique em **Enviar**.
   A nova classe de dados é adicionada. Se a classe de dados for secundária, ela será listada abaixo de primária na barra de navegação à esquerda.

Classificar dados

Agrupe dados por tipo, usando classificações de dados predefinidas ou definidas por usuário. Atribua classificações de dados a colunas de tabela específicas na tabela Dicionário [sys_dictionary]. Quando você atribui classificações de dados, ele cria entradas na tabela Dicionário-Classe de Dados [m2m_dictionary_dataclass], que você pode revisar no painel Visão geral.

Antes de Iniciar

Função necessária: data_classification_admin, administrador

Procedimento

1. Selecione **Novo** para atribuir dados de uma tabela a ser classificada.
2. Selecione a classe de dados no menu suspenso.
3. Selecione os registros que refletem as tabelas e colunas a serem classificadas.
   Escolha linhas adicionais a serem exibidas por página na tabela para simplificar a localização de uma tabela específica.
4. Selecione **Classificar dados**.
   Os dados são classificados sob o Nome de classificação na tabela Dados classificados.
5. Exiba ou exporte os dados para Excel, CSV, JSON ou PDF.
   Escolha baixar os dados no formato escolhido ou recebê-los por e-mail.

Anonimização em tempo real

Use a política de RTA (Real Time Anonymization) para anonimizar as entradas de dados em tempo real.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Visão geral da RTA

Os usuários criam uma política de RTA por meio da página Políticas de anonimização. É possível selecionar as colunas das tabelas de destino para RTA. Nesse caso, usam-se os padrões de dados ativos e aplicam-se as políticas delas a todas as entradas de registro válidas das colunas selecionadas para RTA. Se uma entrada corresponder a um padrão de dados ativo, a técnica de anonimização associada a ele será usada para anonimização.

Dica: Se for necessário mudar a técnica de anonimização, consulte Configurar Descoberta de dados padrões.

Falhas da anonimização em tempo real

Se uma política de RTA apresentar falha, você poderá revisar o status dela com a tabela Falhas da anonimização em tempo real.

Falhas da anonimização em tempo real

Revise as falhas da RTA (Real Time Anonymization)

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Navegue até **Todos** > **Segurança do sistema** > **Privacidade de dados(Clássico)**.
2. Revise as falhas de RTA na tabela.

Título do campo	Descrição
Coluna da tabela	A coluna da tabela em que a falha ocorreu.
Motivo da falha	Categoria da causa das falhas.
Detalhes do motivo da falha	Descrição resumida da causa da falha.
Configuração de privacidade	A configuração de privacidade da RTA que falhou.
Registro	O registro específico que falhou.
Nome da tabela	Tabela em que a falha ocorreu.
Carimbo de data/hora	Hora da falha.

Descoberta de dados

Use Descoberta de dados para identificar dados confidenciais em uma instância, como informações de cartão de crédito, e-mails ou números de CPF.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Explore a Descoberta de dados Conheça a Descoberta de dados.	Configure a Descoberta de dados Obtenha ajuda para configurar a Descoberta de dados.
Funções na Descoberta de dados Saiba mais sobre as funções na Descoberta de dados.	Resultados da Descoberta de dados Analise os resultados da Descoberta de dados.

Como explorar o Descoberta de dados

Use Descoberta de dados para identificar dados confidenciais em uma instância, como informações de cartão de crédito, e-mails ou números de CPF.

Descoberta de dados executa um conjunto de tarefas definido pelo usuário em um conjunto de tabelas. As tarefas pesquisam e reportam informações confidenciais para revisão no painel do Descoberta de dados. Um trabalho agendado usa automaticamente todos os padrões de dados ativos e tabelas de destino quando é executado.

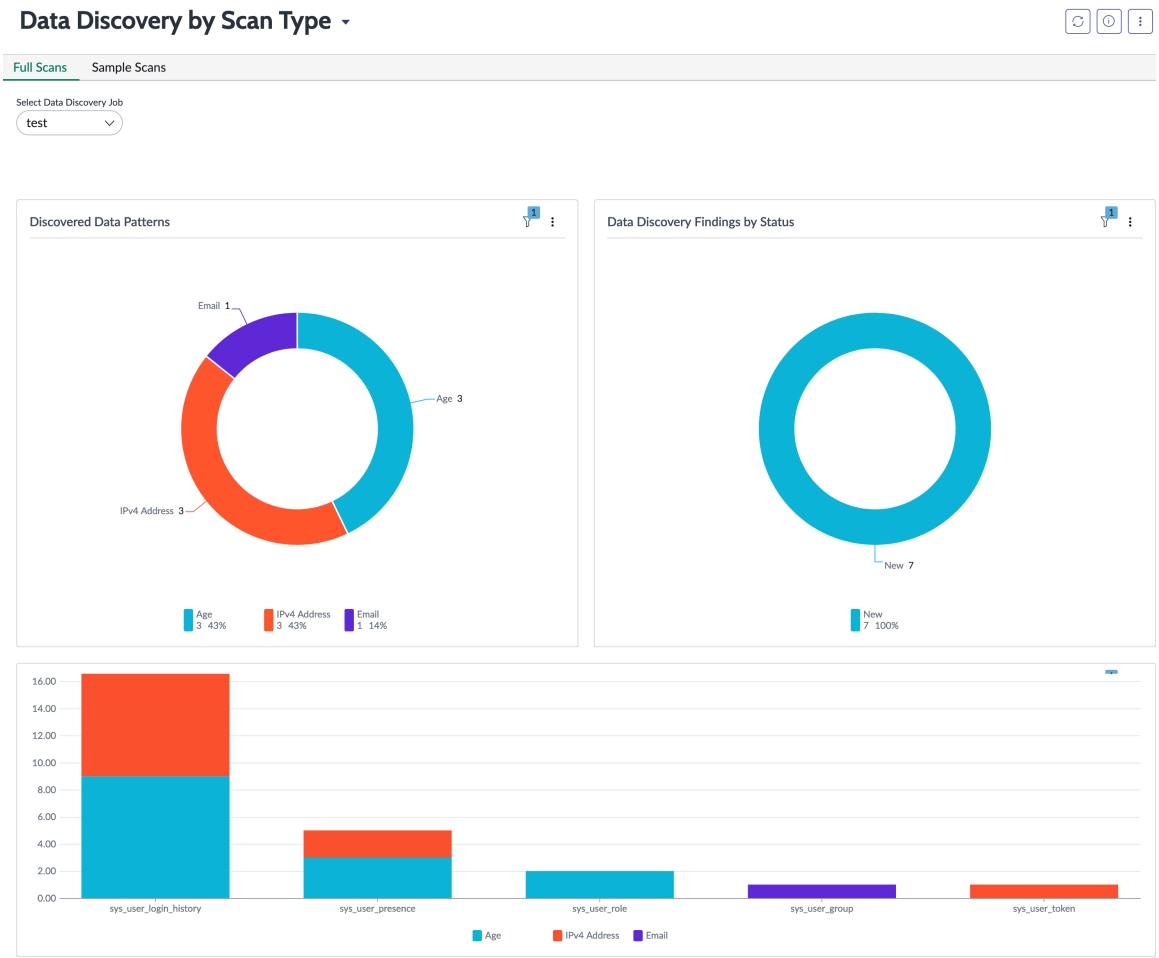
Descoberta de dados também inclui funções pré-alocadas com níveis variados de acesso aos dados.

Acessar os painéis de Descoberta de dados

Navegue até **Todos** > **Segurança do sistema** > **Descoberta de dados (Clássico)** > **Painel** para exibir o painel do Descoberta de dados e revisar os achados da sua tarefa atual.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Painel da Descoberta de dados



Padrões de dados descobertos

Dica: Selecione um registro para exibir mais informações e tomar medidas adicionais com os resultados. Consulte Resultados da tarefa do Descoberta de dados para obter mais informações.

O gráfico "Padrões de dados descobertos" exibe o número e a porcentagem dos padrões de dados descobertos no momento. Selecione uma seção para realizar outras ações.

Resultados da descoberta de dados por status

O gráfico "Resultados da descoberta de dados" revisa o número e a porcentagem de padrões de dados descobertos no momento de acordo com o status deles.

Tabelas com descobertas

As "Tabelas com descobertas" destacam em quais tabelas estão os dados descobertos no momento e o padrão de dados deles.

Colunas com dados descobertos

A seção "Colunas com dados descobertos" revisa os dados descobertos no momento por coluna.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Como ativar o Descoberta de dados

A aplicação instala plug-ins e aplicações de Descoberta de dados e aplicações de ServiceNow® Store relacionados, caso ainda não estejam instalados.

Antes de Iniciar

A descoberta de dados requer uma assinatura separada do restante do Now Platform.

Para adquirir uma assinatura, entre em contato com o seu gerente de contas ServiceNow. Quando você compra uma assinatura, determinados plug-ins são ativados automaticamente. Se um plug-in pago não for ativado automaticamente, você poderá ativá-lo manualmente na lista Todas as aplicações em sua instância.

Nota:

Antes de comprar uma assinatura, você pode avaliar o recurso em uma instância de não produção sem custos, solicitando-o em Now Support Catálogo de serviços.

Função necessária: admin

Por Que e Quando Desempenhar Esta Tarefa

Os seguintes itens são instalados com a descoberta de dados:

- Funções
- Tabelas

Para obter mais informações sobre as funções e tabelas instaladas, consulte Funções Descoberta de dados e Padrões de dados padrão.

Procedimento

1. Navegue até **Todos** > **Aplicações do sistema** > **Todas as aplicações disponíveis** > **Todas**.
2. Encontre o plug-in de Descoberta de dados (sn_data_discovery) usando os critérios de filtro e a barra de pesquisa.

   Pesquise o plug-in pelo nome ou ID. Se não conseguir encontrar um plug-in, talvez seja necessário solicitá-lo ao pessoal ServiceNow.

3. Selecione **Instalar** para iniciar o processo de instalação.

   Nota: Quando a separação de domínio e o administrador delegado estão habilitados em uma instância, o usuário administrativo deve estar no domínio **global**. Caso contrário, será exibido o seguinte erro: `A instalação da aplicação não está disponível porque há outra operação em execução: ativação de plug-in para <plugin name>.`

   Você verá uma mensagem após a conclusão da instalação.

Classificar dados na página de descobertas de Descoberta de dados

Classifique os dados confidenciais encontrados por todas as tarefas bem-sucedidas por meio das descobertas de Descoberta de dados.

Antes de Iniciar

Função necessária: data_discovery_admin

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Uma tarefa deve concluir uma execução bem-sucedida antes que qualquer dado de resultado possa aparecer para ser classificado.

Por Que e Quando Desempenhar Esta Tarefa
A página de descobertas de Descoberta de dados mostra todas as entradas de dados que foram encontradas por uma tarefa. A página de Descobertas permite revisar as entradas e associá-las a uma classificação.

Procedimento

1. Navegue até **Segurança do sistema** > **Descoberta de dados (clássico)** > **Achados da descoberta de dados**.
2. Selecione a entrada que você deseja classificar.
3. Na lista de descobertas de Descoberta de dados, selecione **Classificar**.
4. Selecione as classes de dados que você deseja associar às entradas da tabela.
5. Selecione **Classificar**.

Trabalhos do Descoberta de dados

Descoberta de dados revisa suas informações de destino usando padrões de dados definidos pelo usuário e tabelas de destino.

Descoberta de dados funciona primeiro programando uma tarefa na seção **Tarefa de Descoberta de dados**. Quando uma tarefa programada é executada, todos os padrões de dados ativos são pesquisados nas tabelas de destino atuais. Para obter mais informações sobre como criar e configurar uma tarefa Descoberta de dados, consulte Configuração de um trabalho de Descoberta de dados.

Nota: Os exemplos de trabalhos de verificação examinam até dez mil registros por tabela por padrão.

Aviso: Se houver duas execuções de um trabalho em um pequeno período, o número de linhas verificadas poderá exibir 0 para a segunda execução.

Padrões de dados do Descoberta de dados

A seção **Padrões de dados** mostra todos os padrões de dados atuais, ativos e inativos. Um padrão de dados é uma expressão regular usada para corresponder a dados confidenciais. Para obter mais informações sobre como acessar e configurar padrões de dados, consulte Configurar Descoberta de dados padrões. A seção **Padrões de dados ativos** mostra somente padrões ativos. Os padrões inativos não são exibidos.

Tabelas de destino

A seção **Tabelas de destino** lista todas as tabelas que podem ser processadas para um trabalho. Para acessar as tabelas de destino, selecione **Tabelas de destino**.

As tabelas a seguir não são compatíveis:

- sr
- sysx
- v
- sh$
- syslog

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- ua
- usageanalytics
- ecc
- clone
- jrobin
- pa
- sla_repair_log
- scan
- gcf
- fm_log
- log
- np$
- sn_data_discovery
- dp_configuration
- dp_federated_job
- dp_field_technique
- dp_job
- dp_job_summary
- dp_primary_reference
- dp_technique
- data_classification
- m2m_dictionary_dataclass

Configuração granular

A ferramenta de configuração granular permite controles mais específicos e refinados para descobrir dados confidenciais em uma tabela. No entanto, há diferenças importantes em sua operação, em comparação com um trabalho tradicional de descoberta de dados. Uma configuração granular verifica somente as colunas especificadas de uma tabela para descoberta, relatando os resultados de acordo com o registro. As descobertas da verificação de configurações granulares, chamadas de descobertas granulares, têm suas ações especificadas por registro e exigem a anonimização da função data_privacy_admin.

Configuração de um trabalho de Descoberta de dados

Configure um trabalho de Descoberta de dados e revise o status dos trabalhos em andamento. Um trabalho de Descoberta de dados define quando um padrão é executado em uma tabela de destino.

Antes de Iniciar

Função necessária: data_discovery_admin

Procedimento

1. Navegue até **Segurança do sistema** > **Descoberta de dados(Classic)** > **Trabalho de descoberta de dados**.
2. Na lista Trabalhos de Descoberta de dados, selecione **Novo**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Preencha os campos no formulário de trabalho de Descoberta de dados.

Campos de trabalho de Descoberta de dados

Campo	Descrição
Nome	Nome do trabalho.
Descrição	Descrição do trabalho.
Tipo de Verificação	Número de entradas a serem verificadas. Os estados possíveis são os seguintes: ◦ **Amostra**: verifica 10.000 entradas. ◦ **Completa**: verifica todas as entradas.
Contexto	Detalhes do trabalho sobre padrões verificados, metas de entradas de tabelas atingidas e tempo decorrido.
Estado	Estado do trabalho de Descoberta de dados. Estes são os estados possíveis: ◦ **Pronto para programar**: estado-padrão para novos trabalhos. ◦ **Programado**: o trabalho está programado para ser executado. ◦ **Em andamento**: o trabalho está em execução. ◦ **Concluído**: o trabalho foi concluído com sucesso. ◦ **Erro**: o trabalho parou devido a um erro. ◦ **Cancelado**: o trabalho foi cancelado. ◦ **Pausado**: o trabalho está pausado.
Resumo	Exibe os resultados do trabalho depois de você executá-lo.
Data de início	Define a data de início do trabalho.
Início da janela de tempo	O início da janela de tempo para executar este trabalho. O trabalho será executado após a hora inserida neste campo. A hora inserida no campo **Início da janela de tempo** deve ser antes da hora inserida no campo **Término da janela de tempo**. **Nota:** Os horários válidos devem estar no Tempo Universal Coordenado e em ciclos de 24 horas.
Fim da janela de tempo	O fim da janela de tempo para executar este trabalho. O trabalho é executado até a hora inserida neste campo. Se o trabalho ainda não tiver sido concluído, ele será pausado e retomado na próxima janela de tempo. A hora inserida no campo **Término**

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	da janela de tempo deve ser depois da hora inserida no campo **Início da janela de tempo**. **Nota:** Os horários válidos devem estar no Tempo Universal Coordenado e em ciclos de 24 horas.

4. Selecione **Enviar**.
   Os botões **"Programar trabalho"** e **"Atualizar"** serão exibidos.
5. Clique em **"Programar trabalho"** para executar seu trabalho.
   O trabalho é executado entre as horas selecionadas nos campos **Início da janela de tempo** e **Término da janela de tempo**. Se o trabalho não tiver sido concluído durante a janela de tempo de início e término, o trabalho continuará no próximo início da janela de tempo.
6. Opcional: Escolha uma das opções a seguir:
   - **Cancelar trabalho**: cancela o trabalho.
   - **Pausar**: pausa o trabalho.
   - **Retomar**: reinicia um trabalho pausado.

Configurar Descoberta de dados padrões

Configure um padrão de Descoberta de dados e revise os padrões atuais. Um padrão de Descoberta de dados define a expressão regular usada para corresponder dados a uma tabela de destino.

Antes de Iniciar

Função necessária: data_discovery_admin

Procedimento

1. Navegue até**Segurança do sistema** > **Descoberta de dados** > **Todos os padrões de dados**.
2. Na lista de padrões ativos de Descoberta de dados, selecione **Editar**.
3. No formulário de campos de trabalho de Descoberta de dados, preencha os campos.

Campos de trabalho de Descoberta de dados

Campo	Descrição
Escopo interno	Escopo do padrão.
Descrição	Descrição do trabalho.
Nome	Nome do padrão de dados.
Aplicação	Escopo da aplicação do padrão.
Expressão	Expressão regular usada para descobrir o padrão de dados. **Nota:** O tamanho da expressão deve ser inferior a 1.000 caracteres.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Palavra-chave (opcional)	Uma palavra específica (ou palavras separadas por vírgula) a ser pesquisada em uma expressão. Deve ser usado com **Proximidade da palavra-chave** **Nota:** Uma palavra-chave pode ser usada para pesquisar contexto adicional para um padrão. Por exemplo, usar a palavra-chave pode ajudar a diferenciar entre uma data de nascimento e uma data de contratação, desde que elas tenham a mesma formatação de DD/MM/AA.
Proximidade da palavra-chave (opcional)	A que distância da expressão as palavras-chave devem ser pesquisadas. Deve ser usado com a **Palavra-chave** **Nota:** O padrão é de 30, com limite superior de 64

4. Selecione **Enviar**.
   - O botão **Testar** permite que você teste sua expressão regular antes de enviar a lista de padrões de dados.

O padrão de dados precisa ser definido como ativo para ser usado com trabalhos agendados.

5. Navegue até**Segurança do sistema** > **Descoberta de dados** > **Padrões de dados ativos**.
6. Na lista de padrões ativos de Descoberta de dados, selecione **Editar**.
7. Selecione a lista de padrões em **Listas disponíveis** e mova-a para **Listas selecionadas**.

Padrões de dados padrão

Revise as expressões regulares de padrão de dados incluídas no Descoberta de dados. Esses padrões de dados padrão podem ser usados para filtrar entradas de tabela para classificação adicional.

A seguir estão os padrões padrão disponíveis para descoberta de dados.

Nome	Descrição	Expressão regular	Palavras-chave	Exemplos
Idade	A idade de uma pessoa entre 0 e 99	\b([0-9] | [1-9] [0-9] | 1[012] [0-9])\b	age	Correspondente 24 Não correspondente • 103 • -2

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome	Descrição	Expressão regular	Palavras-chave	Exemplos
Data de nascimento	Data de nascimento usando o formato DD/MM/AAAA	\b[0-3]?[0-9]/[0-3]?[0-9]/(?:[0-9]{2})?[0-9]{2}\b	dn, aniversário, data de nascimento	Correspondente • 06/18/2012 • 1/1/19
E-mail	Endereço de e-mail padrão	\b[\w!#$%&'*+/=?`{\|}~^-]+(?:\.[\w!#$%&'*+/=?`{|}~^-]+)*@(?:[a-zA-Z0-9-]+\.)+[a-zA-Z]{2,6}\b		Correspondente • joaodasilva@servidordee • professordehistoria@facu Não correspondente • naoéumemail.com • emailinválido@.org
Número de identificação do veículo	Um VIN (Vehicle Identification Number, número de identificação do veículo)	\b[A-HJ-NPR-Z0-9]{17}\b		Correspondente AHUYA31581L000000
Endereço IP	Endereço IP padrão	IP de quatro dígitos \b(?:(?:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.){3}(?:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\b IP de seis dígitos \b(((?:[0-9A-Fa-f]{1,4}(?::[0-9A-Fa-f]{1,4})*)?)::((?:[0-9A-Fa-f]{1,4}(?::		IP de quatro dígitos correspondente 102.28.46.103 IP de seis dígitos correspondente 914b:d45a:61ea:6346:59bc

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome	Descrição	Expressão regular	Palavras-chave	Exemplos
		[0-9A-Fa-f]{1,4})*)?)) | ((?:[0-9a-fA-F]{1,4}:){7}[0-9a-fA-F]{1,4})\b		
Cartão de crédito - Visa	Número do cartão de crédito Visa	\b4[0-9]{12}(?:[0-9]{3})?\b		Correspondente 4444434342424242
Cartão de crédito - American Express	Número do cartão de crédito American Express	\b3[47][0-9]{13}\b		Correspondente 378225246366005
Cartão de crédito - Mastercard	Número do cartão de crédito Mastercard	\b(?:5[1-5][0-9]{2}|222[1-9]|22[3-9][0-9]|2[3-6][0-9]{2}|27[01][0-9]|2720)[0-9]{12}\b		Correspondente 5555444455554444
Cartão de crédito - Diners Club	Número do cartão de crédito Diners Club	\b3(?:0[0-5]|[68][0-9])[0-9]{11}\b		Correspondente 3056930009020004
Cartão de crédito - Discover	Número do cartão de crédito Discover	\b6(?:011|5[0-9]{2})[0-9]{12}\b		Correspondente 6011025690875424
Cartão de crédito- CCV	Número de segurança do cartão de crédito	\b[0-9]{3,4}\b	cvv,código de verificação,código de segurança	Correspondente 124
Cartão de crédito- Data de validade	Validade do cartão de crédito no formato MM/AAAA	\b(([1-9])|(0[1-9]|1[0-2]))\/?([0-9]{4}|[0-9]{2})\b	validade,val	Correspondente • 02/2027 • 04/23 Não correspondente 03/9
EUA- Número de seguridade social	Número de seguridade social para cidadãos dos EUA	\b(?!666|000|9\d{2})\d{3}-(?!00)\d{2}-(?!0{4})\d{4}\b		Correspondente 001-22-111

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome	Descrição	Expressão regular	Palavras-chave	Exemplos
EUA - Número de telefone	Número de telefone dos EUA **Aviso:** Não usa o código de chamada dos EUA.	\b\(?([0-9]{3})\)?[-.]?([0-9]{3})[-.]?([0-9]{4})\b		Correspondente 2065550199 Não correspondente 1 555 238 0199
EUA- Número de passaporte	Número de passaporte dos EUA com nove dígitos	\b[a-zA-Z0-9]\\d{8}\b		Correspondente 770022122
EUA- ID do contribuinte	Número de ID de contribuinte dos EUA	\b(9\d{2})([\-]?)([7]\d|8[0-8])([\-]?)(\d{4})\b		Correspondente 927 70 5828
EUA- Número da carteira de habilitação do estado da Califórnia	Número da carteira de habilitação do Estado da Califórnia, EUA	\b[a-zA-Z]\d{7}\b		Correspondente A0002144
EUA- Número de roteamento do banco	Número de roteamento do banco dos EUA (ABA)	\b((0[0-9])|(1[0-2])|(2[1-9])|(3[0-2])|(6[1-9])|(7[0-2])|80)([0-9]{7})\b		Correspondente 125210305

Configure tabela de destino da Descoberta de dados

Adicione tabelas de destino a serem usadas em trabalhos de Descoberta de dados. Somente tabelas de destino serão verificadas quanto a padrões de dados.

Antes de Iniciar

Função necessária: data_discovery_admin

Por Que e Quando Desempenhar Esta Tarefa

Quando um trabalho de Descoberta de dados for executado, ele será executado em todas as tabelas de destino com todos os padrões ativos.

Procedimento

1. Selecione **Segurança do sistema** > **Descoberta de dados (Clássica)** > **Tabelas de destino**.
2. Selecione **Novo**.
3. Selecione sua tabela de destino no campo **Nome da tabela**.
4. Selecione **Enviar**.

Ativação de trabalhos paralelos da Descoberta de dados

Use trabalhos paralelos para reduzir o tempo de execução de trabalhos da Descoberta de dados.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: administrador

Procedimento
Por padrão, a Descoberta de dados executa trabalhos usando uma só thread. É possível ativar várias threads para verificações completas da Descoberta de dados.

1. No filtro de navegação, digite `sys_properties.list`.
2. Crie a propriedade `com.glide.data_discovery.max_concurrent_item_workers`
3. Verifique se o **Tipo** é `inteiro`.
4. **Importante:** É recomendável iniciar com um pequeno número de processos de execução por nó (dois ou três).

   No campo **Valor**, insira um número máximo de cinco para os processos de execução dos trabalhos paralelos.

Funções Descoberta de dados

Você pode atribuir funções do Descoberta de dados para limitar o acesso do usuário a determinados tipos de dados.

Administrador de descoberta de dados [sn_data_discovery.data_discovery_admin]

Exiba, crie e modifique padrões de dados e trabalhos relacionados.

- Padrões de dados:
  - Criar
  - Leitura
  - Atualizar
  - Excluir
- Padrões de dados ativos:
  - Excluir
  - Leitura
- Tarefas:
  - Criar
  - Leitura
  - Atualizar
  - Excluir
  - Programação
  - Pausar
  - Retomar
  - Cancelar
- Tabelas de destino:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

  - Criar
  - Leitura
  - Gravar
- Configuração granular:
  - Criar
  - Leitura
  - Atualizar
  - Excluir
- Descobertas granulares:
  - Criar
  - Leitura
  - Ações

    Nota: Usuários com esta função só podem realizar a ação de ignorar

Contém as funções

Lista de funções contidas na função.

- data_classification_auditor
- data_classification_admin
- sn_data_discovery.data_discovery_api_processor

Grupos

Lista de grupos aos quais esta função está atribuída por padrão.

Nenhum.

Considerações especiais

Esta função é atribuída automaticamente aos administradores na instalação do produto.

Nota: Evite conceder uma função de administrador quando houver mais funções especializadas disponíveis.

Auditor de descoberta de dados [sn_data_discovery.data_discovery_auditor]

Leia padrões de dados e tabelas de destino.

- Ler padrões de dados
- Ler padrões de dados ativos
- Ler tarefas do Descoberta de dados
- Ler tabelas de destino
- Revisar a configuração granular
- Revisar descobertas granulares

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Contém as funções

Lista de funções contidas na função.

Nenhum.

Grupos

Lista de grupos aos quais esta função está atribuída por padrão.

Nenhum.

Considerações especiais

Nenhum.

Administrador de classificação de dados [data_classification_admin]

Leia a tabela de padrões de dados, trabalhos de descoberta e data_classification quando uma descoberta de padrão específica habilitada for classificada.

Contém as funções

A função de classificação de dados contém a lista de funções contidas na função data_classification_auditor.

Grupos

Lista de grupos aos quais esta função está atribuída por padrão.

Nenhum.

Considerações especiais

Nota: Para obter mais informações sobre a função de administrador de classificação de dados, consulte Instalando dados de demonstração do plug-in Data Classification.

Resultados da tarefa do Descoberta de dados

A página de descobertas do Descoberta de dados mostra detalhes sobre os dados encontrados por uma tarefa. Você pode usar a página Descobertas para revisar os resultados de uma tarefa e começar a classificar os dados.

A página Descobertas do Descoberta de dados exibe os seguintes detalhes após a conclusão de uma tarefa.

Coluna	Descrição
Entrada do dicionário	Coluna da tabela de destino em que os dados estavam
Tabela	Tabela de destino em que os dados foram encontrados
Padrão de dados	Padrão de dados usado para localizar os dados

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Coluna	Descrição
Contagem de correspondência de padrão de dados	Número de entradas de dados que correspondem ao padrão de dados
Contagem total de verificação de linha	Número de linhas verificadas durante a tarefa
Percentual de linhas correspondentes	Percentual de linhas na tabela de destino que correspondem ao padrão de dados
Tarefa do Descoberta de dados	Tarefa usada na tabela de destino
Status	Status da entrada

Depois de executar uma tarefa do Descoberta de dados, os resultados ficam com o status Novo. Se nenhuma ação for necessária, você não precisa mexer nos dados, o que define automaticamente o status como Ignorado. Caso contrário, você pode classificar os dados, por exemplo, criando classificações de dados definidas pelo usuário, para se preparar para a anonimização de dados usando a ferramenta Data Classification.

Descobertas granulares

Os usuários podem selecionar a ação **Rastrear descobertas granulares** para usar a página Descobertas granulares a fim de tomar medidas sobre registros descobertos específicos. Para obter mais informações, consulte Descobertas granulares.

Proteções Disponíveis

Selecione o botão **Proteções disponíveis** para revisar o serviço de controle de entradas, o status, as anotações e o último check-in. A partir da versão Xanadu, esse recurso somente dá suporte à Criptografia em nível de coluna.

Também é possível acessar os serviços de proteção no "Painel". Para obter mais informações sobre o painel, consulte Descoberta de dados.

Consolidar descobertas

Os resultados do trabalho podem ser consolidados usando o botão **Consolidar descobertas**. Os resultados do trabalho compartilhados entre dois trabalhos separados serão consolidados no último trabalho executado.

Nota: Somente trabalhos de verificação completa concluídos podem ser consolidados

Classificar dados na página de resultados de tarefa do Descoberta de dados

Classifique os dados em Descoberta de dados diretamente da página de resultados de uma tarefa.

Antes de Iniciar

Função obrigatória: data_discovery_admin e admin

Uma tarefa deve concluir uma execução bem-sucedida antes que qualquer dado de resultado possa aparecer para ser classificado.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Vá para **Segurança do sistema** > **Descoberta de dados** > **Tarefa de descoberta de dados**.
2. Selecione a entrada que você deseja classificar.
3. Na lista de descobertas de Descoberta de dados, selecione **Classificar**.
4. Selecione as classificações de dados que você deseja associar às entradas da tabela.
5. Selecione **Classificar**.

Tipos de dados compatíveis com a Descoberta de dados

Verifique quais tipos de campo são compatíveis ao usar a Descoberta de dados.

Nota: Nem todos os tipos de campo que foram classificados estão disponíveis para a Descoberta de dados.

Alguns tipos de campo de alto risco estão desativados por padrão, conforme detalhado na tabela. Para obter mais informações sobre campos, consulte Tipos de campo.

Tipos de campo compatíveis com a descoberta de dados

Tipo de campo	Disponível por padrão
áudio	Não
condição	Não
condition_string	Não
moeda	Sim
decimal	Sim
due_date	Sim
variável	Sim
glide_date	Sim
glide_date_time	Sim
glide_duration	Não
glide_time	Sim
html	Não
ícone	Não
inteiro	Sim
ip_addr	Não
ip_address	Não
registro	Sim
journal_input	Sim
journal_list	Sim
longint	Sim
name_values	Não

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tipo de campo	Disponível por padrão
percent_complete	Não
phone_number_e164	Sim
preço	Sim
cadeia de caracteres	Sim
string_full_utf8	Sim
translated_html	Não
translated_text	Não
url	Não
user_image	Não
vídeo	Não
wiki_text	Não

Como fazer verificações com a configuração granular

É possível usar a verificação granular para analisar colunas específicas de tabelas para fins de descoberta. Os trabalhos tradicionais da Descoberta de dados verificam a tabela inteira para descobrir dados, enquanto a verificação granular direciona colunas específicas da tabela, o que oferece mais controle sobre o processo de descoberta

Antes de Iniciar

Função necessária: admin, sn_data_discovery_admin, data_privacy_admin

Procedimento

1. Navegue até **Todos** > **Segurança do sistema** > **Descoberta de dados (Clássica)** > **Configuração granular**.
2. Na lista **Configurações granulares**, selecione **Novo**.
3. No formulário **Configuração granular**, preencha os campos.

Campos da configuração granular

Campo	Descrição
Entrada do Dicionário	Coluna para verificação.
Tabela	Tabela para verificação.
Rótulo da coluna	Rótulo da coluna para verificação
Ponto de início da verificação	A descoberta de dados confidenciais ocorrerá somente para o dia de ponto de início da verificação e depois dele.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: Se você deixar o ponto de início da verificação em branco, todas as entradas da coluna serão verificadas. Se você mudar o ponto de início da verificação, a verificação será redefinida para iniciar a partir do carimbo de data/hora recém-configurado.
Ativo	Selecione para ativar a configuração granular.

4. Selecione **Enviar**.
   É possível selecionar tabelas secundárias das tabelas extensíveis para configuração.
5. Opcional: Selecione a Configuração granular da tabela primária e a opção **Selecionar tabelas secundárias** e indique as tabelas secundárias para verificação.

Resultados
Haverá a verificação da coluna específica da tabela de destino para fins de descoberta. A verificação granular usa Padrões de dados dos **Padrões de dados ativos**. É possível revisar os resultados e realizar ações sobre eles em **Todos** > **Segurança do sistema** > **Descoberta de dados(Clássica)** > **Resultados granulares**. Para obter mais informações, consulte Descobertas granulares.

Descobertas granulares

É possível revisar as descobertas granulares usando a ferramenta Descobertas granulares.

Revisão das descobertas granulares

Usam-se as **Descobertas granulares** para revisar até 500 descobertas de Configurações granulares. Quando há 500 descobertas, a verificação de configurações granulares será pausada até a realização da ação.

Rótulo da coluna	Descrição
Registro	Registro descoberto.
Tabela	Tabela primária do registro.
Coluna	Coluna do registro onde houve a descoberta de informações confidenciais.
Padrões de dados	Padrão usado para descobrir o registro.
Ação	Ação a ser tomada nas descobertas. Selecione para mudar **Importante:** A função data_privacy_admin é necessária para realizar a ação Anonimizar em um registro. Revisão

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Rótulo da coluna	Descrição
	O registro está com revisão pendente. Essa ação é designada a novas descobertas granulares. Ignorar Nenhuma ação será realizada no registro Anonimizar O registro será anonimizado.
Status	Status do registro. Novo Status atribuído à descoberta após a primeira comunicação dela Processado Quando se aplica a ação escolhida à descoberta com sucesso **Nota:** O armazenamento das descobertas processadas ocorre durante três dias na tabela "Descobertas granulares" antes da exclusão Revisão manual Quando há falha ao aplicar a ação que o usuário escolheu. **Aviso:** Na ação de "Revisão manual", depois de realizar as ações adequadas, os usuários devem excluir as descobertas.

Aviso: O rollback não é compatível com a anonimização acionada a partir de Descobertas granulares.

Data Classification

Agrupe dados por tipo, usando classificações de dados predefinidas ou definidas por usuário. Se você tiver uma função de auditor ou administrador de classificação de dados atribuída, será possível administrar diferentes classes de dados ou analisar visualmente o estado atual de diferentes tipos de dados na instância.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Explore a Classificação de dados Saiba mais sobre a Classificação de dados.	Configure a Classificação de dados Crie e configure suas próprias classes de dados.
Referência para Classificação de dados Saiba como a Classificação de dados funciona com dados de demonstração.	Analise Classificações de dados Saiba como analisar Classificações de dados.

Explorando a classificação de dados

Explore sobre a classificação de dados.

Data Classification habilita suporte para:

- Visibilidade nos tipos de dados hospedados em instâncias Now Platform.
- Conformidade com as leis de privacidade e cumprimento dos requisitos de regulamentação para indústrias como serviços financeiros e fabricação de dispositivos médicos.

Classificações de dados

A classificação de dados é um processo independente no qual você aplica manualmente as classificações de dados nas entradas de dicionário existentes em qualquer tabela. Consulte Tabelas Dicionário de dados para obter informações adicionais.

- Classifique os dados conforme achar apropriado para o seu negócio e poderá alterar as classes de dados disponíveis conforme necessário.
- Ao classificar dados, é possível usar as classificações de dados predefinidas ou criar suas próprias. Embora o uso de classificações de dados predefinidas seja opcional, é aconselhável fazê-lo como ponto de partida. Essas classificações de dados predefinidas são incluídas nos dados de demonstração que você pode instalar na instância. Para aprender mais, consulte Instalando dados de demonstração do plug-in Data Classification e Componentes instalados com os dados de demonstração de Data Classification.
- Se você criar suas próprias classificações de dados, também poderá projetar um sistema hierárquico em camadas com classificações de dados primários e secundários.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Painel Visão geral

Use o painel Visão geral para entender como suas tabelas de dados atuais são mapeadas para diferentes classificações de dados. Também é possível analisar como seus usuários globais, regionais e internacionais podem precisar de diferentes abordagens para classificação de dados, em relação ao uso ou acesso aos dados. Também é possível personalizar o layout e o conteúdo do painel Visão geral para atender às suas necessidades.

Para saber como usar as REST APIs e de script disponíveis para aplicar os metadados de classificação nos existentes processos, fluxos de trabalho e aplicações, consulte o seguinte:

- Classificação de dados - REST API
- DCManager - Global
- ScopedDCManager - Com escopo

Nota: Data Classification suporta a separação de domínio e a própria tabela data_classification tem processo separado.

Casos de uso

A GDPR (General Data Protection Regulation) é uma regulamentação da União Europeia cujo propósito é fornecer aos indivíduos controle sobre seus próprios dados pessoais. É possível usar classificações de dados, como informações de identificação pessoal, para identificar onde os dados pessoais estão sendo armazenados em sua instância. Ao aplicar os mecanismos de segurança apropriados para proteger esses dados pessoais contra vazamento, a sua organização satisfaz os requisitos da GDPR.

Se você armazenar as informações do cliente no Now Platform, use o código de classificação das informações de identificação pessoal (PII) onde for necessário para rastrear os dados sujeitos à regulamentação pelas leis de privacidade local. Ao instalar os dados de demonstração, eles aplicam automaticamente este código de classificação a certos campos sensíveis à segurança na tabela Usuário [sys_user]. Para saber mais, consulte:

- Componentes instalados com os dados de demonstração de Data Classification
- Atribuindo classificações de dados a entradas do dicionário

É possível aplicar uma classificação de dados Restritos a colunas da tabela de funcionários que armazenam informações confidenciais de funcionário como número do seguro social (SSN). Os administradores e auditores então podem usar o painel Visão geral para confirmar que você designou as classificações de dados atribuídos às colunas corretas. Eles também podem exibir detalhes de classificação para tipos restritos de informações.

Instalando dados de demonstração do plug-in Data Classification

Quando você faz upgrade ou instala Xanadu (e acima), o plug-in Data Classification (com.glide.data_classification) é ativado automaticamente. No entanto, você deve instalar manualmente os dados de demonstração que vêm com o plug-in. Isso inclui várias classificações de dados predefinidas importantes e também atribui uma delas a colunas da tabela usuário [sys_user] específicas em sua instância.

Antes de Iniciar
Função necessária: administrador

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

Independentemente de você instalar dados de demonstração, o plug-in Data Classification ativado adiciona as seguintes funções do usuário na instância:

- data_classification_admin: pode administrar todos os aspectos da aplicação Data Classification, incluindo a configuração de classificação de dados e atribuição.
- data_classification_auditor: pode auditar atribuições de código Data Classification feitas a tabelas e colunas de usuário.

Importante: Aviso sobre o uso por clientes:

Todas as decisões relacionadas à implementação desta aplicação são de responsabilidade exclusiva do cliente. Os clientes reconhecem e concordam que o uso da aplicação não é uma declaração pela ServiceNow de conformidade com qualquer lei ou regulamentação e que qualquer idioma, campo ou classificação sugerido fornecido pronto para uso com a aplicação não constitui aconselhamento jurídico da ServiceNow.

Os clientes permanecem os únicos responsáveis pelo cumprimento de suas obrigações jurídicas de acordo com a lei aplicável, incluindo (mas não se limitando a) proteção de dados, requisitos de segurança e leis de privacidade, além de serem responsáveis por configurar e fazer todas as modificações necessárias nesta aplicação, incluindo (mas não se limitando a) modelos para atender aos próprios requisitos.

Procedimento

1. Navegue até **Aplicações do Sistema** > **Todas as aplicações disponíveis** > **Todas**.
2. Encontre o plug-in Data Classification usando os critérios de filtro e a barra de pesquisa. Uma mensagem `Instalado` é exibida após a localização do plug-in.
3. Clique no ícone com três pontos verticais e selecione **Reparar** para acessar a caixa de diálogo Ativar plug-in.
4. Selecione **Carregar dados de demonstração**e clique em **Reparar**.

Componentes instalados com os dados de demonstração de Data Classification

Quando você instala os dados de demonstração inclusos no plug-in Data Classification (com.glide.data_classification), vários tipos de componentes são instalados na instância. Esses componentes incluem classificações de dados predefinidas e atribuições de código para colunas de usuário [sys_user} específicas.

Classificações de dados instaladas

classificação de dados	Descrição
Confidencial	Dados confidenciais que, se comprometidos, podem afetar negativamente as operações.
Interno	Dados internos não destinados à divulgação pública.
Informações de identificação pessoal	Também conhecidas como PII (Personally Identifiable Information, Informações de identificação pessoal). Dados que podem

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

classificação de dados	Descrição
	ser usados para identificar uma pessoa específica.
Público	Dados que podem ser divulgados gratuitamente ao público.
Restrito	Dados corporativos altamente confidenciais que, se comprometidos, podem colocar a organização em risco financeiro ou jurídico.

Atribuições de Data Classification

Tabela	Coluna atribuída	Classificação de dados atribuída
sys_user	zip	Informações de identificação pessoal
sys_user	first_name	Informações de identificação pessoal
sys_user	e-mail	Informações de identificação pessoal
sys_user	cidade	Informações de identificação pessoal
sys_user	middle_name	Informações de identificação pessoal
sys_user	rua	Informações de identificação pessoal
sys_user	mobile_phone	Informações de identificação pessoal
sys_user	last_name	Informações de identificação pessoal
sys_user	país	Informações de identificação pessoal
sys_user	gênero	Informações de identificação pessoal
sys_user	nome	Informações de identificação pessoal
sys_user	foto	Informações de identificação pessoal
sys_user	estado	Informações de identificação pessoal
sys_user	home_phone	Informações de identificação pessoal

Criando classificações de dados

Crie suas próprias classificações de dados definidas pelo usuário na tabela Data Classification [data_classification] que você pode atribuir a colunas específicas em tabelas específicas.

Antes de Iniciar

Função necessária: data_classification_admin, administrador

Procedimento

1. Navegue até **Todos** > **Segurança do sistema** > **Classificação de dados** > **Classes de dados**.
2. Selecione **Novo**.
3. Preencha os campos no formulário.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Nome da classificação	Nome da classificação de dados.
Descrição	Descrição da classificação de dados.
Primária	Nome da classificação de dados primária à qual esta classificação de dados está subordinada. Deixe o campo em branco se estas classificações de dados não forem classificações de dados primária para secundária.
Aplicação	Escopo da aplicação para esta classificação de dados.

4. Se esta classificação de dados for uma classificação de dados primária para secundária, clique em **Novo**.
   Se você não quiser criar classificações de dados secundárias, ignore esta etapa.
5. Preencha os campos no formulário.

Título

Campo	Descrição
Nome da classificação	Nome da classificação de dados secundária.
Descrição	Descrição da classificação de dados secundária.
Primária	Nome da classificação de dados primária à qual esta classificação de dados está subordinada. Deixe o campo em branco se estas classificações de dados não forem classificações de dados primária para secundária.
Aplicação	Escopo da aplicação para esta classificação de dados secundária.

6. Clique em **Enviar**.

Atribuindo classificações de dados a entradas do dicionário

Atribua classificações de dados a colunas de tabela específicas na tabela Dicionário [sys_dictionary]. Quando você atribui classificações de dados, ele cria entradas na tabela Dicionário-Classe de Dados [m2m_dictionary_dataclass], que você pode revisar no painel Visão geral.

Antes de Iniciar

Função necessária: data_classification_admin e administrador

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. No painel Navegador, digite `sys_dictionary.list`.
2. Em Entradas de dicionário, selecione cada um dos elementos aos quais você deseja atribuir classificações de dados específicas.
3. Depois de selecionar os elementos, clique **em Ações nas linhas selecionadas**e selecione **Classificar**.

   Nota: Para limpar classificações de dados atribuídas anteriormente para elementos de dicionário selecionados, você pode selecionar **Limpar classificação**.

4. Quando a caixa de diálogo Atribuir à classe de dados for exibida, selecione as classificações de dados que você deseja atribuir aos elementos de dicionário selecionados e clique em **Classificar**.

   Aviso: Isso substituirá qualquer classificação existente para os itens de dicionário selecionados.

   Você pode selecionar várias classificações de dados conforme necessário.

   Consulte Tabelas Dicionário de dados para obter informações adicionais.

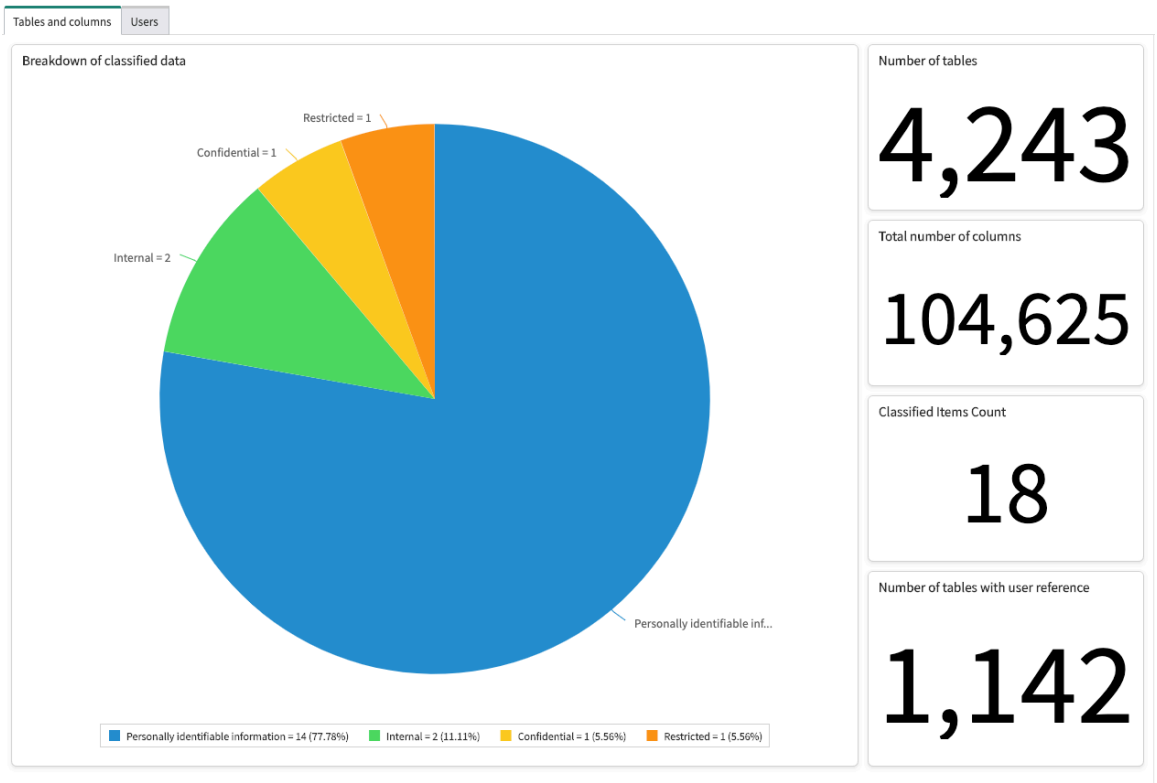
Análise das classificações de dados usando o painel de Visão geral

O painel Visão geral relata o estado atual das classificações de dados na sua instância e como os usuários são distribuídos por local.

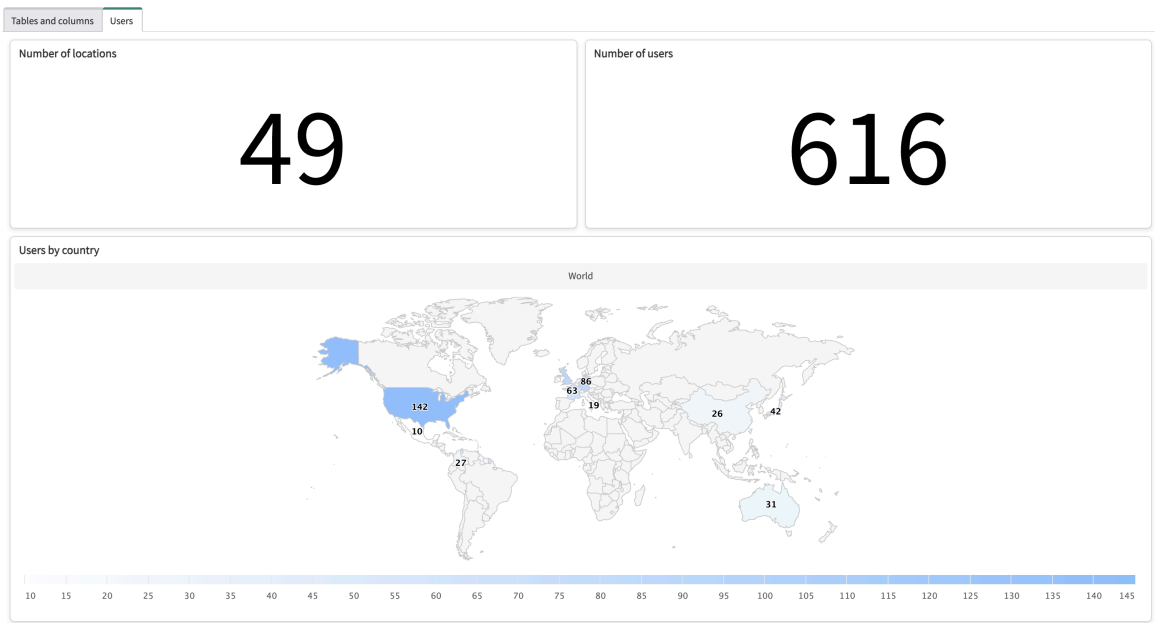
Se você tiver uma função de administrador ou auditor de classificação de dados, poderá visualizar a confidencialidade atual dos dados da instância, o que ajuda a aumentar a segurança e a conformidade com as leis de privacidade. Usando o campo Local em registros de usuário, os administradores mapeiam usuários em diferentes regiões que têm diferentes regulamentações de privacidade.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia Tabelas e colunas



Guia Usuários



Funções necessárias de Now Platform

- data_classification_admin: administra todos os aspectos da aplicação Data Classification, incluindo a configuração de classificação de dados e atribuição.
- data_classification_auditor: audita atribuições de código Data Classification

Casos de uso

Para obter mais exemplos de como as pessoas de sua empresa podem usar esse painel, consulte Casos de uso em Data Classification.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Usuário	Uso do painel
data_classification_admin	Certifique-se de ter atribuído classificações de dados aos campos corretos na instância.
data_classification_auditor	Audite a senilidade e a segurança dos dados na instância.

Relatórios

Título	Tipo	Tabela de origem	Descrição
Detalhamento de dados classificados	Gráfico de donut	m2m_dictionary_data_class	Apresenta um detalhamento das classificações de dados da instância por classe de dados e exibe o total no centro.
Total de tabelas	Pontuação única	sys_dictionary	Número total de tabelas de dados em todo o dicionário.
Colunas Total	Pontuação única	sys_dictionary	Número total de colunas de dados classificados em todo o dicionário.
Colunas de referência a usuário	Pontuação única	sys_dictionary	Número total de colunas de referência a usuário no dicionário.
Número de localizações de usuário	Pontuação única	sys_user	Número total de locais distintos encontrados para os usuários
Contagem de usuários	Pontuação única	sys_user	Número total de registros de usuário na sua instância.
Usuários por país	Mapa	sys_user	Detalhamento dos registros de usuário por país.

Domain Separation e Data Classification

A separação de domínio é compatível com o Data Classification . O Domain Separation permite separar dados, processos e tarefas administrativas em agrupamentos lógicos chamados de domínios. Você pode controlar vários aspectos dessa separação, incluindo quais usuários podem ver e acessar os dados.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nível de suporte: Aprimorado

- Inclui os níveis **Básico** e **Padrão**.
- O processo orientado por dados permite que os clientes do provedor de serviços modifiquem a lógica de negócios baseada em casos de uso definidos. Essas configurações são baseadas em IU e à prova de falhas para que as configurações de um cliente não possam afetar outro.
- Os locatários da instância devem ser capazes de configurar por conta própria a lógica de negócios do produto minimamente viável (MVP) e os parâmetros de dados. Essa lógica e os parâmetros seriam esperados para a função normal do aplicativo.

Exemplo de caso de uso: os clientes locatários de um ambiente compartilhado devem ser capazes de modificar o impacto, a urgência ou a matriz de prioridade para definir a prioridade em seu domínio.

Para obter mais informações sobre os níveis de suporte, consulte Suporte de aplicação para separação de domínio.

Como o Domain Separation funciona no Data Classification

Para o Domain Separation, a aplicação usa separação de processo para a tabela Data Classification [sys_data_classification]. Para a tabela Dicionário-Classe de dados [m2m_dictionary_dataclass], ele usa separação de dados. Para saber mais sobre separação de dados e processos, consulte Domain Separation explicado.

Informações relacionadas

Domain Separation para provedores de serviço

Anonimização de dados

A anonimização fornece uma maneira de transformar facilmente os dados para que eles não sejam identificáveis e estejam mais em conformidade com as regulamentações da privacidade de dados.

Os administradores podem executar o processo de anonimização em instâncias de produção e não produção. A privacidade de dados pode ser usado em instâncias de produção para desidentificar usuários. A anonimização de classes de dados só deve ser usada com instâncias de não produção. Esta preservação assegura que os dados como endereços de e-mail ou endereços físicos sejam substituídos por versões formadas de forma semelhante, mas anonimizadas.

Os administradores também podem usar a anonimização como parte dos processos de regulamento de proteção geral de dados (GDPR, General data protection regulation) Direito a ser esquecido (RTBF, Right to be forgotten) para tornar as informações do usuário anônimas. Consulte https://gdpr-info.eu/art-17-gdpr/ para obter mais informações.

Use a seção de anonimização da privacidade de dados para criar e exibir políticas e técnicas de privacidade e para executar a atribuição de privacidade em massa. Exiba todos os trabalhos, com a descrição, a política privada usada e o status. Para acessar a seção de anonimização, um administrador deve primeiro elevar para as funções data_privacy_admin e data_privacy_processor.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Técnicas de anonimização

Técnicas de anonimização são opções que você seleciona para determinar como os dados se tornam anônimos. Você deve criar uma técnica de anonimização para fazer referência no trabalho de anonimização. Consulte Criação de técnicas de anonimização para associar uma técnica de privacidade a uma **configuração de técnica de anonimização associada**.

Políticas de anonimização

Configure uma política de anonimização para especificar quais técnicas de privacidade de dados são usadas ao tornar seus dados anônimos. Consulte Criação de políticas de anonimização para obter detalhes.

Trabalhos de anonimização

Os trabalhos de anonimização usam todos esses componentes para tornar seus dados anônimos. Para obter mais informações sobre esses trabalhos, consulte Criação de trabalho de anonimização.

Criação de técnicas de anonimização

Crie uma configuração de técnica de privacidade de dados para personalizar como ele anonimiza seus dados.

Antes de Iniciar

Função necessária: data_privacy_admin e administrador

Procedimento

1. Eleve para a função **data_privacy_admin**.
   Para obter detalhes sobre a elevação de função, consulte Elevar para uma função privilegiada.
2. Navegue até **Segurança do sistema** > **Privacidade de dados** > **Anonimização**.
3. Selecione **Exibir técnicas**.
   Existem várias técnicas predefinidas disponíveis para seleção.

Técnica	Descrição
Substituição seletiva	Esta técnica faz uma substituição seletiva de dados de cadeia de caracteres. Todos os caracteres entre os índices inicial e final da entrada são substituídos pelo caractere escolhido. Você pode especificar caracteres a serem excluídos do mascaramento: ◦ start_index: a técnica mascara os dados que começam no caractere especificado. Se deixado em branco, o mascaramento começará com o primeiro caractere. ◦ end_index: a técnica mascara os dados desde o início da cadeia de caracteres até o caractere especificado. Se deixado em branco, o mascaramento terminará com o último caractere. ◦ exclude_char: define um caractere a ser excluído do mascaramento. ◦ replacement_char: define um caractere usado para mascaramento. Se nenhum for fornecido, serão usados asteriscos (*) por padrão.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Técnica	Descrição
Substituição estática	Esta técnica troca valores por valores estáticos. Dados de Cadeia de caracteres, Número e Data podem usar esta técnica: ◦ date_time_value: substitui os valores de data por esta data. Use o formato aaaa-MM-dd HH:mm:ss. ◦ date_value: substitui os valores de data por esta data. Use o formato aaaa-MM-dd. ◦ number_value: substitui os valores de número por este número. ◦ string_value: substitui os valores de cadeia de caracteres por este texto. ◦ number_type: aceita um número inteiro
Substituição aleatória	Esta técnica troca valores por valores gerados aleatoriamente. Dados de cadeia de caracteres e números podem usar esta técnica.
Remover	Esta técnica remove valores, substituindo-os por valores vazios (nulos).
Nenhuma ação	Esta técnica é um espaço reservado. Ela não modifica os campos quando selecionada.
Substituição seletiva com X	Transforma dados da cadeia de caracteres e substitui seletivamente caracteres confidenciais pela letra X. **Nota:** Técnica padrão para padrões de dados em Como explorar o Descoberta de dados.
Anonimização de padrão de dados	Somente anonimiza os padrões de dados descobertos em campos de dados não estruturados, mantendo o contexto subjacente intacto. **Nota:** As configurações desta técnica fazem referência às configurações da técnica de anonimização do padrão de dados em Como explorar o Descoberta de dados.

4. Selecione **Adicionar técnica personalizada** se não estiver usando uma técnica predefinida.
5. Preencha os campos no formulário **Personalizar técnica**.

Campo1	Descrição
Técnica de base	Selecione uma técnica predefinida, já que as técnicas personalizadas são baseadas nas técnicas predefinidas.
Nome da técnica	Insira um nome para a técnica.
Descrição da técnica	Insira uma descrição para a técnica.

6. Selecione **Avançar**.
7. Insira os parâmetros da técnica.
   Os valores com parâmetros disponíveis dependem de qual técnica de privacidade você selecionou. Não há valores com parâmetros para as técnicas **Nenhuma ação** e **Remover**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Valores parametrizados de privacidade para as técnicas de base

Técnica de base	Valor do parâmetro de técnica de privacidade	Descrição	Valor-padrão
Substituição seletiva	end_index	A técnica mascara os dados desde o início da cadeia de caracteres até o caractere especificado. Se deixado vazio, o mascaramento terminará com o último caractere.	(Vazio)
Substituição seletiva	exclude_char	Caractere para ignorar o mascaramento. Somente um único caractere pode ser usado neste valor. Se mais de um for inserido, o primeiro caractere será usado.	(Vazio)
Substituição seletiva	replacement_char	Caractere a ser usado ao substituir valores usando uma substituição seletiva.	Um asterisco (*****) será usado se nenhum outro valor for inserido.
Substituição seletiva	start_index	A técnica mascara os dados que começam no caractere especificado.	Se deixado em branco, o mascaramento começará no primeiro caractere.
Substituição estática	date_time_value	Substitui os valores de data e hora por esta data. Use o formato aaaa-MM-dd HH:mm:ss.	1988-11-11 10:10:10
Substituição estática	date_value	Substitui os valores de data por esta data. Use o formato aaaa-MM-dd.	1988-11-11
Substituição estática	number_value	Substitua os valores de Número por este número.	1234567
Substituição estática	string_value	Substitua os Valores de cadeia de caracteres por este texto.	TEXT123

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Técnica de base	Valor do parâmetro de técnica de privacidade	Descrição	Valor-padrão
Substituição aleatória	preserve_data_length	Defina como **verdadeiro** para preservar o tamanho dos dados. Os dados desidentificados terão o mesmo comprimento que os dados originais.	Verdadeiro

8. Selecione **Criar técnica personalizada**.
   Sua técnica personalizada é adicionada às técnicas de Anonimização.

O que Fazer Depois

Consulte Criação de políticas de anonimização para configurar uma política de anonimização para especificar quais técnicas são usadas para anonimizar seus dados.

Criação de políticas de anonimização

Configure uma política de anonimização para especificar quais técnicas são usadas ao tornar seus dados anônimos.

Antes de Iniciar

A configuração da Privacidade de dados define tabelas, sys_user e outros, além de colunas para o desidentificado dependendo do caso de uso e especifica tipos parametrizados das técnicas a serem usadas durante a desidentificação de dados.

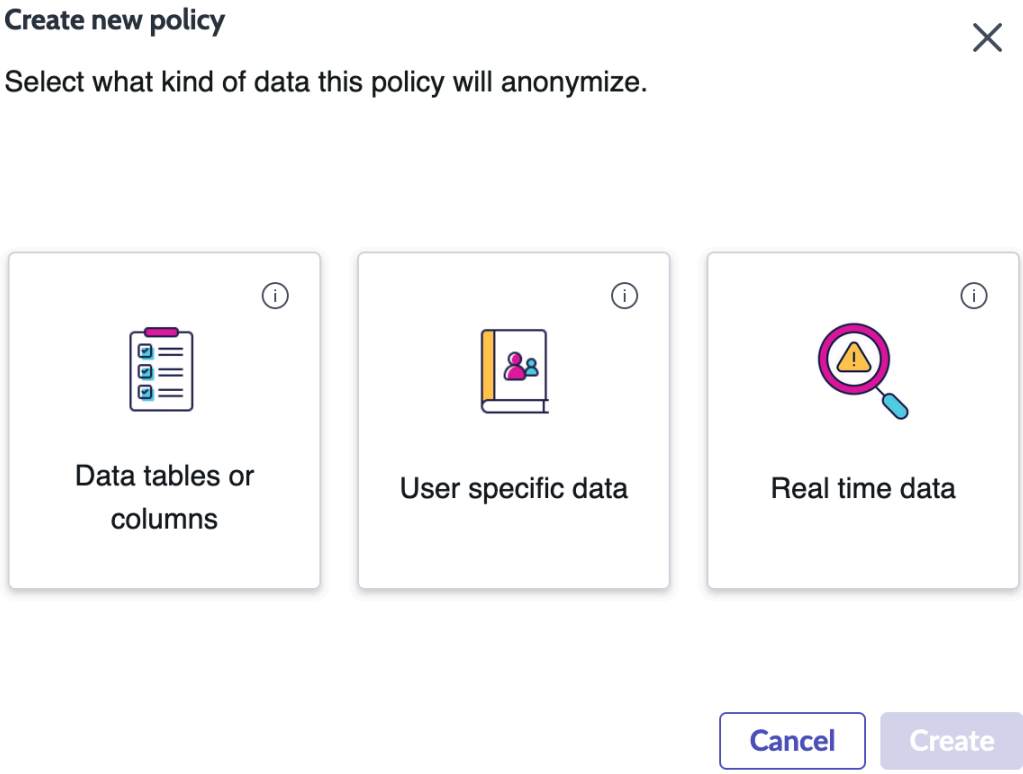
> **Nota:** Para concluir uma configuração de privacidade, você deve primeiro configurar uma configuração de técnica da Privacidade de dados. Para obter mais informações, consulte Criação de técnicas de anonimização.

Função necessária: data_privacy_admin e administrador

Procedimento

1. Eleve para a função **data_privacy_admin**.
   Para obter detalhes sobre a elevação de função, consulte Elevar para uma função privilegiada.
2. Navegue até **Segurança do sistema** > **Privacidade de Dados** > **Anonimização**.
   Todas as políticas de anonimização são exibidas. As políticas publicadas estão disponíveis para programar o trabalho de anonimização.
3. Selecione **Criar nova política**.
4. Selecione para tornar anônimas **Tabelas ou colunas de dados**, **Dados específicos do usuário** ou **Dados em tempo real**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Tipo de Dados	Descrição
Tabelas ou colunas de dados	Os registros que corresponderem à política de dados serão anonimizados.
Dados específicos do usuário	Selecione um conjunto de usuários ou grupos de usuários para anonimização.
Dados em tempo real	Anonimize entradas em tempo real de um conjunto de colunas.

As políticas da privacidade de dados só podem ser aplicadas a dados classificados. Para obter mais informações sobre classificação de dados, consulte Classificação de dados.

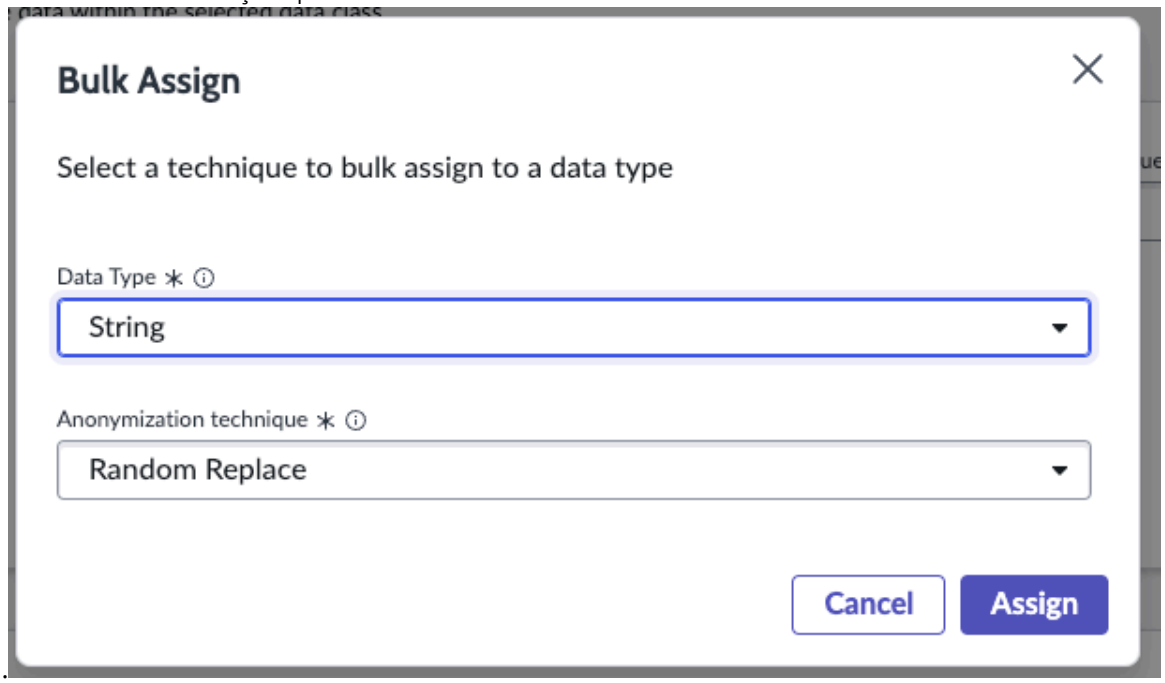
5. Selecione **Criar**.
   Há etapas sequenciais necessárias para concluir a política, **Definir detalhes** e **Atribuir técnicas**. **Selecionar referência de usuário** também é necessário ao definir a política para dados específicos do usuário.
6. Defina os detalhes da nova política de anonimização.
   - Insira o nome da política no campo **Nome** e a descrição da política no campo **Descrição**.
   - No campo **Classe de dados**, selecione a classe de dados a ser usada com esta política.

   Nota: Se você não estiver anonimizando uma entrada, selecione a técnica **Não fazer nada** em vez de deixar a entrada em branco. Políticas com valores em branco no campo Configuração da técnica de privacidade não podem ser executadas quando usadas em trabalhos da privacidade de dados.

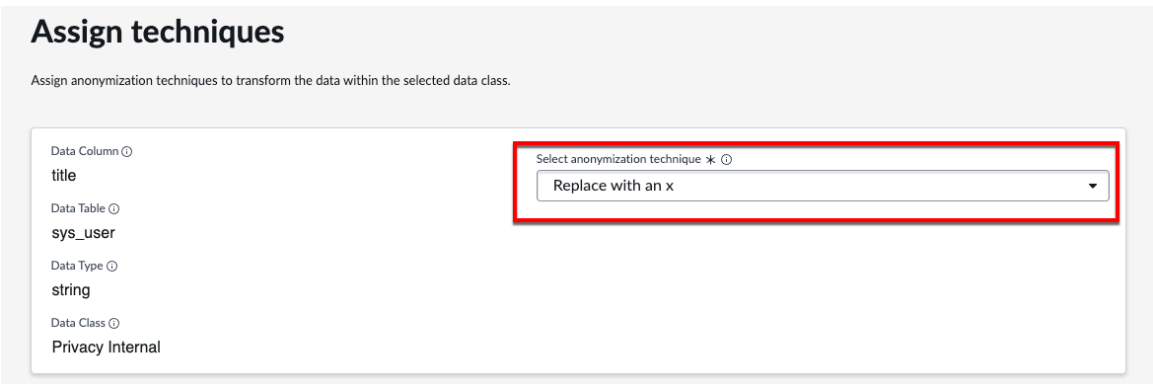
   Depois de selecionar uma classe de dados, o Formulário de técnicas de atribuição é exibido para cada registro retornado para a classe de dados definida.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

7. Atribua técnicas de anonimização para a classe de dados selecionada.



Opção	Descrição
Selecionar **Técnicas de atribuição em massa**	Aplica anonimização a todos os registros de dados na classe de dados escolhida. Selecione o tipo de dados e a técnica de anonimização para aplicar a todas as entradas com o tipo de dados selecionado. Repita esta etapa para atribuições em massa adicionais de diferentes tipos de dados. Consulte Tipos de campos compatíveis para anonimização para obter uma lista de tipos de dados.
Selecionar uma **técnica de anonimização** para cada registro de coluna de dados	Os usuários do processador da privacidade de dados poderão escolher quais registros serão anônimos ao criar trabalhos de privacidade de dados. Aplique anonimização de forma individual a todos os registros de dados na classe de dados escolhida.



© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

8. Opcional: Insira as tabelas secundárias para verificação.
   As tabelas secundárias da tabela primária serão anonimizadas. Se uma tabela não tiver secundárias, essa opção não estará disponível.

   Aviso: Um trabalho primário apresentará falha se um trabalho secundário apresentar falha.

9. Opcional: Se a Anonimização de padrão de dados estiver selecionada, selecione a técnica de anonimização a ser usada.
10. Opcional: Defina a ordem dos padrões de dados.
11. Opcional:

    Dica: Use o recurso de **teste** para testar entradas de amostra. É possível revisar as métricas do resultado, como tempo de verificação, resultado e padrões descobertos.

    Clique no botão **Testar** para testar a política.

12. **Importante:** Todas as tabelas devem ter uma entrada sys_dictionary correta.

    Selecione **Salvar**.
13. Selecione **Publicar** para atualizar a política de anonimato para programação e retornar às Políticas de anonimização.

    Nota: Somente políticas publicadas podem ser usadas para programação de trabalho de anonimização.

O que Fazer Depois

Criação de trabalho de anonimização.

Configuração de solicitação de clone de anonimização de dados

A integração do clone da privacidade de dados é configurada usando um script PostClone para criar e executar trabalhos da privacidade de dados para políticas configuradas no destino. Depois de executar o script, os usuários verão os dados não identificados e não terão acesso aos dados originais.

Antes de Iniciar

O script PostClone da privacidade de dados é instalado com a ativação do plug-in de privacidade de dados (com.glide.data_privacy). Consulte Ativação da privacidade de dados para obter detalhes.

Função necessária: data_privacy_clone_processor, data_privacy_admin e administrador

Procedimento

1. Ative o plug-in de privacidade de dados (com.glide.data_privacy) na instância de origem.
   O script PostClone da privacidade de dados está instalado.
2. Eleve para a função **data_privacy_admin**.
   Para obter detalhes sobre a elevação de função, consulte Elevar para uma função privilegiada.
3. Navegue até **Segurança do sistema** > **Privacidade de Dados** > **Anonimização**.
4. Selecione **Criar nova política**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Consulte Criação de políticas de anonimização para obter detalhes.

5. Selecione **Tabelas ou colunas de dados**.
6. Selecione **Criar**.
7. Insira um nome e selecione uma classe de dados.
8. Selecione para **Ativar a política durante a clonagem**.
9. Selecione a ordem da política a ser executada se houver várias políticas de clone.
   Um trabalho da privacidade de dados para Configuração PostClone com um Pedido de aplicação superior poderá iniciar antes de outro trabalho de ordem inferior se o trabalho com o pedido superior não envolver qualquer tabela relacionada a outro trabalho de pedido inferior.
10. Selecione **Continuar**.
11. Conclua a configuração da política e publique a política.
12. Faça back-up das configurações da privacidade de dados.
13. Programe o trabalho de anonimização.
    Consulte Criação de trabalho de anonimização para obter detalhes.
14. Como administrador da privacidade de dados, envie uma solicitação de clone.

Resultados

O script PostClone da privacidade de dados é executado na instância de destino e o script PostClone cria um registro de trabalho federado da privacidade de dados na instância de destino. O trabalho federado cria e executa um trabalho da privacidade de dados para cada política pós-clonagem, na Ordem da aplicação, na instância de destino.A origem do backup é clonada para a instância de destino. O script PostClone da privacidade de dados cria e executa trabalhos da privacidade de dados para políticas configuradas na instância de destino.

O processador de clone da privacidade de dados elevado pode fazer logon na instância de destino e monitorar o estado do trabalho federado de pós-clonagem em dp_federated_job.list e dp_job.list.

Criação de trabalho de anonimização

Configure um trabalho da privacidade de dados na instância de produção para usar dados anonimizados na instância de não produção para trabalhos de classe de dados e de usuário.

Antes de Iniciar

O trabalho da privacidade de dados é compatível com dois casos de uso de desidentificação:

- Dados confidenciais de sys_users específicos
- Dados confidenciais de uma classe de dados específica.

Função necessária: data_privacy_processor e administrador

Procedimento

1. Eleve para a função **data_privacy_processor**.
   Para obter detalhes sobre a elevação de função, consulte Elevar para uma função privilegiada.
2. Navegue até **Segurança do sistema** > **Privacidade de Dados** > **Anonimização**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Em uma política de anonimização, selecione **Programar trabalho** para a política a ser usada no trabalho.
   Uma política deve estar em um estado publicado para programar um trabalho de anonimização

> ⚠ **Aviso:** Trabalhos de anonimização são altamente destrutivos e só podem ser revertidos em rollback. Verifique novamente todas as informações, como registros e tabelas processadas, antes de programar um trabalho.

4. No formulário, preencha os campos.

Campos de Trabalho da privacidade de dados

Campo	Descrição
Política usada	Nome somente leitura da configuração de política de privacidade selecionada a ser usada para este trabalho. Edite a política para visualizar informações adicionais sobre a política. Para obter detalhes sobre as configurações de política de privacidade, consulte Criação de políticas de anonimização.
Descrição da vaga	Descrição do trabalho.
Hora de início	O início do tempo para executar este trabalho em **HH:MM:SS**.
Hora de término	O fim da janela de tempo para executar este trabalho em **HH:MM:SS**. A hora de término deve ser posterior à hora de início. O trabalho é executado antes da hora inserida neste campo. Se o trabalho ainda não tiver sido concluído, ele será pausado e retomado no próximo início da janela de tempo.
Simulação	Execute o trabalho como um teste. Nenhum registro é afetado ao executar este trabalho. Os resultados são exibidos na lista **Trabalhos** como se o trabalho tivesse sido executado. **Nota:** A **simulação** deve ser desativada ao configurar um trabalho da privacidade de dados com reversão. Consulte Rollback de trabalho da Privacidade de dados para obter detalhes.
Tipo de seleção do usuário	Selecione usuários ou grupos para anonimização.
Selecionar usuários/grupos	Selecione um conjunto específico de usuários ou grupos para anonimização

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

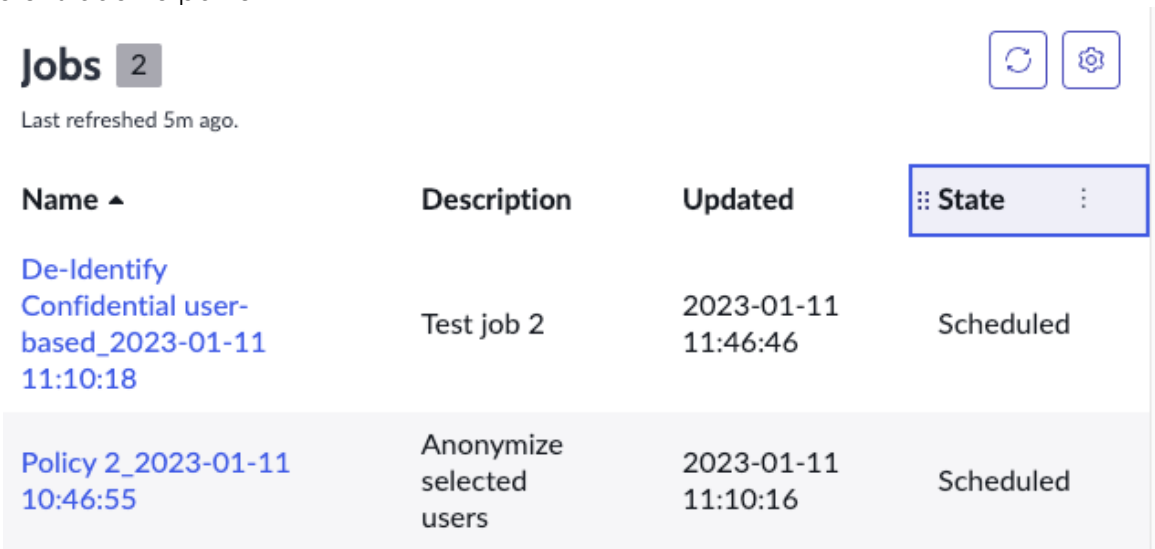
Campo	Descrição
	nesse trabalho. Dá suporte a até 1.000 usuários. **Nota:** Este campo obrigatório é exibido somente quando a condição de política de privacidade selecionada requer uma seleção de registros do usuário.

5. **Importante:** Todas as tabelas devem ter uma entrada sys_dictionary correta antes da programação e durante o trabalho.

Selecione **Programar trabalho** no formulário para colocar a anonimização na fila de trabalhos.
O trabalho é executado entre as horas selecionadas nos campos **Hora de início** e **Hora de término**. Se o trabalho não tiver sido concluído durante a janela de tempo de início e término, o trabalho continuará no próximo início da janela de tempo.

Nota: Um trabalho só poderá ser executado uma vez, mesmo se a **Simulação** estiver selecionada. Para executar um trabalho novamente com base na mesma política, selecione **Programar trabalho** e preencha o formulário usando os mesmos valores de campos.

O trabalho é listado no painel



Trabalhos.

Campo	Descrição
Nome	Nome do trabalho de anonimização.
Descrição	Descrição do trabalho de anonimização.
Atualizado	A data e a hora em que o trabalho foi atualizado pela última vez.
Estado	Estado do trabalho da privacidade de dados:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	◦ **Programado**: estado-padrão para novos trabalhos. ◦ **Concluído**: o trabalho tornou os dados selecionados anônimos com sucesso. ◦ **Cancelado**: o trabalho foi cancelado manualmente. ◦ **Erro**: houve um problema ao salvar o trabalho. Reprogramar o trabalho ou criar um novo trabalho. Pode haver problemas com a configuração se o erro continuar. ◦ **Rollback em andamento**: o trabalho foi definido para reverter a anonimização. ◦ **Rollback concluído**: o rollback do trabalho de anonimização foi concluído com sucesso. Um campo somente leitura.

6. Selecione um trabalho no painel **Trabalhos** para abrir o resumo do trabalho.
Depois que um trabalho é programado, os botões **Cancelar trabalho** e **Pausar** aparecem no resumo do trabalho.

Campos adicionais para trabalhos agendados

Campo	Descrição
Contagem de registro estimada	O número estimado de registros que este trabalho de simulação afeta antes de ser executada. Um campo somente leitura
Total de registros de dados processados	O número total de registros de dados individuais afetados por este trabalho. Um campo somente leitura.
Total de tabelas de dados processadas	O número total de tabelas de dados processadas por este trabalho. Um campo somente leitura.
Tempo restante para o rollback	O tempo restante que um trabalho de anonimização de dados concluído pode ser revertido e desanonimizar os dados. Um campo somente leitura.
Total de usuários processados	O número total de registros de usuário individuais afetados por este trabalho. Um campo somente leitura.
Cancelar trabalho	Selecione para cancelar o trabalho de anonimização. Isso deve ser selecionado antes da hora de início do trabalho. Quando selecionado, o status do trabalho é atualizado para *Cancelado*.
Pausa	Selecione para pausar o trabalho e a gravação de rollback, se o rollback tiver sido selecionado. Uma mensagem de aviso será exibida após um período de expiração de três dias para contextos de rollback. Isso deve ser selecionado após a hora de início do trabalho e antes da hora de término do trabalho.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Quando selecionado, o status do trabalho é atualizado para *Pausado*.
Retomar	Reinicia um trabalho pausado. O rollback não é compatível com trabalhos retomados se pausados. Cancele o trabalho e crie um trabalho da privacidade de dados. A gravação usa um contexto de rollback não expirado. Quando selecionado, o status do trabalho é atualizado para *Programado*.
Exportar	Baixa um arquivo .PDF dos detalhes do trabalho da privacidade de dados.

Como ativar trabalhos paralelos para anonimização de dados

Use trabalhos paralelos para reduzir o tempo de execução dos trabalhos de anonimização.

Antes de Iniciar

Função necessária: administrador

Procedimento

Por padrão, os trabalhos de anonimização baseados em classes de dados e usuários são executados usando uma só thread. É possível ativar várias threads para trabalhos baseados em classes de dados e usuários. Além disso, por padrão, os trabalhos federados usados durante a clonagem usam trabalhos paralelos com três processos de execução.

1. No filtro de navegação, digite `sys_properties.list`.
2. Crie a propriedade `com.glide.data_privacy.max_parallel_workers`
3. Opcional: Para ajustar o número de processos de execução paralelos dos trabalhos federados, edite a propriedade `dp.max_concurrent_clone_item_workers`.
4. Verifique se o **Tipo** é `inteiro`.
5. **Importante:** É recomendável iniciar com um pequeno número de processos de execução por nó (dois ou três).

   No campo **Valor**, insira um número máximo de cinco para os processos de execução dos trabalhos paralelos.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Criptografia

Proteja seus dados confidenciais e mantenha a conformidade com os requisitos e padrões regulatórios.

Estrutura de gestão de chaves

Use a

Estrutura de gestão principal

(Key Management Framework, Estrutura de gestão de chaves) para personalizar e gerenciar totalmente a forma de realizar operações criptográficas em sua instância da .

Certificados

Use certificados para estabelecer conexões seguras e validar assinaturas.

Criptografia em nível de coluna

Use a CLE para permitir e recusar o acesso a dados criptografados com base na função do usuário. Ela inclui gestão básica de chaves usando módulos de criptografia.

Criptografia em nível de coluna para empresas

Use a CLE para permitir e recusar o acesso a dados criptografados com base na função do usuário. Ela inclui gestão básica de chaves usando módulos de criptografia.

Criptografia da nuvem

Criptografe o banco de dados da instância usando criptografia de bloco e gestão aprimorada de chaves.

Pacote de direitos da Criptografia da plataforma

Faça upgrade para o uso ilimitado do Criptografia em nível de coluna para empresas, Criptografia da nuvem e Criptografia de banco de dados.

Criptografia de disco completo (FDE)

A criptografia de disco completo aplica criptografia a todo o sistema de armazenamento, somente dentro do servidor de banco de dados. Porque este

Edge Encryption

Criptografa dados confidenciais nas instalações da empresa antes de enviar dados pela Internet para sua instância da ServiceNow. Os dados

Criptografia de banco de dados

Criptografe todos os dados armazenados em tempo real, protegendo dados on-line e off-line sem perda de funcionalidade.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

é o único componente de armazenamento de dados do cliente.	permanecem criptografados em repouso na instância.	

Estrutura de gestão de chaves

Criptografia é um procedimento criptográfico que converte texto sem formatação em texto cifrado para controlar a divulgação de informações.

Visão geral

O gerenciamento de chaves do ServiceNow inclui as atividades que envolvem o manuseio de chaves criptográficas e parâmetros de segurança relacionados durante o ciclo de vida de chave de ponta a ponta e é um controle eficaz baseado nas diretrizes do Instituto Nacional de Padrões e Tecnologia (NIST) 800-57.

A criptografia é usada para converter cadeias de caracteres de texto sem formatação em texto cifrado, que permanece indecifrável sem acesso à chave correta. Os benefícios de segurança da criptografia são derivados da combinação de algoritmos fortes e um gerenciamento de chaves de qualidade.

Criptografar todas as informações pode não ser necessário para todos os dados e aumentaria muito o tempo de processamento devido ao grande número de dados com suporte em todos as aplicações. Quando você determina que a criptografia é necessária para os dados, estas opções Now Platform estão disponíveis:

Iniciar

Noções básicas sobre a KMF (Key Management Framework, Estrutura de gestão de chaves)	**Noções básicas sobre KMF**	**Ações de gestão de chaves**
	A API/UX (KMF) permite que você personalize e gerencie totalmente como as operações criptográficas serão realizadas na instância .	Exibir, gerenciar e fazer rodízio de chaves criptográficas

Informações de ativação

O pacote de assinatura da ServiceNow Criptografia da plataforma é um direito comercial de grupo que inclui Criptografia em nível de coluna para empresas, Criptografia da nuvem e o Database Encryption.

Criptografia em nível de coluna para empresas é a licença ilimitada de Criptografia em nível de coluna. O plug-in Criptografia em nível de coluna Enterprise está disponível com a ativação do plug-in com.glide.now.platform.encryption. Para obter detalhes, consulte Pacote de assinatura do Gerenciamento de criptografia e chaves.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Pacote de assinatura do Gerenciamento de criptografia e chaves

Com o gerenciamento de chaves, a Criptografia em nível de coluna é atualizada sem custo adicional para os módulos de criptografia altamente configuráveis. Você também tem a opção de fazer upgrade para a licença de uso ilimitado. Assine o novo pacote de direitos de criptografia, Criptografia da plataforma, que inclui Criptografia da nuvem e Criptografia em nível de coluna para empresas.

Recursos da Criptografia em nível de coluna

A Criptografia em nível de coluna com módulos de criptografia está incluída gratuitamente na instância e inclui gerenciamento de chaves NIST 800-57 com o seguinte suporte:

- chaves gerenciadas por ServiceNow são compatíveis (chaves fornecidas pelo cliente não são compatíveis).
- O acesso aos módulos de criptografia é baseado somente em função.
- Rotação manual ilimitada de chaves.
- Pode haver no máximo cinco módulos de criptografia em um determinado momento.
- Pode haver no máximo cinco políticas de acesso de módulo em um determinado momento.
- Tipos de campo existentes compatíveis. (Novos tipos de campo criados em versões posteriores não serão compatíveis com a versão não corporativa)
- A API compatível pode ser utilizada com base no acesso à função.
- Auditoria de ações de criptografia.
- Tour guiado da Criptografia em nível de coluna.

ServiceNow Recursos do grupo de Criptografia da plataforma

O grupo Criptografia da plataforma adiciona os seguintes recursos e ofertas:

- Criptografia em nível de coluna para empresas:
  - Chaves fornecidas pelo cliente.
  - Rotação automática de chave.
  - Suporte de tipo de campo avançado e atualizações futuras.

    Nota: O suporte ao tipo de campo expandido inclui os tipos de campo **Registro**, **Lista de registros**, **Entrada de registro** e **HTML e Traduzido (Campo /Texto /HTML)**.

  - Suporte avançado a anexos.
  - O acesso ao módulo de criptografia pode ser concedido com uma política de acesso ao módulo com base no seguinte:
    - Usuário do sistema
    - Script
    - Escopos de aplicação específicos
  - Módulos de criptografia ilimitados e políticas de acesso ao módulo.
  - Importação de uma chave do serviço web.
  - Defina a data de rotação futura para chaves de criptografia.
- Criptografia da nuvem com gerenciamento de chave.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Informações adicionais

Para saber mais sobre gerenciamento de chaves, consulte Noções básicas sobre a estrutura de gerenciamento de chaves.

Noções básicas sobre a estrutura de gerenciamento de chaves

A API/UX Estrutura de gestão principal (KMF) permite que você personalize e gerencie totalmente como as operações criptográficas serão realizadas na instância ServiceNow. A ServiceNow Estrutura de gestão principal fornece uma interface segura e abrangente para serviços de gerenciamento de chaves criptográficas do lado da instância.

De acordo com as diretrizes do NIST 800-57, a KMF fornece os seguintes recursos:

- Segregação de tarefas com funções dedicadas para gerenciamento e operações de criptografia, auditoria e integração
- Os módulos criptográficos permitem a configuração de especificações criptográficas para finalidades criptográficas exclusivas e tipos de chave
  - Chave simétrica: criptografia e descriptografia, encapsulamento e desencapsulamento de chave e autenticação
  - Chave assimétrica: geração e verificação de assinatura digital, criptografia e descriptografia, encapsulamento e desencapsulamento de chave
- Gerenciamento de ciclo de vida de chave para gerar, girar, revogar e suspender chaves, incluindo suporte a vários estados de ciclo de vida de chave
- Imposição de controles de acesso com políticas de acesso ao módulo, garantindo que o acesso seja concedido somente aos módulos criptográficos conforme configurados nas políticas.
- Proteção de chave: raiz de confiança (RoT - Root of Trust) de hardware FIPS (Federal Information Processing Standards) 140-2-L3, infraestrutura de chave pública (PKI - Public Key Infrastructure), hierarquia de chave e criptografia de envelope
- Auditoria que inclui estatísticas de uso de chave

Ativação da KMF

KMF está ativa por padrão.

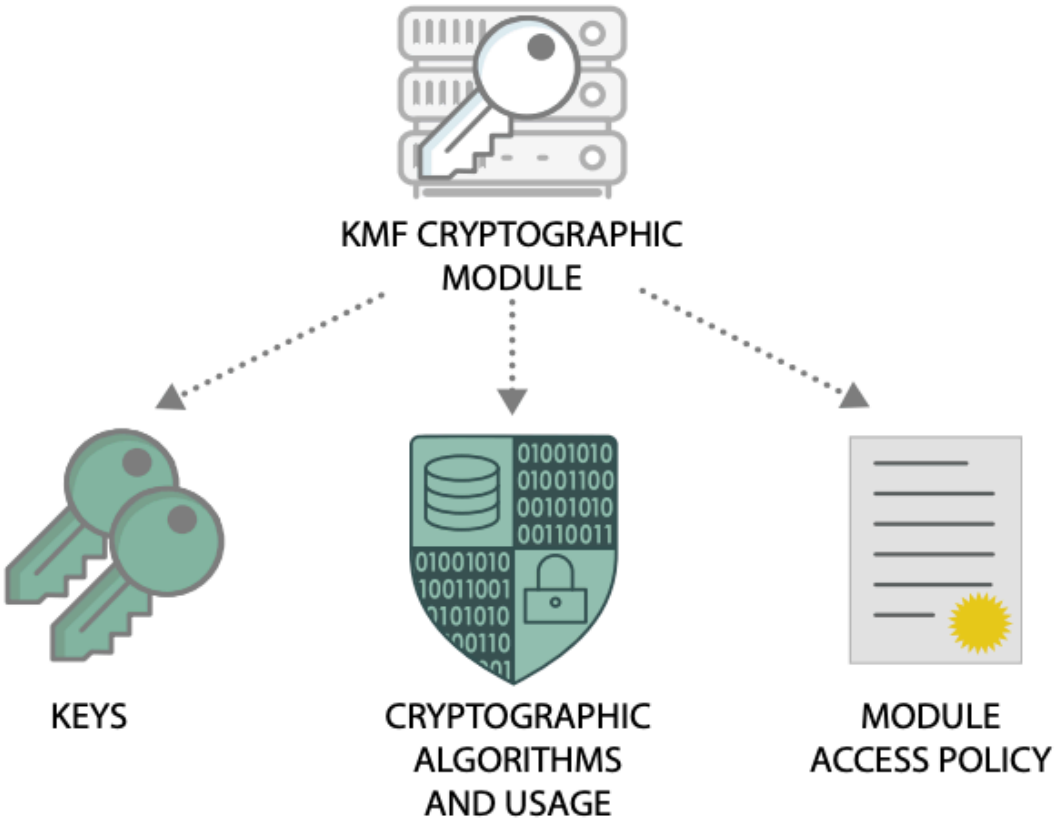
Nota: A KMF não oferece suporte ao Domain Separation, mas pode ser usada com instâncias no local.

Como a KMF funciona

Este gráfico mostra os componentes que compõem a KMF:

- Os módulos criptográficos são usados para definir o método de criptografia.
- A especificação criptográfica é uma configuração que define um algoritmo para criptografia.
- A especificação também permite definir a chave do módulo, uma chave ServiceNow ou sua própria chave fornecida pelo cliente.
- Uma política de acesso ao módulo é uma política no nível de instância que rege as condições nas quais o acesso é concedido ou negado aos módulos criptográficos.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Para obter mais informações sobre a KMF, comece com Visão geral do módulo criptográfico.

A Estrutura de gerenciamento de chaves (KMF - Key Management Framework) apresenta funções específicas para o módulo criptográfico e configurações relacionadas ao gerenciamento de chaves. Somente administradores da KMF podem atribuir usuários a outras funções da KMF. Para obter mais informações, consulte Funções instaladas com o Key Management Framework.

Para obter mais informações sobre a estrutura de criptografia que é a sucessora do CLE, consulte Criptografia em nível de coluna para empresas.

Visão geral do módulo criptográfico

Os módulos criptográficos são a peça central do (KMF). Eles definem os mecanismos criptográficos específicos usados para operações criptográficas de um determinado caso de uso.

Um módulo criptográfico aplica o mecanismo criptográfico de sua escolha a um caso de uso definido por você. Por exemplo, se você quiser proteger os dados em sua aplicação de RH com um AES-CBC com uma chave simétrica de 256 bits, poderá criar um módulo para essa finalidade.

Os módulos criptográficos também oferecem suporte ao gerenciamento do ciclo de vida da chave. Você pode criar e girar suas chaves criptográficas e definir seu método de criptografia. Os módulos criptográficos são compostos pelos seguintes componentes:

Especificação criptográfica

Define aspectos do seu módulo, incluindo sua finalidade criptográfica e quais algoritmos usar.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Chaves criptográficas

A chave que seu módulo usa para codificar ou decodificar dados criptográficos. Pode ser uma chave gerada por sua instância ou uma chave fornecida pelo cliente que você cria e carrega.

Políticas de acesso ao módulo

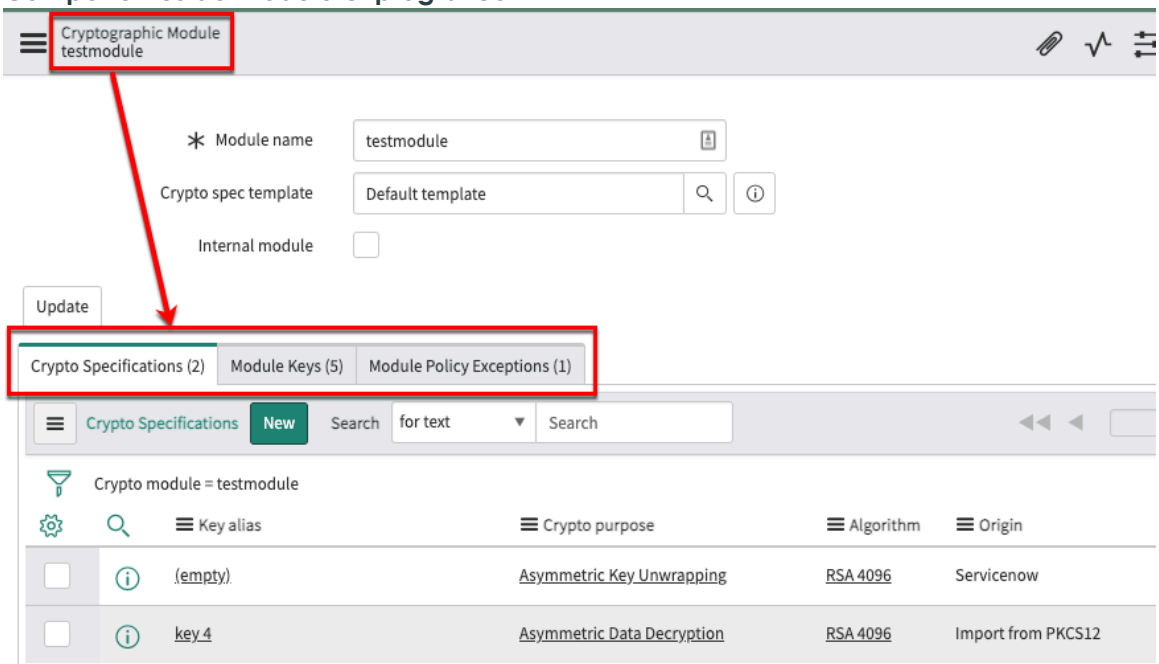
As políticas de acesso ao módulo são os mecanismos de controle de acesso que limitam a criptografia ou a descriptografia dos dados.

Exceções às políticas de módulo

Mecanismo de controle para definir exceções a uma política de acesso a um módulo.

A tela a seguir mostra esses componentes de alto nível em um módulo criptográfico:

Componentes do módulo criptográfico



Para obter detalhes sobre como criar módulos criptográficos, consulte Criação de um módulo criptográfico.

Visão geral da política de acesso ao módulo

As políticas de acesso ao módulo são os controles de acesso que você aplica aos seus módulos criptográficos para definir controles em nível de instância.

Políticas de acesso ao módulo

As políticas de acesso ao módulo são introduzidas com o Estrutura de gestão principal (KMF) no sistema de base.

Nota: É necessária uma assinatura para usar a funcionalidade Criptografia em nível de coluna para empresas. Consulte Ativação do Criptografia em nível de coluna para empresas para obter mais informações sobre Criptografia em nível de coluna para empresas.

As políticas de acesso ao módulo expandem a designação baseada em função fornecida com os módulos de criptografia. As políticas de acesso ao módulo podem ser baseadas em:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

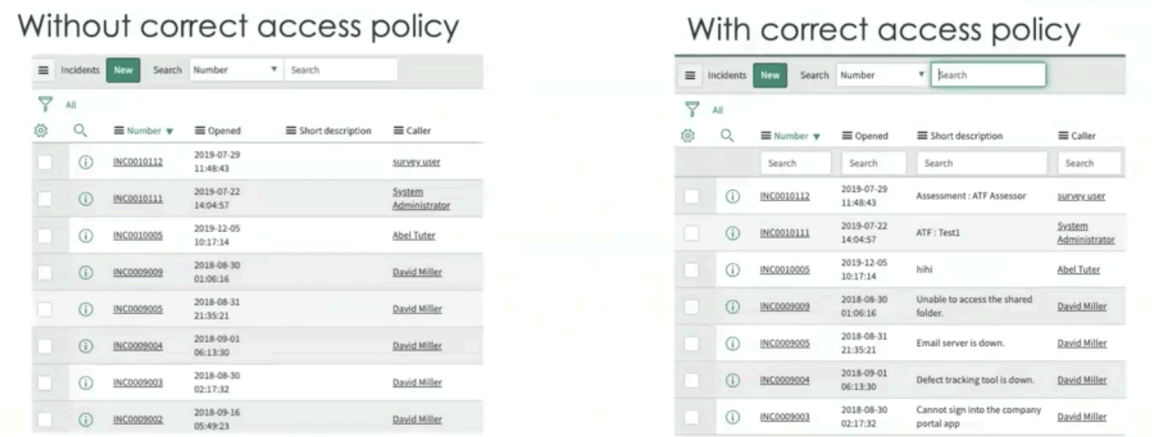
- Básico (escopo)
- Função
- Usuário do sistema
- Script
- Resource Exchange

Nota: Consulte Troca de recursos do Key Management Framework para obter detalhes.

Em um módulo criptográfico, você deve configurar as políticas de acesso ao módulo corretas para alocar o acesso aos dados criptografados. Sem uma política de acesso ao módulo associada a um módulo criptográfico, os dados criptografados não ficam visíveis para os usuários e os campos e colunas associados nas listas são exibidos em branco.

Nessa imagem, a ausência de uma política de acesso ao módulo no campo Descrição resumida criptografada oculta o conteúdo de todos os usuários que acessam a tabela de incidentes. Com uma política de acesso ao módulo em vigor, os usuários com a função permitida podem ver os dados criptografados.

Descrições resumidas criptografadas com e sem políticas de acesso ao módulo



Nota: Os dados na coluna também aparecem vazios para usuários sem a função correta especificada na política de acesso ao módulo.

Consulte Criação de uma política de acesso ao módulo para obter a configuração.

Políticas automáticas

As políticas do Autogen são geradas automaticamente pelo sistema com base na política de acesso ao módulo padrão definida para o módulo criptográfico fornecido. Estas são as políticas de nível global que serão geradas e aplicadas se não houver políticas de nível granular definidas quando o sistema ou o script tentar acessar o módulo criptográfico fornecido.

Importante:

As regras de política Autogen não são aplicadas para tipos de trabalhos agendados ou módulos de Edge Encryption (módulos em que o módulo primário é Criptografia em nível de coluna).

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Chaves de nível de instância na estrutura de gerenciamento de chave

A arquitetura Estrutura de gestão principal (KMF) apresenta uma estrutura de chave específica criada com foco em segurança. Usando um módulo de segurança de hardware (HSM), KMF usa criptografia de envelope para garantir que todas as chaves da plataforma sob gerenciamento de KMF sejam protegidas por meio de uma cadeia de chaves. As chaves de criptografia de dados do cliente (CDEKs) criadas pelo KMF também estão incluídas.

No nível da instância, o KMF define várias chaves que são usadas internamente para variados fins criptográficos em toda a Now Platform.

A criptografia de envelope é a prática de criptografar uma chave com outra chave. A figura a seguir fornece um exemplo de criptografia de envelope. Aqui, as CDEKs são criptografadas por envelope pela IKEK, que por sua vez é criptografada por envelope pela IRK, que finalmente é criptografada por envelope pela RK. Como a IRK só pode ser acessada pelo HSM, a IKEK deve ser carregada para descriptografia.

Essa tabela fornece exemplos de um subconjunto de clientes/chaves de aplicativos disponíveis que são gerenciados e protegidos por KMF.

Chave	Local	Descrição
Chave raiz (RK)	Modelo de segurança de hardware (HSM)	Chave raiz usada para descriptografar o IRK.
Chave raiz da instância (IRK)	HSM	Uma chave exclusiva para sua instância que é usada para criptografar por envelope várias chaves internas da instância.
Chave HMAC da instância (IHK)	Instância	Única por instância, a IHK é usada internamente para fins de código de autenticação de mensagem baseado em hash (HMAC). A IHK garante a autenticidade e integridade das chaves do módulo e é encapsulada no KeySecure ou no Repositório de chaves do arquivo.
Chave de criptografia da chave de instância (IKEK)	Instância	A IKEK agrupa as chaves do módulo e é agrupada no KeySecure ou no Repositório de chaves do arquivo.
Chave de criptografia assimétrica da instância (IAEK)	Instância	Uma chave exclusiva por instância que é usada internamente para fins de criptografia assimétrica. A IAEK é usada para transmitir mensagens confidenciais entre uma instância durante a aprovação do consumidor do Key Exchange ou Replicação de dados da instância.
Chave de assinatura de instância (ISK)	Instância	Uma chave exclusiva para sua instância que é usada internamente para fins de assinatura.
Password2 (PW2)	Instância	Com KMF, a chave para campos PW2 é totalmente gerenciada por KMF.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países. Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Chave	Local	Descrição
Chave de criptografia de dados do cliente (CDEK)	Instância	As chaves de criptografia criadas por meio de KMF são criptografadas em envelope pela IKEK.
Chave de criptografia de dados (DEK) da Replicação de dados da instância (IDR)	Instância	Chaves de criptografia específicas usadas para o processo de IDR.

Finalidade criptográfica, algoritmos e informações de chave

As especificações criptográficas podem ser adequadas a uma finalidade criptográfica especificada, cobrindo operações criptográficas baseadas em chaves assimétricas e simétricas. A seleção de uma finalidade criptográfica oferece mais opções, como um conjunto de algoritmos compatíveis e configurações de tamanho de chave.

Finalidade criptográfica, algoritmos e principais informações

Finalidade criptográfica	Algoritmo	Principais informações
Descriptografia assimétrica de dados	RSA	Assimétrica – chave de 2048, 3072 e 4096 bits
Criptografia assimétrica de dados	RSA	Assimétrica – chave de 2048, 3072 e 4096 bits
Desencapsulamento assimétrico de chave	RSA	Assimétrica – chave de 2048, 3072 e 4096 bits
Encapsulamento assimétrico de chave	RSA	Assimétrica – chave de 2048, 3072 e 4096 bits
Geração de assinatura	RSA	Assimétrica – chave de 2048, 3072 e 4096 bits
Verificação de assinatura	RSA	Assimétrica – chave de 2048, 3072 e 4096 bits
Autenticidade simétrica	HMAC	Simétrica – chave de 256, 384 e 512 bits
Criptografia/Descriptografia simétrica de dados*	AES-CBC *	Simétrica – chave de 128, 192 e 256 bits
	AES-CFB	
	AES-OFB	
	AES-CTR	
	AES-GCM **	
Encapsulamento/Desencapsulamento simétrico de chave*	AES-CBC *	Simétrica – chave de 128, 192 e 256 bits
	AES-CFB	
	AES-OFB	
	AES-CTR	

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Finalidade criptográfica, algoritmos e principais informações

Finalidade criptográfica	Algoritmo	Principais informações
	AES-GCM **	

* O AES-CBC oferece suporte a opções de preservação de igualdade. Criptografia em nível de coluna para empresas utiliza AES-CBC.

** O AES-GCM tem integridade de dados interna.

A configuração desses parâmetros é abordada em Criação de um módulo criptográfico.

Estados do ciclo de vida da chave do Key Management Framework

O KMF oferece suporte a vários estados de ciclo de vida da chave criptográfica ao fazer que ações permitidas específicas sejam cumpridas. Por exemplo, somente as chaves em estado ativo podem ser usadas integralmente para a finalidade criptográfica pretendida. A tabela a seguir fornece mais detalhes sobre os diferentes estados do ciclo de vida da chave.

Estado ou ação do ciclo de vida da chave	Descrição
Ativo	Só pode haver uma chave ativa para uma determinada especificação criptográfica em um módulo criptográfico.
Comprometido	Podem existir várias chaves no estado comprometido para serem revogadas em determinada especificação criptográfica em um módulo criptográfico Qualquer chave ativa ou suspensa pode ser movida para um estado comprometido. As chaves comprometidas não podem ser usadas para gerar novo conteúdo, como criptografia ou assinatura, mas ainda podem ser usadas para identificar a finalidade do conteúdo existente, como descriptografia ou verificação.
Desativado	Qualquer chave ativa pode ser desativada. Pode haver várias chaves em um estado desativado para uma determinada especificação criptográfica em um módulo criptográfico. Por exemplo, quando a chave é girada, a chave ativa atual é desativada. As chaves desativadas não podem ser usadas para gerar novo conteúdo, como criptografia ou assinatura, mas ainda podem ser usadas para identificar finalidades do conteúdo existente, como descriptografia ou verificação. **Nota:** Chaves comprometidas e revogadas são tratadas como chaves desativadas.
Destruído	Quando uma chave é destruída, seu material é removido permanentemente e não pode mais ser usado para fins criptográficos. Qualquer chave desativada pode ser destruída usando a automação do ciclo de vida se não tiver sido usada no intervalo de tempo designado configurado. Pode haver várias chaves no estado destruído para uma determinada especificação criptográfica em um módulo criptográfico.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

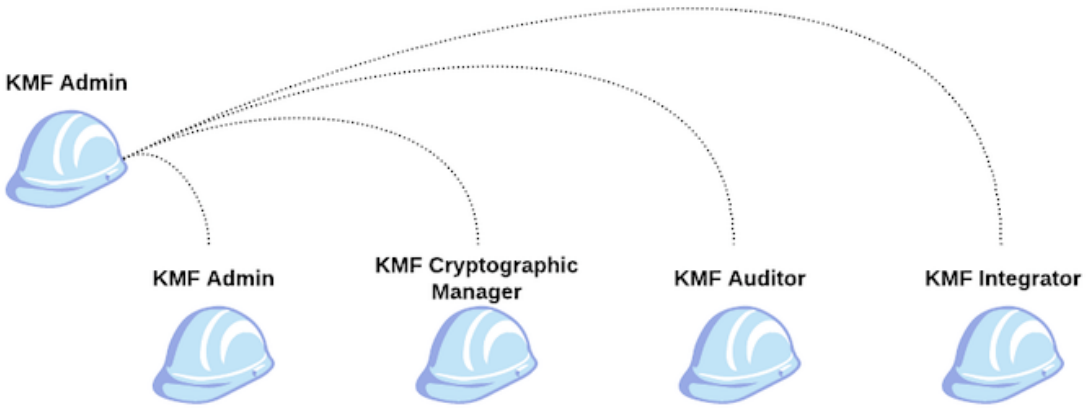
Estado ou ação do ciclo de vida da chave	Descrição
	⚠ **Aviso:** Os dados associados a uma chave destruída não podem mais ser acessados, portanto, deve-se ter muito cuidado ao executar uma ação de destruição de chave.
Gerado	Podem existir várias chaves no estado gerado para uma determinada especificação criptográfica em um módulo criptográfico Uma chave gerada pode ser movida para o estado ativo quando não houver chave ativa para a especificação criptográfica fornecida. A primeira chave gerada é definida automaticamente como ativa. **Nota:** Se a escolha for gerar uma nova chave, então uma nova chave será gerada e ativada mesmo que existam chaves em estado gerado para a especificação criptográfica fornecida.
Renovado	Uma chave ativa com data de expiração pode ser renovada várias vezes para estender o período do ciclo de vida da chave. **Nota:** A diferença entre a data de ativação e a data de expiração será calculada e a data de expiração será adiada para essa duração a partir do dia em que a renovação for feita.
Retomar	A ação de IU está disponível para que chaves suspensas sejam movidas de volta para um estado ativo quando não existir nenhuma outra chave ativa para a especificação criptográfica fornecida.
Revogado	Qualquer chave ativa ou suspensa pode ser movida para o estado de revogada. As chaves revogadas não podem ser usadas para gerar novo conteúdo, como criptografia ou assinatura, mas ainda podem ser usadas para identificar a finalidade do conteúdo existente, como descriptografia ou verificação. Podem existir várias chaves no estado revogado para determinada especificação criptográfica em um módulo criptográfico.
Girado	A rotação de chave resulta na desativação da chave ativa atual e na ativação de outra chave. Selecione a nova chave ativa entre as seguintes: • Geração de uma nova chave. • Aponte para uma chave importada existente. Qualquer chave ativa pode ser girada.
Suspenso	Pode haver várias chaves em estado suspenso para uma determinada especificação criptográfica em um módulo criptográfico. Quando a chave está suspensa, ela pode ser retomada e um estado ativo pode ser reatribuído quando não existir nenhuma outra chave ativa para essa especificação criptográfica.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Funções instaladas com o Key Management Framework

O Estrutura de gestão principal (KMF) apresenta funções específicas para o módulo criptográfico e configurações relacionadas ao gerenciamento de chaves.

Importante: Para atribuir a função de administrador do KMF, você deve ter as funções admin, security_admin e sn_kmf_admin. Use a função de administrador do KMF para atribuir outras funções do KMF. Para obter detalhes sobre como atribuir funções do KMF, consulte Atribuição de funções do KMF.



Administrador do KMF [sn_kmf.admin]

Atribui funções a outros usuários para executar operações no Estrutura de gestão principal da ServiceNow.

Contém funções

Lista de funções contidas na função.

Nenhum.

Grupos

Lista de grupos aos quais esta função está atribuída por padrão.

Nenhum.

Considerações especiais

Importante: Evite conceder uma função de administrador quando houver mais funções especializadas disponíveis.

- Esta função é atribuída por meio do processo mostrado em Atribuição de funções do KMF.
- Você deve ter essa função para designar funções do KMF e, além disso, pode executar todos os recursos do gerenciador de criptografia do KMF.

Gerenciador de criptografia do KMF [sn_kmf.cryptographic_manager]

Crie, leia e atualize operações em módulos criptográficos (associação de chaves para uso de criptografia e configurações de algoritmo) e políticas de acesso ao módulo. Além disso, os gerenciadores de criptografia do KMF podem executar operações de gerenciamento de chaves (gerar, girar, revogar) e de ciclo de vida.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Contém funções

Lista de funções contidas na função.

Nenhum.

Grupos

Lista de grupos aos quais esta função está atribuída por padrão.

Nenhum.

Considerações especiais

Nenhum.

Auditor de criptografia do KMF [sn_kmf.cryptographic_auditor]

Exibir informações do módulo criptográfico, metadados de chave e detalhes relacionados ao ciclo de vida, bem como informações de política de acesso ao módulo (MAP).

Contém funções

Lista de funções contidas na função.

Nenhum.

Grupos

Lista de grupos aos quais esta função está atribuída por padrão.

Nenhum.

Considerações especiais

Nenhum.

Integrador de criptografia do KMF [sn_kmf.cryptographic_integrator]

Integre Estrutura de gestão principal a armazenamentos de chaves ou sistemas externos.

Contém funções

Lista de funções contidas na função.

Nenhum.

Grupos

Lista de grupos aos quais esta função está atribuída por padrão.

Nenhum.

Considerações especiais

Nenhum.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Operador de criptografia do KMF [sn_kmf.cryptographic_operator]

Acesse parte do ciclo de vida da chave ServiceNow Estrutura de gestão principal: renovação, rotação, revogação.

Contém funções

Lista de funções contidas na função.

Nenhum.

Grupos

Lista de grupos aos quais esta função está atribuída por padrão.

Nenhum.

Considerações especiais

Nenhum.

Atribuição de funções do KMF

Atribua funções KMF aos administradores, que por sua vez podem atribuir outras funções KMF.

Antes de Iniciar

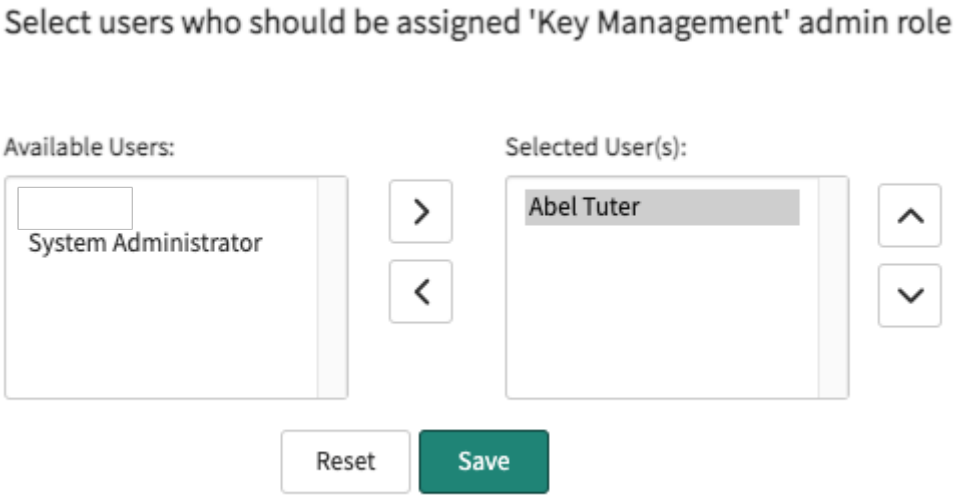
Funções necessárias: admin e security_admin

Você deve elevar para a função security_admin antes de atribuir a função de administrador do KMF. Para obter instruções, consulte Elevar para uma função privilegiada.

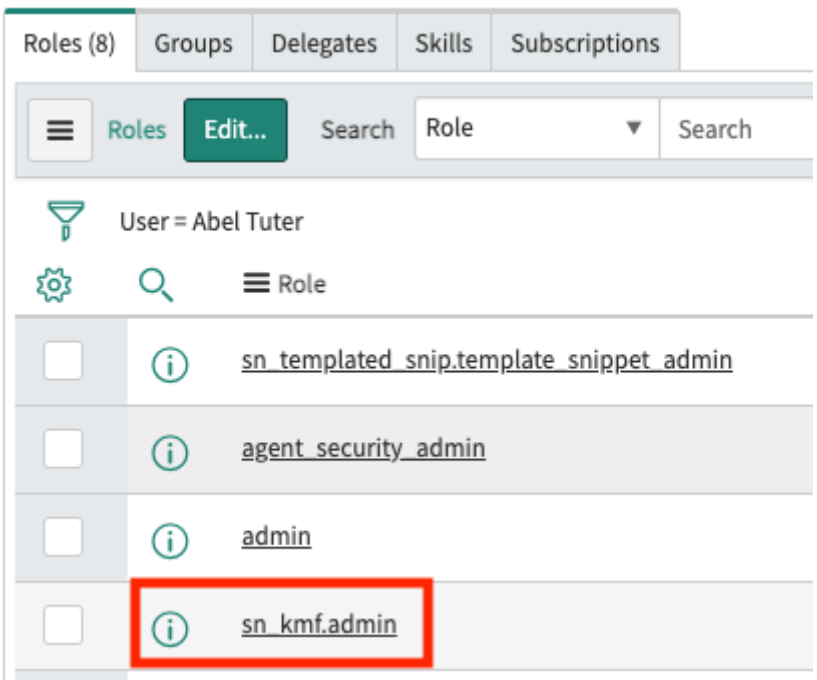
Procedimento

1. Elevação para a função de administrador de segurança.
2. Navegue até **Administração de usuário** > **Usuários** e selecione o usuário que você deseja que seja o administrador do KMF.
3. Verifique se o usuário já tem as funções admin e security_admin.
   Caso contrário, selecione **Editar** na lista relacionada de Funções e adicione **admin** e **security _admin**.
4. Navegue até **Segurança do sistema** > **Administração de gerenciamento de chave**.
5. Selecione o usuário que deseja que seja administrador do KMF na coluna **Usuários disponíveis** e mova-o para a coluna **Usuários selecionados**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



6. Selecione **Salvar**.
7. Navegue até **Administração de usuário** > **Usuários** e selecione o usuário ao qual acabou de atribuir a função sn_kmf.admin.
   O usuário tem a função sn_kmf.admin na lista relacionada **Funções** e pode atribuir outras funções KMF.

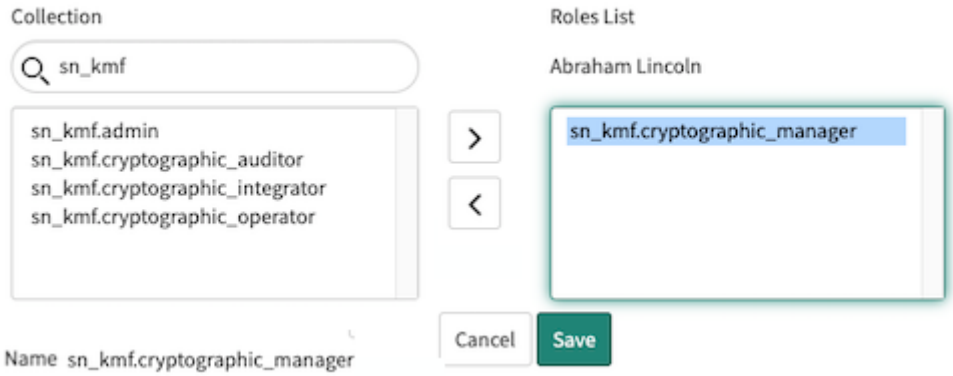


O que Fazer Depois

Se você tiver a função de administrador do KMF, siga estas etapas para atribuir outras funções do KMF:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

1. Navegue até **Administração de** > **Usuários** e selecione o usuário para o qual você deseja dar outra função do KMF, como Gerenciador de criptografia do KMF.
2. Na lista relacionada de Funções, clique em **Editar** e selecione as funções do KMF que deseja atribuir aos usuários. Todas as funções KMF começam com `sn_kmf`.



Definição das configurações de Edge Encryption para selecionar o tipo de chave

Defina as configurações de Edge Encryption para usar as chaves fornecidas por ServiceNow ou suas próprias chaves fornecidas pelo cliente (CSK) para criptografia na Now Platform.

Antes de Iniciar

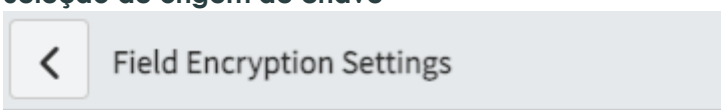
As chaves fornecidas pelo cliente são compatíveis somente com Criptografia em nível de coluna para empresas.

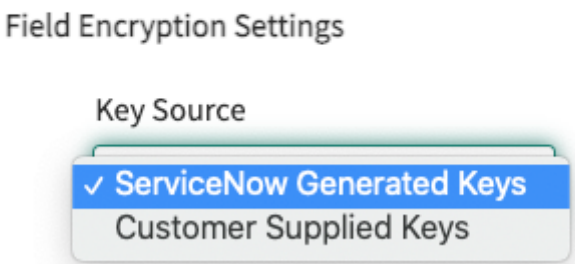
Funções necessárias: sn_kmf.cryptographic_manager e security_admin

Procedimento

1. Navegue até **Todos** > **Segurança do sistema** > **Configurações de Edge Encryption**.
2. Em Configurações de Edge Encryption, selecione **Chaves geradas pela ServiceNow** ou **Chaves fornecidas pelo cliente** na lista **Origem de chave**.

Seleção de origem de chave





© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Esta opção muda a propriedade `com.glide.encryption.cle_kmf.key_source` para **Chaves geradas pela ServiceNow** ou **Chaves fornecidas pelo cliente**.

3. Selecione **Salvar**.

O que Fazer Depois

- Se você estiver usando suas próprias chaves fornecidas pelo cliente, consulte Usar chaves fornecidas pelo cliente com a Criptografia em nível de coluna para empresas.
- Se você estiver usando chaves fornecidas por ServiceNow, comece a criar seu módulo criptográfico. Consulte Criação de um módulo criptográfico.

Criação de um módulo criptográfico

Crie um módulo criptográfico para definir os mecanismos usados para operações criptográficas. Depois de criar o módulo, você cria uma especificação criptográfica, onde define um algoritmo para criptografia e gera uma chave.

Antes de Iniciar

Se estiver fornecendo suas próprias chaves, vá para Configure e carregue a chave fornecida pelo cliente.

Função necessária: sn_kmf.cryptographic_manager

Por Que e Quando Desempenhar Esta Tarefa

Este procedimento descreve as opções disponíveis com KMF no ServiceNow sistema de base da plataforma. A funcionalidade Criptografia em nível de coluna para empresas está disponível apenas quando o plug-in *`com.glide.now.platform.encryption`* está ativo. Consulte Ativação do Criptografia em nível de coluna para empresas para obter mais informações sobre como obter Criptografia em nível de coluna para empresas. Consulte Criação de um módulo criptográfico do Criptografia em nível de coluna..

Nota: Os registros do módulo criptográfico [sys_kmf_crypto_module] não podem ser excluídos.

Procedimento

1. Navegue até **Todos** > **Gerenciamento de chave** > **Módulos criptográficos** > **Criar novo**.
2. No formulário, preencha os campos:

Campos do Módulo criptográfico

Campo	Descrição
Nome do módulo	Cadeia de caracteres alfanuméricos a ser referenciada ao executar scripts.
Modelo de especificação de criptografia	Selecione o modelo **Padrão** a ser usado para criar o módulo criptográfico, pois ele contém mapeamentos de algoritmos compatíveis para especificações de criptografia.
Valor da política de acesso ao módulo padrão	◦ Depende de padrão do sistema: ◦ Rejeitar ◦ Rastrear
Resultado real da política	Rejeitar ou rastrear, com base no valor de política padrão ou no valor selecionado durante a criação da política de acesso ao módulo.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
de acesso ao módulo	
Nome	Nome do módulo criptográfico anexado ao nome do escopo da aplicação.
Estado do ciclo de vida do módulo de criptografia	Ciclo de vida refere-se à criação, ao uso e à desativação de um módulo criptográfico. Defina como **Rascunho** inicialmente durante a configuração. Ao usar o módulo, defina este campo como **Publicado**. O modelo Padrão é definido automaticamente como Publicado.

3. Selecione **Enviar**.

⚠ Aviso:

Para usuários de suporte a criptografia legada:

Se estiver usando a versão não Enterprise de Criptografia em nível de coluna, há um limite de cinco módulos. Se você excedeu esse limite, o seguinte aviso será exibido:

Esta inserção excede o limite de módulos publicados para o Criptografia em nível de coluna#disponíveis com a assinatura do produto. A assinatura Enterprise para o Criptografia em nível de coluna é necessária para outros módulos. Entre em contato com sua equipe de conta.

Após o envio bem-sucedido, seu módulo criptográfico será listado na tabela Módulos criptográficos. O sistema adiciona o nome ao escopo para evitar conflito com outras aplicações com escopo. Por exemplo, se você criar um módulo com o nome `my_crypto_module` no escopo da aplicação global, o nome será salvo como `global.my_crypto_module`.

O que Fazer Depois

Criação de uma especificação criptográfica

.

Criação de uma especificação criptográfica

Após criar um módulo criptográfico, crie uma especificação criptográfica para definir os algoritmos do módulo.

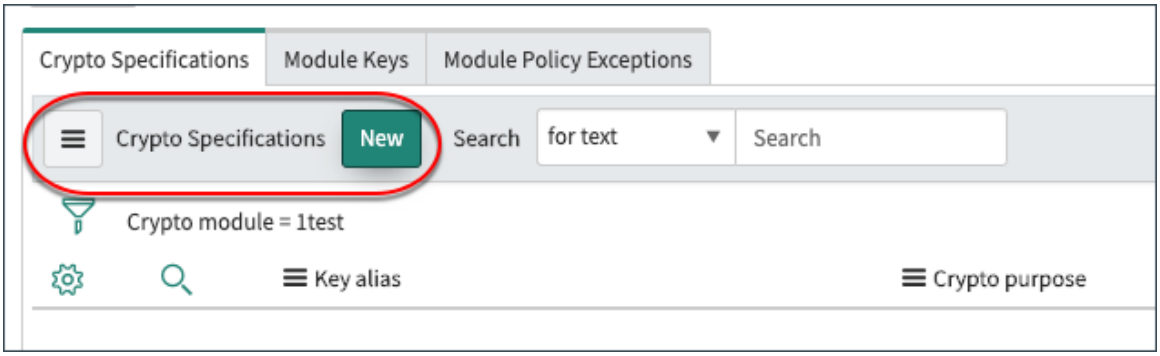
Antes de Iniciar

Função necessária: sn_kmf.cryptographic_manager

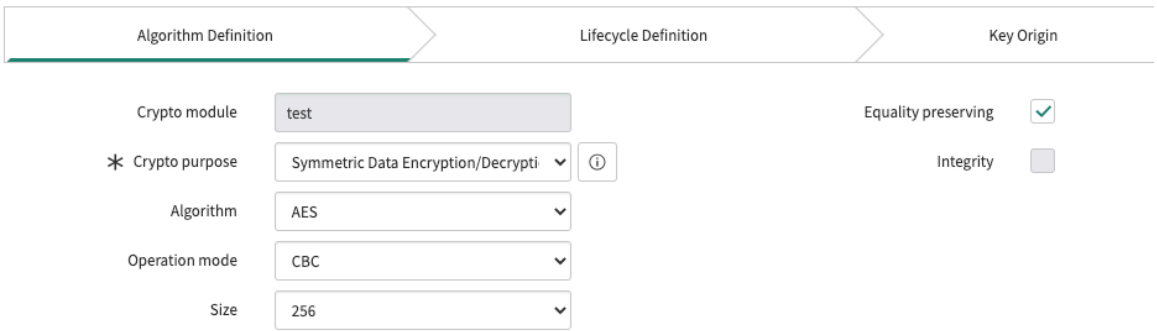
Procedimento

1. Navegue até **Gerenciamento de chave** > **Módulos criptográficos** > **Todos**.
2. Selecione o módulo criptográfico a ser definido para abrir as opções de configuração.
3. Na guia **Especificações de criptografia**, clique em **Novo**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Preencha o formulário de Definição de algoritmo.
   Consulte Finalidade criptográfica, algoritmos e informações de chave para obter detalhes.



A tela de definição do algoritmo é aberta. Selecione opções para a geração de chave. Repita essa etapa para gerar várias chaves para o módulo de criptografia selecionado.

Campos da Definição de algoritmo

Campo	
Módulo criptográfico	Somente leitura. O nome do módulo criptográfico selecionado é exibido.
Finalidade da criptografia	Selecione a finalidade deste módulo. Por exemplo, você pode usá-lo para criptografia de dados, geração de assinatura ou encapsulamento de chave. Os algoritmos disponíveis são ajustados com base na finalidade de criptografia selecionada. Consulte Finalidade criptográfica, algoritmos e informações de chave para obter detalhes.
Algoritmo	Tipo de algoritmo usado para realizar a finalidade da criptografia. O algoritmo também controla a origem da chave. Ajusta-se automaticamente com base na finalidade de criptografia selecionada. Finalidade criptográfica, algoritmos

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	
	e informações de chave para obter detalhes.
Modo de operação	Este campo pode ser exibido com base na finalidade de criptografia selecionada.
Tamanho	Selecione o tamanho do bit.
Hash	Este campo se torna disponível com base no algoritmo selecionado.
Preservação de igualdade	Habilita a criptografia não determinística. Esta opção aparece ao selecionar **Criptografia/descriptografia simétrica de dados** com **AES** e no modo **Cipher Block Chaining (CBC)**. Selecionar essa opção significa que se os mesmos dados forem criptografados novamente, os dados codificados serão os mesmos todas as vezes. A criptografia não determinística não é compatível com a filtragem de uma lista de dados criptografados usando operadores de comparação de igualdade.
Integridade	O modo de operação GCM fornece integridade.

5. Clique em **Avançar**.
   A especificação criptográfica é listada na tabela Ciclo de vida da chave com base nos algoritmos selecionados.

O que Fazer Depois
Execute uma das seguintes operações:

- Selecione uma entrada na tabela Ciclo de vida da chave para definir o comportamento do ciclo de vida da chave. Consulte Configuração de estados do ciclo de vida da chave para obter detalhes para concluir a definição do ciclo de vida da chave.
- Clique em **Avançar** para criar uma chave criptográfica. Consulte uma das tarefas a seguir para geração de chaves:
  - Geração de uma chave criptográfica da ServiceNow.
  - Configurar propriedades de chaves fornecidas pelo cliente.
  - Importação do par de chaves de encapsulamento/desencapsulamento.

Configuração de estados do ciclo de vida da chave

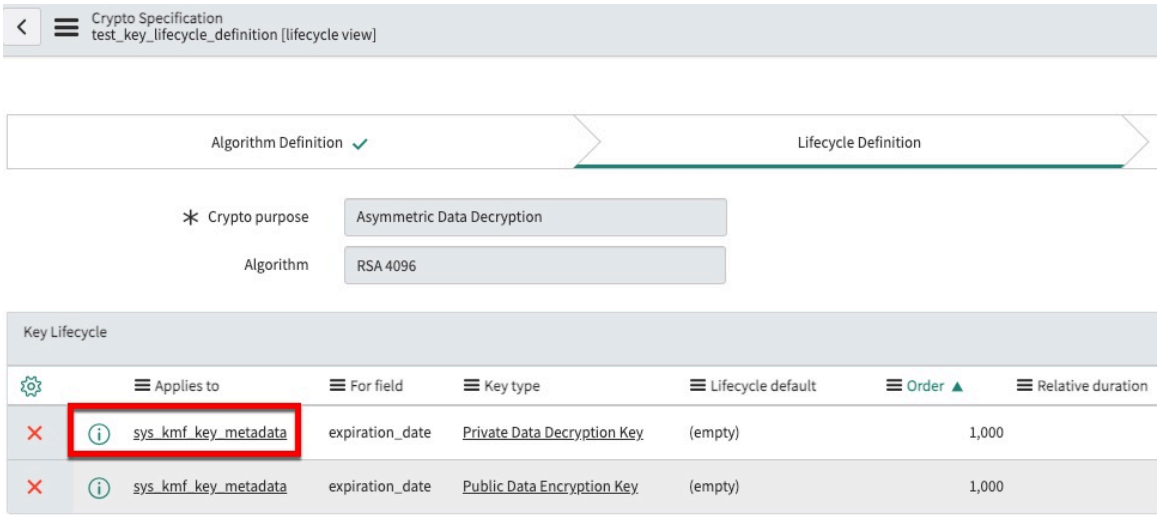
Após criar uma especificação criptográfica, é possível configurar as ações de ciclo de vida para as chaves em sua instância.

Antes de Iniciar
Função necessária: sn_kmf.admin

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

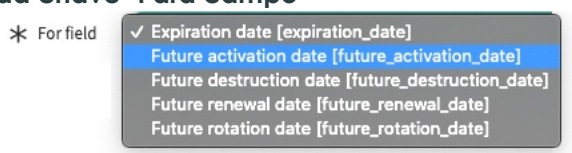
Procedimento

1. Navegue até **Gerenciamento de chave** > **Módulos criptográficos** > **Todos**.
2. Selecione o módulo criptográfico para configurar o ciclo de vida de uma chave.
3. Clique em um alias de chave na guia Especificações criptográficas.
   O formulário de Definição de algoritmo será aberto para a chave selecionada.

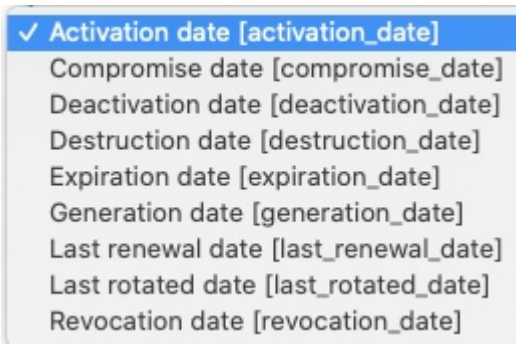


4. Clique em **Avançar**.
   O campo Modelo de ciclo de vida será carregado. Os valores padrão do ciclo de vida da chave são criados com base nos algoritmos selecionados para a especificação de criptografia definida.
5. Selecione um ciclo de vida da chave na coluna **Aplica-se a** na etapa de Definição de ciclo de vida da especificação criptográfica.

Campos do Ciclo de vida da chave

Campo	Descrição
Aplica-se a	Chave selecionada à qual o ciclo de vida se aplica.
Para campo	Selecione o tipo de controle da chave à qual o ciclo de vida se aplica. **Valores de gerenciamento de ciclo de vida da chave "Para campo"** 
Tipo	Selecione se a avaliação do ciclo de vida da chave é um valor relativo ou um valor absoluto: ◦ **Relativo**: insira um valor que dependa de outras entradas de dados no sistema, como geração de chave, ativação e desativação. ◦ **Absoluto**: insira um valor exato, como uma data.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Ciclo de vida padrão	Somente leitura. Exibe um valor caso tenha sido definido.
Ordem	Insira a sequência na qual processar o estado do ciclo de vida da chave da especificação criptográfica.
Tipo de duração relativa	Duração do ciclo de vida: **Anos**, **Meses**ou **Dias**.
Duração relativa	Número de anos, meses ou dias em que a chave é válida.
Operação relativa	**Antes**ou **Depois**.
Relativo a	Campo ao qual a duração é relativa. Exibe se uma duração relativa ou operação foi selecionada. 

Geração de uma chave criptográfica da ServiceNow

Siga este procedimento para carregar e configurar uma chave criptográfica ServiceNow para criptografar dados confidenciais.

Antes de Iniciar

Função necessária: sn_kmf.cryptographic_manager

Por Que e Quando Desempenhar Esta Tarefa

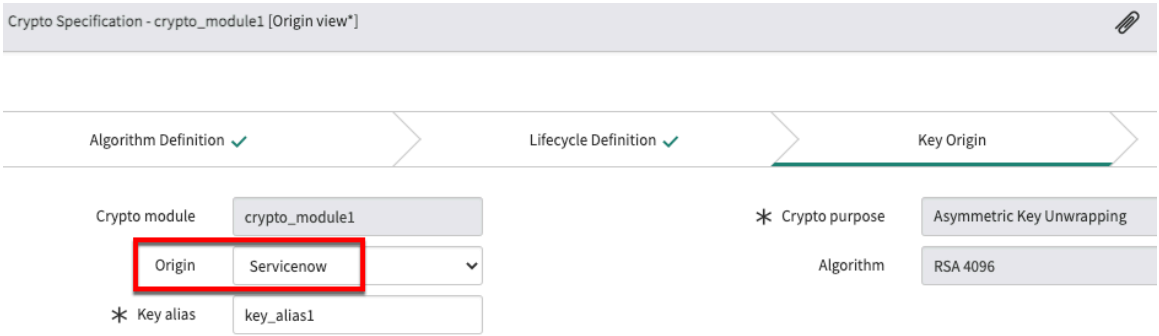
Os gerentes criptográficos têm a opção de usar chaves fornecidas pela ServiceNow ou suas próprias chaves fornecidas pelo cliente (CSK) para criptografia em Now Platform com Criptografia em nível de coluna para empresas. Para obter informações sobre CSK, consulte Configurar propriedades de chaves fornecidas pelo cliente.

Procedimento

1. Defina as configurações de criptografia de campo para usar as chaves geradas pela ServiceNow. Consulte Definição das configurações de Edge Encryption para selecionar o tipo de chave para obter detalhes.
2. Navegue até **Gerenciamento de chave** > **Módulos criptográficos** > **Todos**.
3. Selecione o módulo de criptografia correspondente para abrir a página de detalhes do módulo de criptografia.
4. Clique na coluna de entrada de alias de chave na guia Especificações de criptografia. Se uma chave ainda não tiver sido gerada, o campo de alias da chave estará vazio.
5. Clique em **Avançar** para navegar até a guia Origem da chave dos Componentes de especificação de criptografia.
   A guia Definição do ciclo de vida será exibida junto com a tabela Ciclo de vida da chave e pode ser revisada ou editada. Consulte Configuração de estados do ciclo de vida da chave para obter detalhes.

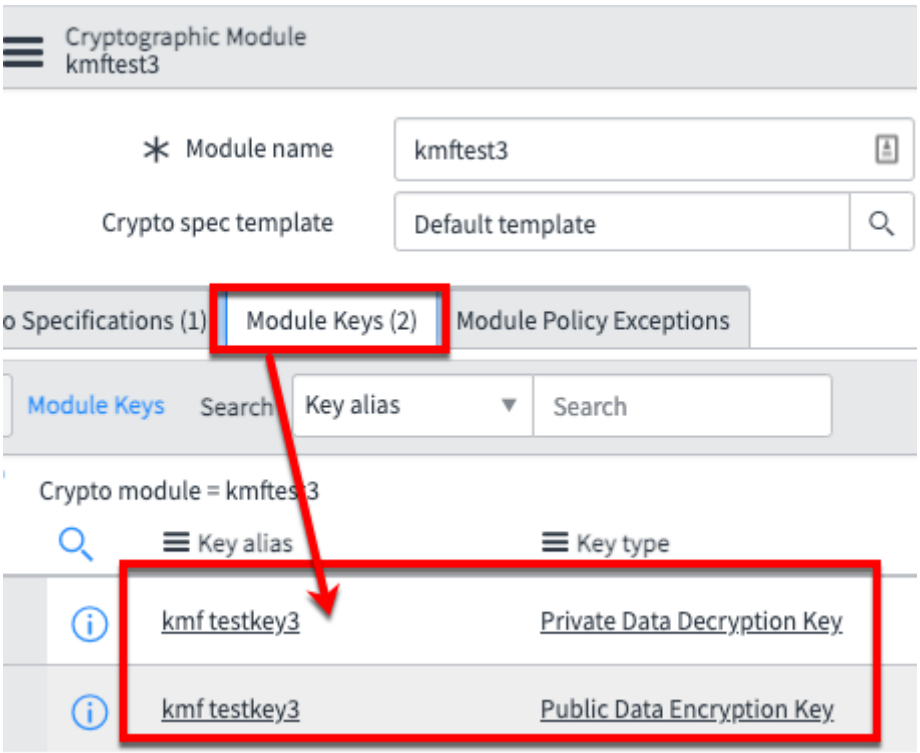
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

6. Selecione **Servicenow** no campo



Origem.
Este campo varia de acordo com as configurações de Edge Encryption da Etapa 1 e o algoritmo selecionado. Para usar uma chave importada, consulte Importação do par de chaves de encapsulamento/desencapsulamento. Consulte Configurar propriedades de chaves fornecidas pelo cliente se você estiver usando sua própria chave.

7. Insira um nome amigável de alias da chave.
8. Clique em **Avançar** para ir para a guia Criação de chave.
9. Clique em **Gerar chave**.
   Após gerar a chave, o formulário do Módulo criptográfico será recarregado exibindo a especificação criptográfica.
10. Clique na guia **Chaves do módulo** para exibir as chaves.
    As informações seguras da chave serão armazenadas na guia Chaves do módulo junto com o número de chaves existentes para a especificação criptográfica.



11. Selecione uma chave para executar ações de gerenciamento de chaves. Consulte Ações de gerenciamento de chave para obter detalhes.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Criação de uma política de acesso ao módulo

Crie políticas de acesso ao módulo para estabelecer limites sobre se os dados podem ser criptografados ou descriptografados.

Antes de Iniciar

Função necessária: sn_kmf.cryptographic_manager ou sn_kmf.admin

Por Que e Quando Desempenhar Esta Tarefa

A Criptografia em nível de coluna (CLE) oferece suporte a políticas de acesso ao módulo baseadas em função e opções de configuração adicionais ficam disponíveis com a funcionalidade (CLE_Ent).

- Configure a operação criptográfica específica nas políticas de acesso do módulo para módulos criptográficos que dão suporte operações simétricas Por exemplo, um usuário pode ter permissão para criptografar dados, mas não para descriptografar dados.
- Define um valor padrão de política de acesso ao módulo por ou módulo criptográfico.
- Associa versões de script em que as mudanças no script são rastreadas e invalida a política de script, fornecendo melhor segurança para políticas de acesso ao módulo do tipo script.

A funcionalidade CLE_Ent está disponível com uma assinatura paga. Consulte para conhecer os recursos suportados e as opções disponíveis com cada oferta. Para obter mais informações, consulte Criptografia em nível de coluna para empresas.

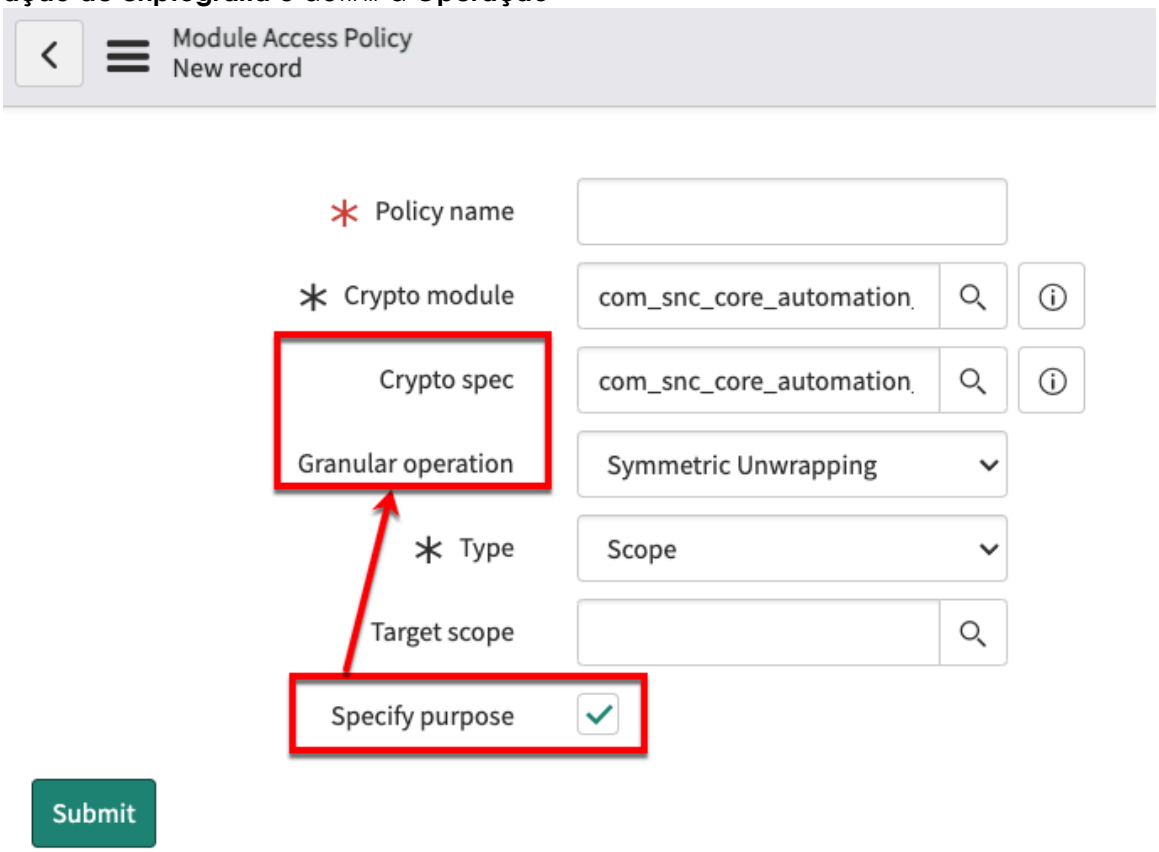
Nota: O comportamento padrão das políticas de acesso ao módulo (MAPs) é Rejeitar para ajudar a impedir qualquer acesso não autorizado, a menos que explicitamente declarado nos registros MAP.

Procedimento

1. Navegue até **Todos** > **Gerenciamento de chave** > **Políticas de acesso ao módulo** > **Todas**.
   Quando você cria um módulo criptográfico configurado para criptografia/descriptografia de dados simétricos, uma política de acesso de módulo é criada manualmente e será listada na tabela.
2. Clique em **Novo**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Selecione **Especificar finalidade** para escolher uma **Especificação de criptografia** e definir a **Operação granular**.



© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

◦ Com as especificações criptográficas para criptografia/descriptografia simétrica de dados e encapsulamento/desencapsulamento simétrico, o campo **Operação granular** ficará disponível se você marcar a caixa de seleção **Especificar finalidade**.

3. Preencha o formulário.

Campos de políticas de acesso ao módulo

Campo	Descrição
Nome da política	Insira um nome para a política.
Módulo de criptografia	Clique no ícone de pesquisa ( ) para selecionar um módulo.
Especificação de criptografia	Selecione ou crie uma nova especificação criptográfica ao gerar a política de acesso ao módulo. Este campo se torna disponível quando a caixa de seleção **Especificar finalidade** é marcada.
Operação granular	Selecione a finalidade criptográfica na especificação criptográfica. Os valores disponíveis dependem do tipo de especificação criptográfica selecionada. Consulte para obter detalhes sobre finalidades de criptografia.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Tipo	◦ **Escopo**: controla o acesso pelo escopo da aplicação. ◦ **Usuário do sistema**: permite que os usuários do sistema acessem os módulos de criptografia. ◦ **Script**: controla o acesso por script. Consulte para obter mais informações ◦ **Função**: controla o acesso por função do usuário. ◦ **Troca de recurso**: controla o acesso usando Resource Exchange. Para obter mais informações, consulte . **Nota:** Somente o tipo Função é compatível com a Criptografia em nível de coluna Todos os outros tipos estão disponíveis com Criptografia em nível de coluna para empresas.
Escopo de destino	O campo está visível como um identificador do tipo **Escopo**. Refere-se à funcionalidade da política. Selecione as aplicações no menu de pesquisa. **Nota:** O escopo de destino não é compatível e só pode ser definido com Criptografia em nível de coluna para empresas
Função de destino	O campo está visível como um identificador do tipo **Função**. Função á qual essa política se aplica.
Tabela de scripts Scripts de destino	Esses campos aparecem quando você seleciona **script** como o tipo. O campo está visível como um identificador do tipo **Script**. Seleciona uma tabela à qual essa política se aplica. Documento ao qual essa política se aplica. Selecione o **Nome da tabela** e o documento relacionado à política. Na primeira vez que um script chama um módulo criptográfico, o acesso ao módulo é negado e o desenvolvedor recebe um erro. Isso concede ao proprietário do módulo a capacidade de conceder ou recusar acesso ao módulo.
Troca de recursos: ◦ Especificação de criptografia ◦ Tipo de aprovação ◦ Host de instância de destino	Essas opções aparecem quando você seleciona como tipo. Resource Exchange é compatível com KMF e quando o módulo primário é **column_level_encryption**. Selecione a especificação de criptografia, Única ou Recorrente, e o URL da instância de destino. Para obter mais informações, consulte .
Representação	Nas políticas de acesso ao módulo baseadas em função, os usuários podem acessar dados criptografados usando uma sessão de representação. Quando usuários,

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	como os administradores, representam outros usuários, essas políticas de acesso ao módulo habilitadas para representação são aplicadas.
Especificação de finalidade	Selecione para alternar o campo de especificação de criptografia como um campo disponível para a política.
Ativo	Selecione para ativar a política.
Resultado	Selecione uma das seguintes propriedades: ◦ **StrictReject** rejeita o acesso em todas as circunstâncias. ◦ **Rejeitar** rejeita os usuários com a **Função de destino** ou o **Escopo de destino** acessem este módulo de criptografia, a menos que outra política permita o acesso. ◦ **Rastrear** para permitir o acesso e monitorar o uso do módulo.

4. Selecione **Enviar**.

> **Aviso:**
>
> Para usuários de suporte a criptografia legada:
>
> Se estiver usando a versão não Enterprise de Criptografia em nível de coluna, há um limite de cinco módulos. Se você excedeu esse limite, o seguinte aviso será exibido:
>
> Esta inserção excede o limite de módulos publicados para o Criptografia em nível de coluna#disponíveis com a assinatura do produto. A assinatura Enterprise para o Criptografia em nível de coluna é necessária para outros módulos. Entre em contato com sua equipe de conta.

5. Seleção do nome da política associada ao módulo criptográfico que você deseja examinar.
   Usando a política de acesso ao módulo do tipo Script:

   Uma política de acesso ao módulo é gerada automaticamente com base na configuração de acesso padrão quando o script é executado. O nome do módulo é precedido por `AutoGen-`. Por exemplo, o módulo `Module-TestPolicy` está listado como `AutoGen-Module-TestPolicy` na coluna Nome da política.

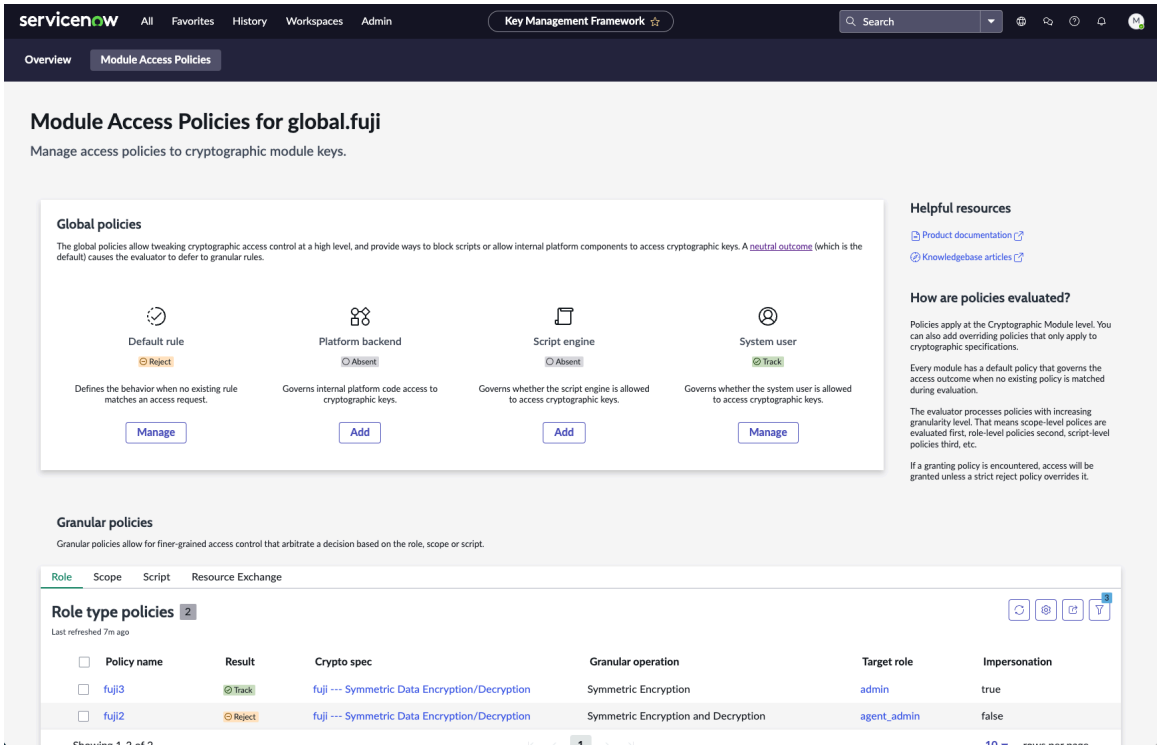
   O formulário de Política de solicitante de criptografia lista a política de solicitante que você selecionou. O campo Escopo de destino especifica o escopo do script que está tentando usar o módulo. Consulte para obter informações adicionais.

   > **Nota:** Com a Criptografia em nível de coluna, são permitidas no máximo cinco políticas de acesso ao módulo. Consulte para opções de configuração.

Visualização da política de acesso ao módulo

Use a visualização da política de acesso ao módulo para exibir todas as informações relevantes do módulo criptográfico em uma única página de IU.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

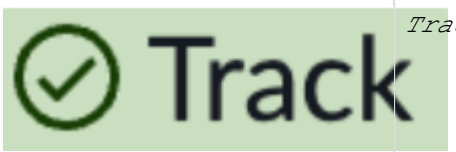


Os administradores do KMF (Key Management Framework) e os gerentes criptográficos podem usar a página de IU da política de acesso ao módulo para exibir todos os mecanismos de controle de acesso relacionados a um único módulo criptográfico. Use as informações coletadas nesta página de IU para determinar rapidamente quem tem acesso às informações criptografadas em sua instância.

Usuários com as funções de *sn_kmf.admin* ou *sn_kmf.cryptographic_manager* podem acessar a página da IU de visualização da política de acesso ao módulo navegando até **"Todos"** > **"Gerenciamento de chave"** > **"Módulos criptográficos"** > **"Todos"**.

Rótulos de resultados

As políticas de acesso ao módulo contêm um campo de **Resultado** que determina se o acesso ao módulo criptográfico selecionado deve ser concedido. A página de IU exibe um rótulo nos elementos da página de IU com base no valor desse campo.

Rótulo da IU	Valor do campo de resultado	Definição
	*Track* ou *Allow*	O acesso é concedido a todos os usuários, incluindo scripts.
	Reject	O acesso é negado, a menos que uma política de acesso ao módulo de rastreamento seja encontrada.
	StrictReject	Acesso negado.

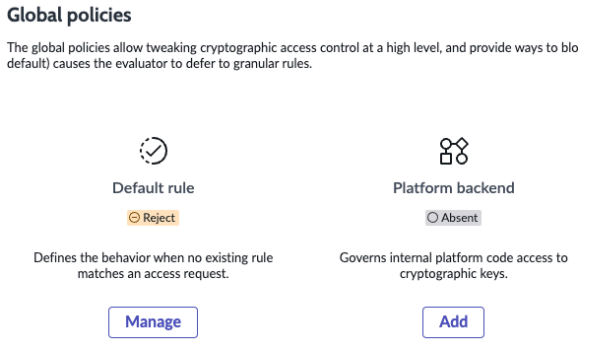
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Rótulo da IU	Valor do campo de resultado	Definição
○ Absent	N/A	A política de acesso ao módulo não existe na instância. Acesso negado a todos.

Políticas globais

Use a seção **Políticas globais** para revisar as políticas de acesso ao módulo que controlam o acesso no nível da plataforma.

Selecione o botão **"Gerenciar"** abaixo de qualquer uma das políticas para navegar até esse registro de política. Se a política não existir, um botão **"Adicionar"** aparecerá abaixo dessa entrada. Selecione o botão **"Adicionar"** para navegar até um novo registro de política onde você pode definir a política.

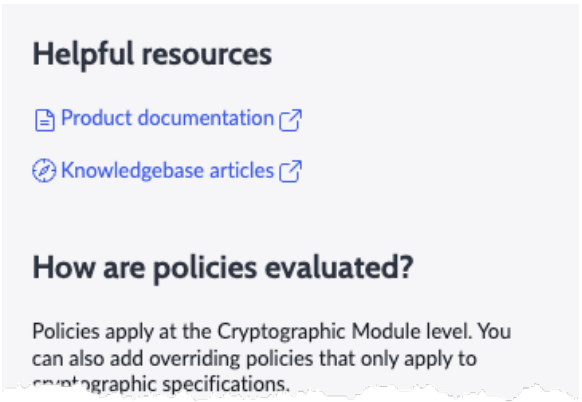


Política	Definição
Regra padrão	A política de regra padrão define o comportamento quando nenhuma regra corresponde a uma solicitação de acesso.
Back-end da plataforma	A política back-end da plataforma controla o acesso ao código da plataforma interna às chaves criptográficas.
Mecanismo de script	A política do mecanismo de script controla se ele tem permissão para acessar chaves criptográficas.
Usuário do sistema	A política de usuário do sistema controla se o usuário do sistema tem permissão para acessar chaves criptográficas.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Recursos úteis

Use a seção **"Recursos úteis"** para encontrar links para a documentação de produtos, artigos de conhecimento relevantes e uma breve descrição sobre como as políticas de acesso ao módulo são avaliadas na plataforma. Para obter uma visão mais profunda de como as políticas de acesso ao módulo são avaliadas, consulte Depurador de política de acesso ao módulo.

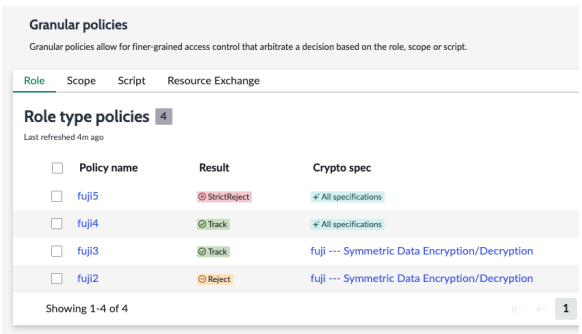


Políticas granulares

Use a seção de **Políticas granulares** para exibir listas de políticas de acesso a módulos separadas por tipo de política. Use as guias acima da lista para selecionar uma categoria de política a ser exibida.

- Função
- Escopo
- Escopo e domínio (se a Separação de domínios estiver ativa)
- Script
- Troca de recursos (se o módulo criptográfico for um Password2 ou submódulo de Criptografia em nível de coluna)
- Identidade (se a Gestão de segredos Enterprise estiver ativa)

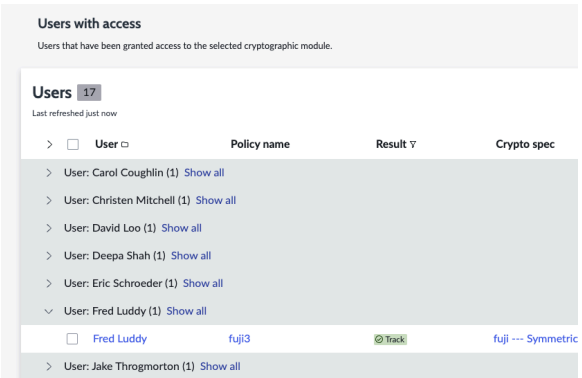
Por padrão, cada lista exibe somente as políticas ativas. Use o ícone de filtro para alterar o filtro padrão da lista.



© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Usuários com acesso

Use a seção **Usuários com acesso** para ver uma lista de todos os usuários que têm acesso ao módulo criptográfico selecionado. A lista é agrupada por usuário, pois cada usuário pode ter várias funções que concedem acesso a um módulo criptográfico.

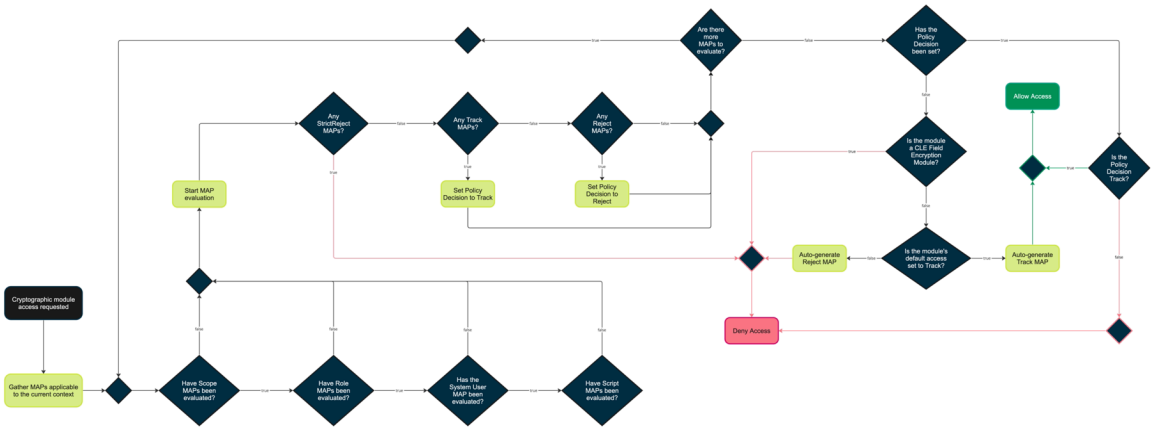


Depurador de política de acesso ao módulo

Use o depurador de política de acesso ao módulo para revisar as informações de registro em log e entender por que seus usuários têm ou não acesso a um contexto criptografado.

As MAPs (políticas de acesso ao módulo) definem controles no nível da instância para acesso a módulos criptográficos. Os solicitantes (por exemplo, um usuário ou script) necessitam de acesso explícito para usarem um módulo criptográfico para criptografia e descriptografia. Nem sempre fica claro quais MAPs são avaliados quando os solicitantes tentam acessar um módulo criptográfico. Use o depurador para ver quais políticas são avaliadas quando um solicitante tenta acessar um módulo criptográfico e saiba a razão pela qual o acesso está sendo concedido ou não.

Este fluxograma mostra como sua instância avalia as solicitações de acesso a um módulo criptográfico.



Como controlar o acesso aos logs de depuração

O acesso aos logs de depuração de acesso ao módulo é determinado pela sua função. Usuários com as funções *sn_kmf.admin* e *sn_kmf.cryptographic_manager* sempre têm acesso ao depurador. Conceda acesso a outras funções usando a propriedade *glide.kmf.module_access_policies.debugger.authorized.roles* do sistema. O valor desta propriedade é uma lista com funções, separadas por vírgulas, que acessam os logs de depuração.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Como habilitar ou desabilitar o depurador

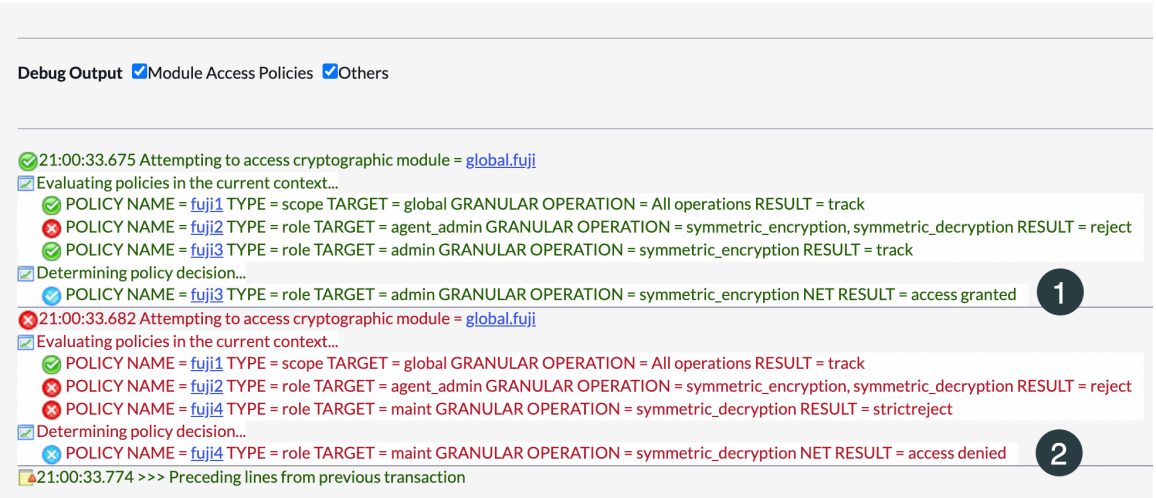
Para habilitar o registro em log de mensagens de depuração para políticas de acesso ao módulo, navegue até **"Todos"** > **"Diagnóstico"** > **"Depuração de sessão"** > **"Políticas de acesso ao módulo de depuração"** > **.**

Quando terminar a depuração, você poderá desabilitar as mensagens de registro em log navegando até **"Todos"** > **"Diagnóstico"** > **"Depuração de sessão"** > **"Desabilitar tudo"** > **.**

Como acessar of logs

Depois de habilitar a depuração, navegue até uma página que aciona uma avaliação de MAP para exibir os logs de depuração de MAP. As mensagens de depuração aparecem na parte inferior da página.

Dica: Você pode usar a representação para solucionar problemas de acesso de outros usuários. Para obter mais detalhes sobre a representação, consulte Representação de usuários. Para exibir os logs de depuração a partir da perspectiva de outro usuário, certifique-se de que suas políticas de acesso ao módulo com o tipo `role` tenham o campo **Representação** definido como **true (verdadeiro)**.



Neste exemplo, um solicitante faz duas solicitações de acesso ao módulo criptográfico `global.fuji`. Uma criptografia simétrica que é concedida, e uma descriptografia simétrica que foi negada.

Noções básicas sobre entradas no log

As informações de depuração são estruturadas da seguinte forma.

1. Esta primeira linha exibe o módulo criptográfico que está recebendo a solicitação de acesso.
2. As linhas entre a primeira e a última linha exibem os MAPs na ordem em que foram avaliados e incluem nome, tipo, meta, operação granular e resultado.
3. A última linha exibe a Policy Decision (decisão de diretrizes) (se aplicável) e o resultado do acesso à rede para o solicitante (se o solicitante foi concedido acesso).

Cada linha começa com um ícone que indica seu tipo de mensagem.

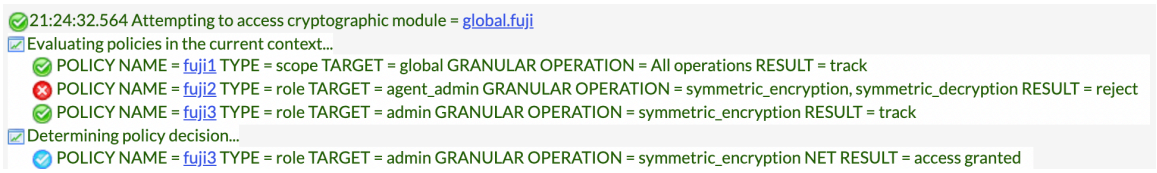
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Ícones de mensagens

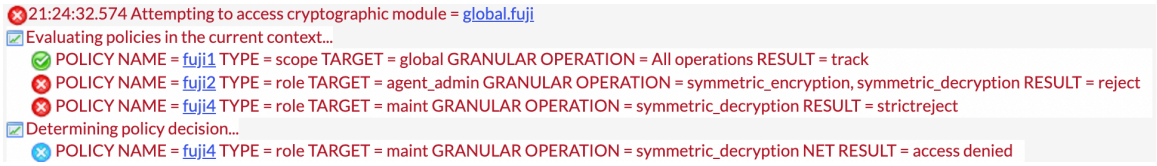
Ícone	Tipo de mensagem
	Mensagem informativa
	A política de acesso ao módulo concede acesso
	A política de acesso ao módulo nega acesso
	O solicitante tem acesso concedido
	O solicitante tem acesso negado
	Sem política de acesso ao módulo para avaliação

Exemplos de logs de depuração

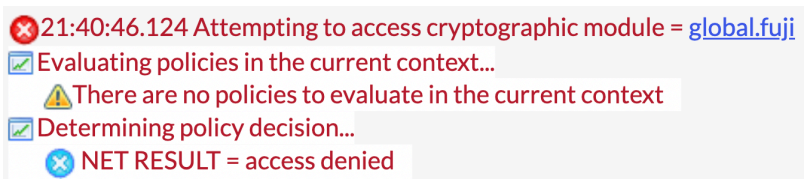
Mensagem de acesso concedido



Mensagem de acesso negado



Acesso negado (Sem política de acesso ao módulo para avaliação



Acesso negado (falta de permissão)

Crie uma política de ciclo de vida de módulo criptográfico

Crie uma política de ciclo de vida do módulo criptográfico para impor limites aos módulos criptográficos, como por quanto tempo a chave é válida. Crie políticas para proteger módulos criptográficos, limitando sua exposição.

Antes de Iniciar

Função necessária: sn_kmf.cryptographic_manager

Por Que e Quando Desempenhar Esta Tarefa

Uma política de ciclo de vida do módulo criptográfico é uma política de nível de instância. Quanto mais exposição uma chave criptográfica tiver, maior será a probabilidade de ela ser comprometida. Proteja as chaves limitando por quanto tempo elas podem ser usadas e quem pode usá-las.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Os seguintes recursos regem os módulos criptográficos:

- As políticas de instância definem limites para a instância. Por exemplo, se você especificar na política da instância que a data de expiração nunca deve ser superior a dois anos após a data de ativação, você não poderá usar as regras de ciclo de vida para definir uma data de expiração cinco anos após a data de ativação.

- Os modelos de ciclo de vida da instância permitem que a definição de políticas diferentes para chaves diferentes. Os modelos oferecem regras de ciclo de vida padrão para módulos criptográficos a fim de que elas não precisem ser recriadas para cada módulo. Por exemplo, é possível definir datas de expiração diferentes para chaves de criptografia de dados simétrica e para chaves públicas.

- As regras de ciclo de vida afetam diretamente as chaves. Por exemplo, se você especificar nas regras do ciclo de vida que a data de expiração deve ser dois anos após a data de ativação, as chaves vão expirar dois anos após a data de ativação.

Procedimento

1. Navegue até **Todos** > **Gerenciamento de chaves** > **Políticas de ciclo de vida** > **Políticas de instância**.
2. Selecione **Novo**.
3. Preencha o formulário.

   Campos das Políticas de ciclo de vida criptográfico

Campo	Descrição
Aplica-se a	Somente leitura. A chave à qual o ciclo de vida se aplica.
Ativo	Selecione para ativar a política.
Condição de política	Declarações de condições que especificam quando ativar, renovar, desativar e destruir o módulo criptográfico.
Resultado	**Rejeitar** para revogar o acesso ao módulo criptográfico ou **Rastrear** para permitir o acesso e monitorar o uso do módulo criptográfico.

O que Fazer Depois

Se quiser adicionar exceções a essa política de ciclo de vida em nível do módulo, consulte Criação de exceções às políticas de ciclo de vida do módulo.

Criação de exceções às políticas de ciclo de vida do módulo

Crie uma exceção da política do módulo para mudar a política de ciclo de vida de uma chave no nível do módulo de uma instância. As exceções se aplicarão somente a esse módulo e não à instância inteira. Por exemplo, se o administrador configurou em um ano a limitação de chaves simétricas no nível de instância, pode ser criada uma exceção no nível do módulo para que ela seja de dois anos.

Antes de Iniciar

Função necessária: sn_kmf.cryptographic_manager e sn_kmf.admin

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegue até **Todos** > **Gerenciamento de chaves** > **Módulos criptográficos Todos**.
2. Selecione o módulo criptográfico que usará as exceções de política.
3. Na tabela Módulo criptográfico, selecione a guia **Exceções às políticas do módulo** .
4. Clique em **Novo**.
5. Preencha o formulário.

Campos das Exceções às políticas do módulo

Campo	Descrição
Módulo de criptografia	Somente leitura, nome do módulo selecionado.
Aplica-se a	A chave especificada é preenchida automaticamente.
Tipo de chave	Selecione o tipo de chave, já que as políticas de exceção estão relacionadas a uma chave específica. Podem ser criadas várias políticas de exceção por módulo criptográfico.
Condição de política	Escolha as condições de qualificação no menu suspenso e preencha os critérios de restrição adicionais.
Novos critérios	Selecione condições de política adicionais, conforme necessário.
Resultado	Selecione **Rejeitar** para rejeitar o uso da chave ou **Rastrear** para permitir seu uso quando os critérios forem atendidos.

6. Clique em **Enviar** para retornar à tabela do Módulo criptográfico.

Ações de gerenciamento de chave

Um dos principais recursos do KMF é fornecer a capacidade de gerenciar chaves, como revogar ou girar chaves. A KMF protege corretamente os dados confidenciais com os materiais de criptografia e as operações de ciclo de vida mais atualizados.

A tabela a seguir fornece um resumo das principais operações de ciclo de vida e ações de gerenciamento. A finalidade do módulo criptográfico foi aplicada aos dados com a configuração do módulo criptográfico e não tem impacto nos dados.

Ação de gerenciamento de chave	Descrição
Gerar chave	Gera uma nova chave para o módulo criptográfico determinado. A primeira chave gerada será definida como *ativa*.
Girar chave	Desativa a chave atual e gera uma nova. A nova chave do módulo será definida como atual (ativa).
Revogar chave	Marca a chave atual e o estado do ciclo de vida como revogados. O módulo criptográfico gera automaticamente uma nova chave sobre novos dados e define o status da chave como ativo. Revogar significa que a chave não será mais usada para criptografia. No entanto, ela ainda pode ser usada para descriptografia. Não é possível destruir uma chave.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Ação de gerenciamento de chave	Descrição
Suspender chave	Marca a chave atual como suspensa. Retome manualmente a chave suspensa ou revogue-a para gerar uma nova chave de módulo antes de usar o módulo criptográfico novamente.
Retomar chave	Marca uma chave suspensa como a chave ativa.
Renovar chave	Estende a vida útil da chave atual. O botão **Renovar** fica disponível nas seguintes circunstâncias: • Você recebeu a função de gerente de criptografia. • O estado do ciclo de vida foi marcado como **Ativo** ou **Renovado**. • Uma data de expiração foi definida na definição de ciclo de vida do módulo.

Exibição e gerenciamento de chaves

Analise o status de qualquer chave para determinar outras ações de chave, como quando renovar, girar, suspender, desativar ou destruir uma chave atual.

Antes de Iniciar

Função necessária: sn_kmf.cryptographic_manager

Procedimento

1. Navegue até **Todos** > **Gerenciamento de chaves** > **Módulos criptográficos** > **Todos** .
2. Selecione um módulo criptográfico

   O formulário de Módulo criptográfico <module-name> aparecerá.
3. Na guia Chaves do módulo, clique no alias da chave para revisar o status da chave no formulário de ciclo de vida <key name>.
4. Revise o formulário, já que todos os campos são somente leitura.

Campos de chaves de ciclo de vida criptográfico

Campo	Descrição
Data de geração	Exibe a data em que a chave foi gerada.
Data de ativação	Exibe a data em que a chave foi ativada.
Data da última renovação	Exibe a data em que a chave foi renovada.
Data da última rotação	Exibe a data em que a chave foi girada.
Data de desativação	Exibe a data em que a chave foi desativada.
Data de destruição	Exibe a data em que a chave foi destruída.
Estado de ciclo de vida da chave	Exibe o estado do ciclo de vida da chave.
Data de ativação futura	Exibe a data de ativação futura da chave.
Data de renovação futura	Exibe a data de renovação futura da chave.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Data de rotação futura	Exibe a data futura da rotação da chave.
Data de destruição futura	Exibe a data futura em que a chave será destruída.
Data de vencimento	Exibe a data de expiração da chave.

5. Para executar uma ação na chave, clique em uma das seguintes opções para que entrem em vigor imediatamente:
   - **Revogar chave** : selecione para desativar a chave e gerar uma nova chave. Insira o motivo pelo qual você está revogando a chave.
   - **Girar chave** : selecione para desativar a chave atual e gerar uma nova chave como substituição. A nova chave será listada na tabela Chave do módulo e o número da Versão da chave será aumentado em 1. Consulte para obter detalhes.
   - **Suspender chave** : selecione para desativar a chave atual.
   - **Retomar chave**: selecione para marcar uma chave suspensa como chave ativa. Essa opção só ficará disponível depois que a chave ativa for suspensa.

Girar chaves

Para aumentar a segurança, você pode girar suas chaves criptográficas em uma programação pré-determinada. A rotação de chave acontece quando você descontinua uma chave de criptografia e substitui a chave antiga por meio da geração de uma nova chave criptográfica.

Antes de Iniciar

Função necessária: sn_kmf.cryptographic_manager

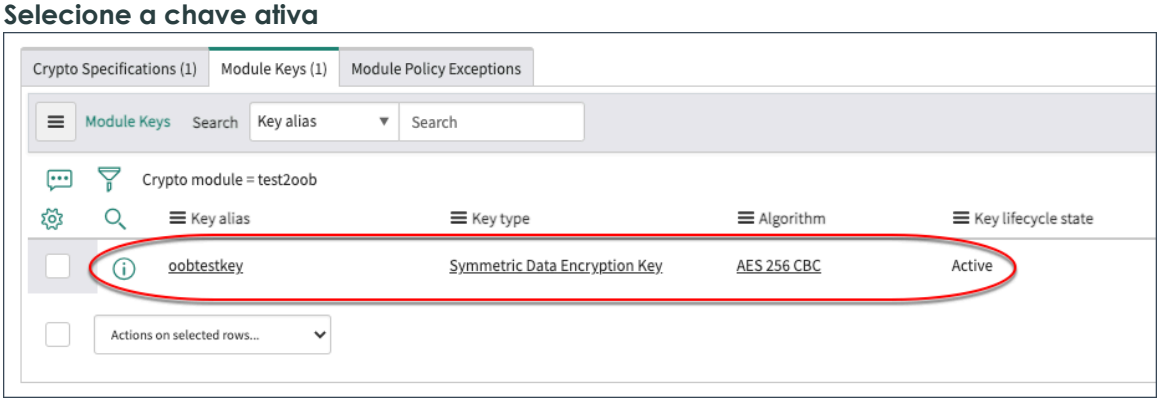
Por Que e Quando Desempenhar Esta Tarefa

Os módulos de criptografia, ao contrário dos contextos de criptografia, oferecem suporte a uma recodificação de registros para nova criptografia com uma nova chave. Abaixo demonstramos como executar manualmente uma operação de rotação de chave em um módulo criptográfico.

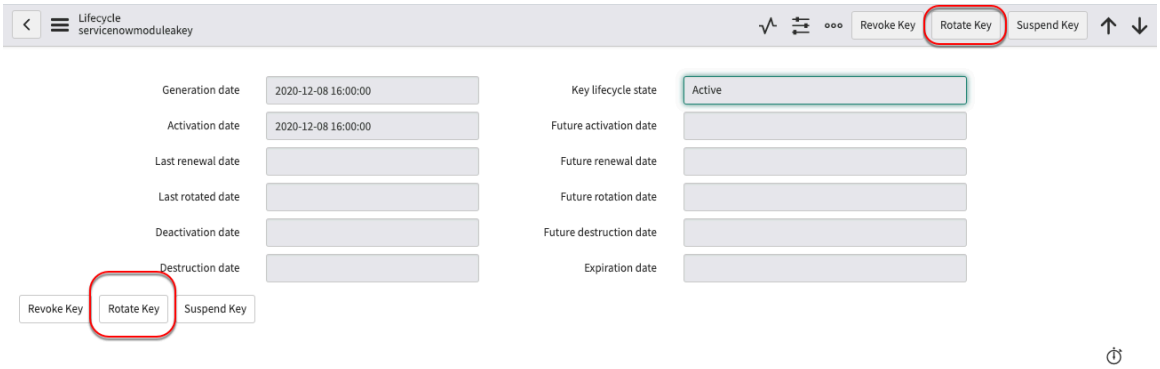
Procedimento

1. Navegue até **Gerenciamento de chave** > **Módulos criptográficos** > **Todos**.
2. Selecione o módulo criptográfico em que se realizará a rotação de chave.
3. Na guia **Chaves do módulo**, selecione a chave Ativa.

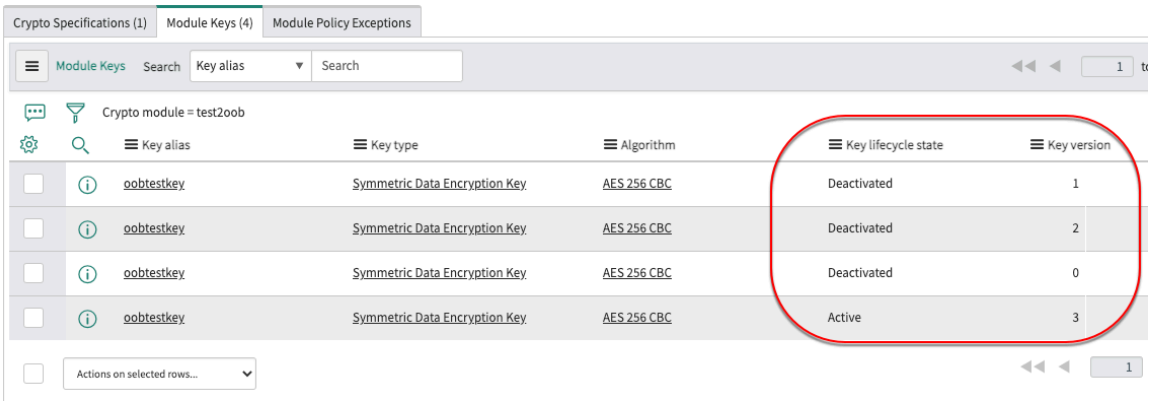
Selecione a chave ativa



© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Selecione **Girar chave**.
   O estado do ciclo de vida da chave mudará para "Desativado". Os campos **Data da última rotação**, **Data da desativação** e **Versão da chave** são atualizados.
5. Retorne a **Módulo criptográfico** > **Chaves do módulo**.



Há uma chave de módulo extra listada na tabela. A chave recém-girada se torna "Ativa" e a última chave é "Desativada".

Importação de uma chave do serviço web

Carregue com segurança uma chave de cliente externa em sua instância usando a importação de uma chave de um serviço web (por exemplo, a REST API chave). As chaves públicas simétricas e assimétricas podem ser importadas para um módulo criptográfico de destino do KMF.

A chave a ser importada (a chave de destino) deve ser criptografada com uma chave de encapsulamento antes de ser carregada no módulo criptográfico de destino da instância. Essa chave de encapsulamento é o componente público de um par de chaves pública/privada, que precisa estar presente na instância. A chave é um pré-requisito antes que a chave de destino encapsulada possa ser carregada por meio de Importar de serviços da Web.

Esses dois procedimentos separados (importar o par de chaves agrupadas e importar a chave de destino agrupada do serviço web) são detalhados na documentação abaixo. Esse par de chaves deve ser gerado e carregado para ficar disponível no módulo criptográfico de Importar chave interno da instância.

Nota: Esse exemplo usa o OpenSSL para a geração de chave e certificado e a ferramenta de teste Postman API para mostrar o uso da API REST. Substitua-os por outras ferramentas comparáveis com base nos requisitos da sua empresa.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Importação do par de chaves de encapsulamento/desencapsulamento

Defina as configurações de importação do Estrutura de gestão principal antes de importar uma chave.

Antes de Iniciar

Função necessária: sn_kmf.cryptographic_manager

Por Que e Quando Desempenhar Esta Tarefa

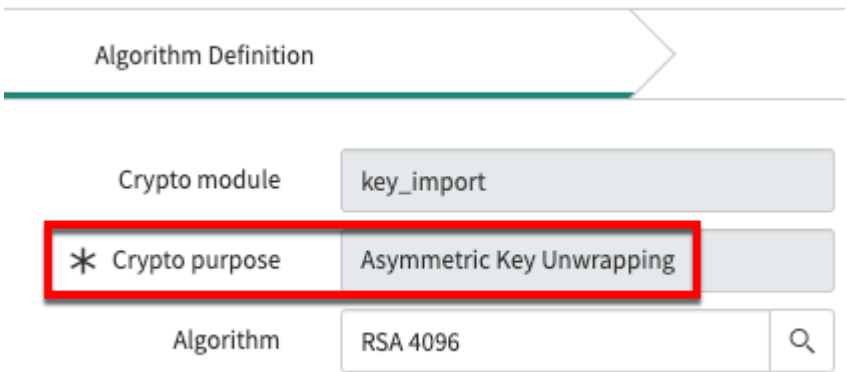
Este exemplo usa o OpenSSL para geração da chave e do certificado. Substitua-os por outras ferramentas comparáveis com base nos requisitos da sua empresa.

Procedimento

1. Em seu ambiente local, use o terminal para criar um certificado.
   Por exemplo: `openssl req -x509 -sha256 -nodes -days 365 -newkey rsa:4096 -keyout wrapping_private.key -out wrapping_public.crt`

   Este certificado é um componente público que contém uma chave. O certificado é usado para encapsular a chave simétrica do AES.

2. Em seu ambiente local, use o terminal para criar um armazenamento de chaves contendo o certificado público (com a chave de encapsulamento) e a chave de desencapsulamento privada.
   Por exemplo: `openssl pkcs12 -export -in wrapping_public.crt -inkey wrapping_private.key -name "wrapping_key_alias" -out wrapping_keystore.p12`
3. Na sua instância, navegue até **Todos** > **Gerenciamento de chaves** > **Configurações de importação** > **Configurações de importação de chaves**.
4. Na seção Definição de algoritmo, verifique se a **Finalidade da criptografia** está definida como *Desencapsulamento de chave assimétrica*.



5. Selecione um algoritmo apropriado que se alinhe com o material da chave assimétrica do armazenamento de chaves importado.
   Consulte Finalidade criptográfica, algoritmos e informações de chave para obter informações adicionais.
6. Selecione **Avançar**.
7. Na seção **Definição do ciclo de vida**, clique em **Avançar** para continuar.
8. Na seção **Origem da chave**, selecione **Importar do PKCS12** ou **Importar do BCFKS** no campo **Origem**.

   Nota: Se estiver usando o armazenamento de chaves de exemplo da etapa 1, selecione **Importar de PKCS12**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

9. Insira um **Alias de chave** para identificar a chave.
   Esse alias deve corresponder ao alias de chave (ou "nome amigável") que foi especificado ao gerar o certificado ou o armazenamento de chaves a ser carregado. Continuando o exemplo acima, seria `wrap_key_alias`.
10. Selecione **Avançar**.
    A seção **Criação de chave** inclui um link **Importar chave**, que exibe uma caixa de diálogo para carregar o armazenamento de chaves. Continuando o exemplo, seria `wrapping_keystore.p12`.

Importar uma chave encapsulada do serviço da Web

Carregue sua chave encapsulada em um módulo criptográfico usando a chave de importação da funcionalidade de Serviço da web. O exemplo usa uma chave simétrica. Etapas semelhantes podem ser usadas para importar uma chave assimétrica.

Antes de Iniciar

Funções necessárias: sn_kmf.cryptographic_manager (configuração do módulo), sn_kmf.cryptographic_operator (autenticação básica da operação REST)

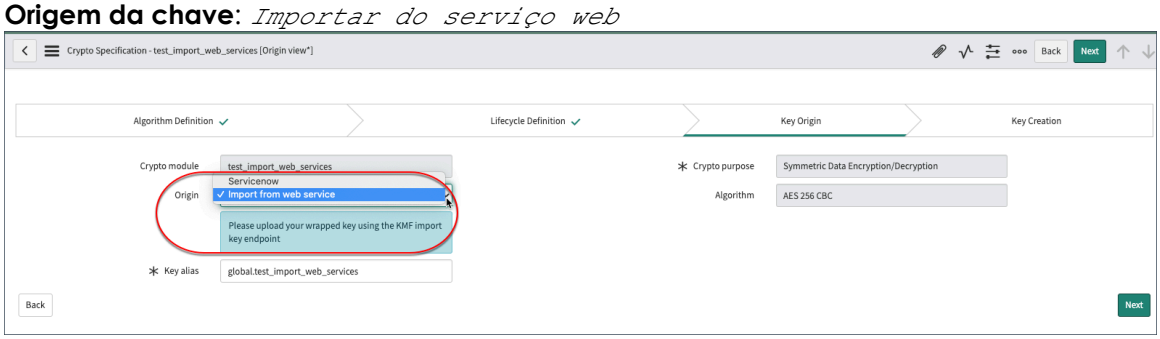
Por Que e Quando Desempenhar Esta Tarefa

KMF A importação do acesso de endpoint da chave é necessária para concluir o processo de importação da chave.

Este exemplo usa o OpenSSL para gerar chaves e certificados. Você pode substitui-lo por outras ferramentas comparáveis com base nos seus requisitos.

Procedimento

1. Usando o terminal no seu dispositivo local, encapsule sua chave simétrica usando a chave de encapsulamento de chave pública do módulo Importação de chave.
   Por exemplo: `openssl pkeyutl -encrypt -pubin -inkey public_wrapping_key.pem -in symmetric_key.bin -pkeyopt rsa_padding_mode:oaep -pkeyopt rsa_oaep_md:sha256 -out wrapped_symmetric_key.txt`
   Este exemplo cria um arquivo de chave encapsulado chamado `wrapped_symmetric_key.txt`.
2. Crie um módulo criptográfico para ser vinculado à API.
   Consulte ou para obter informações adicionais.
3. Adicione uma especificação criptográfica com as seguintes seleções.
   - **Objetivo da criptografia**: *`Criptografia/descriptografia simétrica de dados`*.
   - **Origem da chave**: *`Importar do serviço web`*



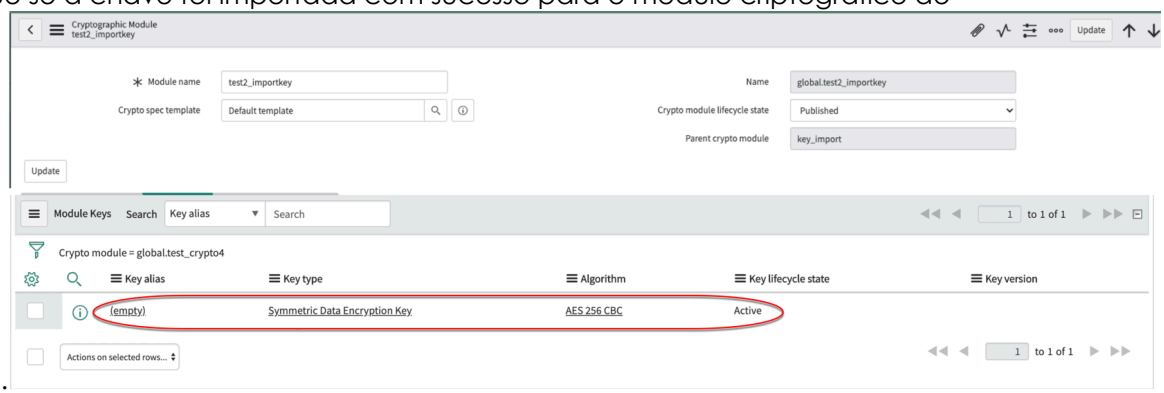
   Consulte ou para mais informações.
4. Execute uma *`solicitação HTTP POST`*para a importação do endpoint REST do serviço web.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Valor/formato
URL do endpoint	*https://<instance>/api/sn_kmf/key/import?cryptoSpecSysID=<sys_id_of_crypto_spec>*.
Parâmetro CryptoSpecSysID	O *sys_id* da especificação de criptografia recém-criada. **Dica:** Clique com o botão direito do mouse no cabeçalho da especificação criptográfica para copiar o *sys_id*.
Tipo de conteúdo do cabeçalho	Aplicação/fluxo de octeto.
Corpo	Deve conter um arquivo anexo-binário e a chave pública a ser importada (wrapped_sensitive_key.txt).
Importar do endpoint REST do serviço web	Usa autenticação básica de *<username/password>* **Nota:** Certifique-se de que o usuário designado tenha a função sn_kmf_cryptographic_operator.

A importação bem-sucedida da chave pública resulta em uma mensagem de resposta HTTP com *Status 200*.

5. Verifique se a chave foi importada com sucesso para o módulo criptográfico de destino.



Integridade do Key Management Framework

Acesse informações sobre o estado de integridade doEstrutura de gestão principal sob demanda. Os erros de advertência e de avarias contêm uma mensagem detalhada.

Antes de Iniciar

Função necessária: sn_kmf_cryptographic auditor ou sn_kmf_admin or sn_kmf_cryptographic_manager

Por Que e Quando Desempenhar Esta Tarefa

Cada componente do Estrutura de gestão principal é descrito e relata os seguintes status e cores:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Verde/operacional: o componente está operacional, nenhum erro a ser relatado.
- Cinza/desativado: o componente está inativo, portanto, nenhuma verificação de integridade foi realizada.
- Amarelo/degradado: advertência. O componente está funcionando, mas é provável que ocorram atrasos ou problemas transitórios.
- Vermelho/avaria: um erro fatal está impedindo o funcionamento do componente, o que provavelmente causará indisponibilidades parciais.

Os componentes podem incluir relatórios individuais de subcomponentes cujo próprio estado de integridade afeta o primário da seguinte forma:

- Se todos os subcomponentes estiverem inativos, o primário será exibido como inativo. Os subcomponentes inativos não afetam a integridade dos primários.
- Se um ou mais subcomponentes estiverem degradados ou com defeito, a integridade do primário será mostrada como degradada.
- Se todos os subcomponentes forem relatados como com avarias, o primário também será relatado como avariado.

Para obter informações adicionais sobre subcomponentes, consulte Chaves de nível de instância na estrutura de gerenciamento de chave.

Nota: As verificações de integridade são executadas a cada 15 segundos. Atualize a página de integridade para executar novamente o relatório.

Procedimento

1. Navegue até **Todos** > **Key Management** > > **Diagnóstico**.
2. Analise as seguintes informações sobre o estado de integridade:

Informações de diagnóstico

Categoria	Detalhes
Chave protegida	Verifica se há uma tentativa de criptografia.
Armazenamento de chaves de arquivo	Verifica se uma tentativa de obtenção de chave raiz de instância (IRK) está ocorrendo. **Nota:** O armazenamento de chave de arquivo é uma alternativa off-line ao Key Secure usada para instâncias no local e instâncias de desenvolvedor.
GlideEncrypter	Verifica se um módulo de criptografia no nível de instância do GlideEncrypter, uma especificação e uma chave estão presentes. **Nota:** O GlideEncrypter é um componente programável que permite a criptografia transparente de campos Password2 e outros usos de criptografia legados por meio do Estrutura de gestão principal.
Chave de criptografia	Verifica se a chave pode ser obtida no armazenamento de chaves de arquivo ou KeySecure.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Categoria	Detalhes
da chave de instância (IKEK)	
Chave HMAC da instância	Verifica se a chave pode ser obtida no armazenamento de chaves de arquivo ou KeySecure.
PKI do Vault	Verifica a conectividade do Vault para verificar se a chave de criptografia assimétrica da instância (IAEK) e a chave de assinatura da instância (ISK) são utilizáveis e podem ser obtidas no Vault.
EJBCA PKI	Verifica a conectividade LDAP para verificar se IAEK e ISK podem ser obtidos no cache e no LDAP.
PKI de instância	Verifica o armazenamento de chaves do arquivo e o KeySecure se a chave pode ser obtida e se o certificado está presente e corresponde à chave simétrica. **Nota:** A PKI da instância está disponível somente em instâncias no datacenter ServiceNow.

Para obter assistência na solução de problemas, entre em contato com Suporte e atendimento ao cliente.

Preparação da sua instância para descontinuação de GlideEncrypter

Use um script de verificação de instância para encontrar e remover chamadas de API GlideEncrypter em sua instância. A remoção dessas chamadas se faz necessária para descontinuar a criptografia 3DES da sua instância.

Antes de Iniciar

Função necessária: administrador

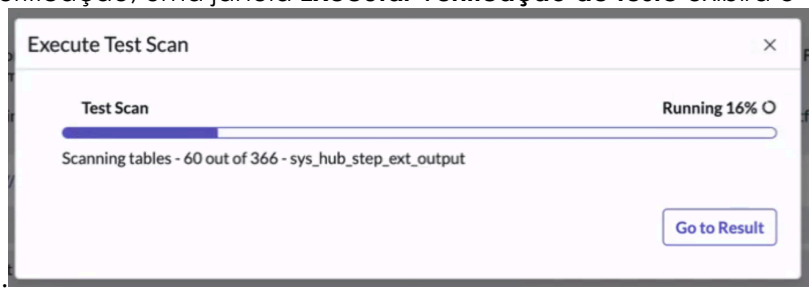
A API do GlideEncrypter está planejada para descontinuação a partir da versão Zurich de ServiceNow. Remover as chamadas GlideEncrypter do seu script também é necessário para descontinuar a criptografia 3DES da sua instância.

Procedimento

1. Navegue até **"Todos"** > **"Verificação de instância"** > **"Pacotes"**.
2. Na lista **Pacotes**, selecione **GlideEncrypter para identificar os registros com usos do GlideEncrypter**
3. No registro **Pacotes**, selecione **GlideEncrypter para identificar os registros com usos do GlideEncrypter** na lista relacionada **Verificações**.
   A **Verificação do tipo de coluna** será exibida. Esse registro contém uma descrição da verificação e links com informações sobre como atualizar os registros encontrados pela verificação.
4. No registro de **"Verificação de tipo de coluna"**, selecione **"Testar verificação"** para executar a verificação.

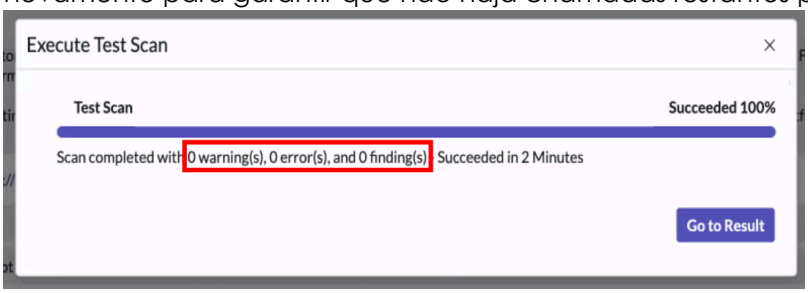
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Durante a verificação, uma janela **Executar verificação de teste** exibirá o andamento.



Nota: Isso irá verificar somente os registros que foram criados ou modificados pelo cliente.

5. Quando a verificação estiver concluída, selecione **"Ir para resultado"** para exibir o registro do **Resultado da verificação**.
   No registro do **Resultado da verificação**, a lista de **Descobertas da verificação** exibirá uma lista de registros da sua instância que estão usando a API **GlideEncrypter**.
6. Selecione o campo **"Contagem"** na lista **"Descobertas da verificação"** para navegar até um registro.
7. Modifique todos os scripts no registro que usem a API **GlideEncrypter**.
   Para obter mais detalhes sobre alternativas ao **GlideEncrypter**, consulte Alternativas às APIs GlideEncrypter descontinuadas.
8. Depois de remover as chamadas do **GlideEncrypter** de seus scripts, execute a verificação novamente para garantir que não haja chamadas restantes para a API.



O que Fazer Depois

Descontinuar o uso do GlideEncrypter do 3DES para campos Password2

Descontinuar o uso do GlideEncrypter do 3DES para campos Password2

Descontinue o uso do GlideEncrypter do padrão de criptografia 3DES na instância para que ela use o AES (Advanced Encryption Standard, padrão de criptografia avançada) mais seguro exclusivamente para a criptografia e a descriptografia dos dados do Password2.

A partir da versão Rome, os dados do password2 passaram a ser protegidos usando o Estrutura de gestão principal, que conta com um algoritmo AES (Advanced Encryption Standard) mais moderno. No entanto, algumas configurações e falhas na lógica do password2 ainda podem fazer com que o algoritmo 3DES seja usado para criptografia e descriptografia.

Na versão Vancouver, os administradores podem optar por descontinuar totalmente o algoritmo 3DES. Com essa mudança, sua instância irá usar exclusivamente a criptografia AES para todas as tarefas de criptografia e descriptografia relacionadas aos dados do Password2. Essa mudança oferece melhor segurança da instância em comparação com a criptografia 3DES e é necessária para permanecer em conformidade com o NIST.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Considerações antes da descontinuação

Transferência de dados do password2 entre instâncias

Ao transferir textos criptografados do password2 para outras instâncias, certifique-se de que o KMF Key Exchange esteja habilitado entre as instâncias de origem e de destino. Essa configuração garante que as chaves usadas para criptografar textos do password2 estejam disponíveis em ambas as instâncias para descriptografar os textos criptografados pelo password2. Antes de descontinuar o 3DES, leve em consideração os seguintes casos de uso que podem afetar a transferência de dados do Password2 entre instâncias.

- Se você tiver aplicações em sua instância que usam dados do password2, certifique-se de que o KMF Resource Exchange esteja instalado nessa instância. KMF Resource Exchange garante que as chaves de nível de instância usadas para criptografar os dados do password2 na instância de origem estejam disponíveis nas instâncias de destino para descriptografia. Para obter mais informações, consulte Troca de recursos do Key Management Framework.
- Se você planeja exportar dados do password2 usando XML ou Fontes de dados, certifique-se de que KMF Key Exchange esteja habilitado na instância de destino. Esta configuração garante que as chaves de nível de instância usadas para criptografar os dados do password2 na instância de origem estejam disponíveis nas instâncias de destino para descriptografia. Para mais detalhes sobre a configuração, consulte Troca de chaves da Key Management Framework.

> **Importante:** Os exemplos acima representam os cenários mais comuns, mas se você estiver fazendo a transferência de texto criptografado do password2 entre instâncias de outra forma, configure KMF Resource Exchange para garantir que a instância de destino possa descriptografar dados do password2.

Como fazer o downgrade de uma instância após a descontinuação do 3DES

Isso só se aplica a instâncias que têm campos do password2 com entradas maiores que 125 caracteres e cujo você já descontinuou a criptografia 3DES.

Antes de fazer o downgrade de uma instância para uma versão anterior a Vancouver usando a Instance Cloning (Clonagem de instância), realize as etapas a seguir antes de iniciar o clone.

1. Verifique se a preservação de dados está configurada para preservar os dados do campo do password2.
2. Em caso afirmativo, antes de solicitar o clone, entre em contato com o suporte de ServiceNow para desabilitar a descontinuidade do 3DES. No campo **"Motivo"**, use "Pré-requisito de downgrade de clone para suporte a password2".

Campos de password2 legados

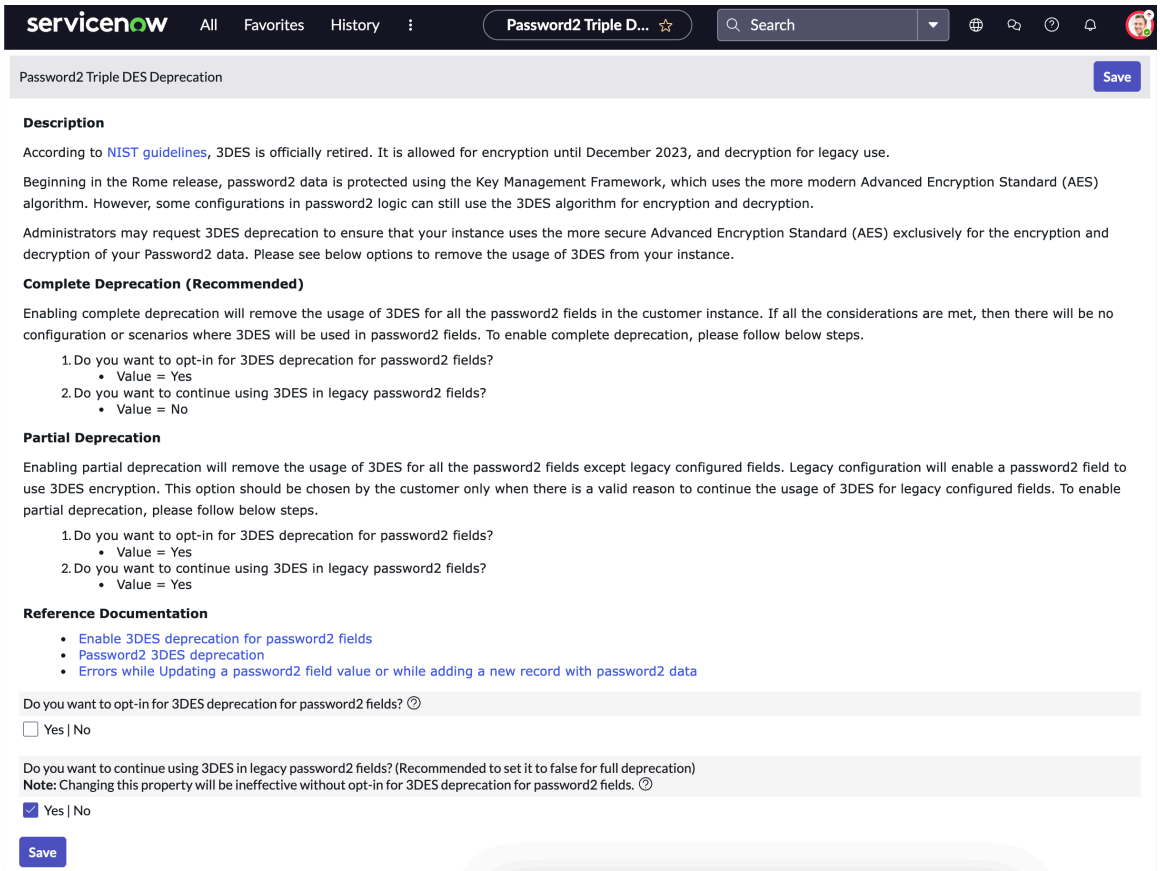
Sua instância usa a criptografia 3DES para converter dados do password2 em dados do password2 legados (pré-Rome). Depois de descontinuar a criptografia 3DES, essa opção não estará mais disponível. Se você ainda precisar desse recurso, solicite a descontinuação parcial (consulte os detalhes na próxima seção).

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Como descontinuar o 3DES

Depois de analisar os casos de uso anteriores, habilite a descontinuação parcial ou completa, dependendo das suas necessidades. Para qualquer uma das opções, você pode acessar o formulário para controlar a descontinuação navegando até **Todos** > **Segurança do sistema** > **Conformidade de segurança** > **Descontinuação do DES triplo para Password2**.

Importante: Você deve ser elevado a administrador de segurança para ver o módulo de **Conformidade de Segurança** e realizar essas etapas. Para obter detalhes sobre esse processo, consulte Elevação para uma função privilegiada.



O formulário de **Descontinuação de DES triplo para Password2** contém informações sobre o processo de descontinuação completa e parcial do 3DES. Selecione as opções para descontinuação completa ou parcial e selecione **Salvar**.

Descontinuação completa

Habilitar a descontinuação completa remove o uso de 3DES para todos os campos de password2 da sua instância. Se todos os pré-requisitos forem atingidos, não haverá configuração ou cenários em que o 3DES seja usado nos campos de password2.

Para permitir a descontinuação completa:

- Selecione **Deseja aceitar a descontinuação do 3DES para os campos Password2?**
- Desmarque **Deseja continuar usando o 3DES em campos Password2 legados?**

Descontinuação parcial

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Habilitar a descontinuação parcial remove o uso de 3DES para todos os campos de password2, exceto para os campos de configuração legada. Os campos de password2 de configuração legada irão continuar a usar a criptografia 3DES. Selecione esta opção somente quando você precisar continuar usando 3DES para campos de configuração legada.

Para permitir a descontinuação parcial:

- Selecione **Deseja aceitar a descontinuação do 3DES para os campos Password2?**
- Selecione **Deseja continuar usando o 3DES em campos Password2 legados?**

Após a descontinuação do GlideEncrypter

Após a conclusão da descontinuação, as informações a seguir serão aplicáveis à sua instância.

- Os campos password2 ainda oferecem suporte à descriptografia (mas não à criptografia) de dados criptografados do 3DES.
- Os dados criptografados do 3DES existentes nos campos de password2 permanecem como estão até que o valor do campo seja atualizado por um usuário ou fluxo de trabalho.
- Qualquer atualização do valor de um campo password2 remove o texto criptografado do 3DES e o substitui pelo texto criptografado de KMFusando AES.
- Em algumas situações, sua instância pode exibir um erro ao salvar dados de senhas:

  ```
  Ação anulada: o valor da senha não pode ser salvo devido a um problema técnico. Consulte KB1296997 para obter ajuda.
  ```

  Se você se deparar com esse erro, consulte as informações de suporte no artigo KB1296997 da base de conhecimento.

Troca de recursos do Key Management Framework

O ServiceNow® Resource Exchange é um recurso do KMF que oferece a capacidade de trocar recursos entre instâncias de maneira segura.

Terminologia

Ao usar o Resource Exchange, consulte a seguinte terminologia:

Resource Exchange Terminologia

Nome	Descrição
Resource Exchange	O processo para trocar recursos entre instâncias.
Key Exchange (KE)	O processo para trocar chaves em instâncias.
Instância de origem da chave (origem da chave)	A instância que possui as chaves.
Instância de destino da chave (destino da chave)	A instância que solicita as chaves.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Visão geral

O Resource Exchange utiliza as APIs criptográficas do KMF para fornecer confidencialidade, integridade, autenticação e não repúdio. Atualmente, o Resource Exchange oferece suporte à funcionalidade Key Exchange. Consulte Troca de chaves da Key Management Framework para obter informações adicionais.

Troca de chaves da Key Management Framework

O KMF Key Exchange é uma função de subconjunto do KMF Resource Exchange. O Key Exchange transfere com segurança dados criptografados em várias instâncias.

Visão geral do Key Exchange

O Key Exchange transfere chaves entre instâncias com segurança.

O KMF Key Exchange fornece uma maneira segura para os clientes trocarem chaves KMF entre instâncias. Um caso de uso de aplicação é o processo de clonagem de dados. Com o Key Exchange, as chaves do módulo de criptografia são copiadas durante a clonagem de dados de componentes do KMF. Módulos criptográficos, especificações de chave de módulo e políticas de acesso ao módulo estão incluídos no processo de clonagem. A transferência de chaves não está incluída.

Como usar Key Exchange

Os administradores que usam o KMF para criptografia no nível de coluna podem usar o Key Exchange para clonar as chaves entre instâncias de produção ao executar a clonagem de dados. Na clonagem de dados, o administrador/gerenciador de criptografia do KMF pode executar o seguinte:

- Trocar todas as chaves com as outras instâncias.
- Trocar chaves específicas uma vez ou periodicamente para a outra instância.
- Enviar solicitações sob demanda da instância de destino para a instância de origem da chave.
- Trocar chaves da origem para o destino para recriar a chave do texto cifrado.
  - Gerenciar o tempo de expiração da solicitação com a capacidade de excluir chaves ou rejeitar a solicitação de troca de chave se a solicitação tiver expirado.
  - Depois que a solicitação for concluída e a chave importada, a chave usada será definida como expirada com carimbo de data/hora.
  - Reinserir o texto cifrado na instância de destino que tenha sido criptografada com chaves da origem.

Modos compatíveis

O Key Exchange é compatível com vários modos no nível de especificação de criptografia do módulo de criptografia:

Modo	Descrição
Automático (sem configuração, comportamento padrão)	Todas as chaves são enviadas automaticamente durante o processo de clonagem de dados sem configuração adicional.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Modo	Descrição
Configurável (configuração única)	O administrador configura as chaves a serem enviadas durante o processo de clonagem de dados.
Manual (pessoa no circuito)	O administrador envia uma solicitação sob demanda na instância de destino para a origem. A solicitação deve ser aprovada por um administrador na instância de origem da chave.
Recriação de chave (solicitação automatizada)	O administrador seleciona a opção de recriação de chave durante o processo de configuração de clonagem.

Configurar troca de chaves

Estrutura de gestão principal (KMF) gera solicitações de troca de chave automáticas para módulos criptográficos compatíveis durante a nova instalação ou upgrade da instância. gerencia a chave de criptografia de dados localmente para a instância.

Antes de Iniciar

Um módulo criptográfico com uma chave deve ser criado nas instâncias de destino e de origem antes de usar o Key Exchange.

Função necessária: sn_kmf.cryptographic_manager

Por Que e Quando Desempenhar Esta Tarefa

As solicitações de Key Exchange são iniciadas a partir da instância de destino.

A troca automática de chaves fica ativa por padrão ao clonar uma instância em que a propriedade é clonada para a instância de destino. Com KMF, configure as propriedades do sistema para gerenciar como as chaves são tratadas durante um clone de instância:

- **Desativar a troca automática de chaves:** defina a propriedade *glide_encryption.auto_key_exchange.enabled* como **falsa** para solicitações de clonagem recorrentes.
- **Enviar solicitações de troca de chave automática**: defina esta propriedade como **verdadeira**.

> **Importante:** A propriedade do sistema de base é definida como **verdadeira** por padrão, o que significa que a troca automática de chave é ativada ao clonar uma instância. Este valor deve ser definido como **falso** se estiver usando Recriação de chave de texto cifrado com o Key Exchange ou a funcionalidade de troca de chave recorrente. Consulte Passo a passo para troca de chave recorrente para obter detalhes adicionais.

Procedimento

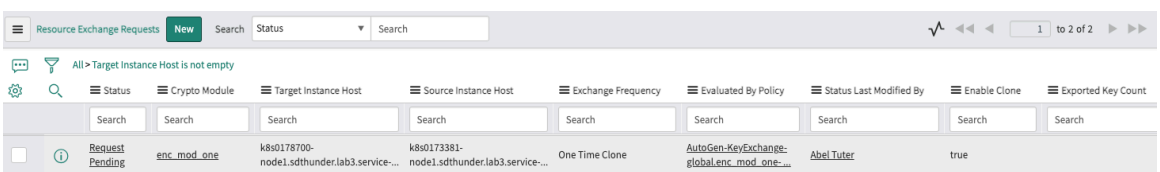
1. Navegue até **Todos** > **Gerenciamento de chave** > **Solicitações de troca de recursos** > **Nova**.
2. No formulário, preencha os campos.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resource Exchange Solicitar campos de formulário

Nome	Descrição
Frequência de troca	◦ **Adhoc**: envia solicitações da instância de destino da chave para a instância de origem. Insira o sys_id da instância e as informações do host da origem. Não compatível com a recriação de chave do Key Exchange. ◦ **Clone único**: troca única das chaves das especificações de criptografia da origem para a instância de destino. ◦ **Clone recorrente**: troca de chaves das especificações criptográficas de origem selecionadas para a instância de destino em um clone recorrente definido.
Instância <Source or Target> sys_id	◦ **Adhoc**: insira o sys_id da instância de origem para solicitar as chaves. ◦ **Clone único**, **clone recorrente**: insira o sys_id da instância de destino que envia as solicitações. **Dica:** Insira `stats.do` no navegador de aplicações para localizar o ID da instância.
Host da instância de <Source or Target>	Insira o local do host ou o nome da instância de origem ou de destino. **Dica:** Por exemplo, `instanceA.service-now.com`
Especificações de criptografia	As chaves da especificação de criptografia em um módulo de criptografia definem as chaves a serem clonadas. Para solicitações de clone únicas e recorrentes, sua instância cria automaticamente uma política de acesso ao módulo **Resource Exchange**. Não é necessário configurar uma política manualmente. **Nota:** Clique na busca usando o ícone de lista ( ) para procurar as especificações criptográficas disponíveis.
Habilitar rechaveamento após importação de chave	Opção para ativar a recriação de chaves automática.

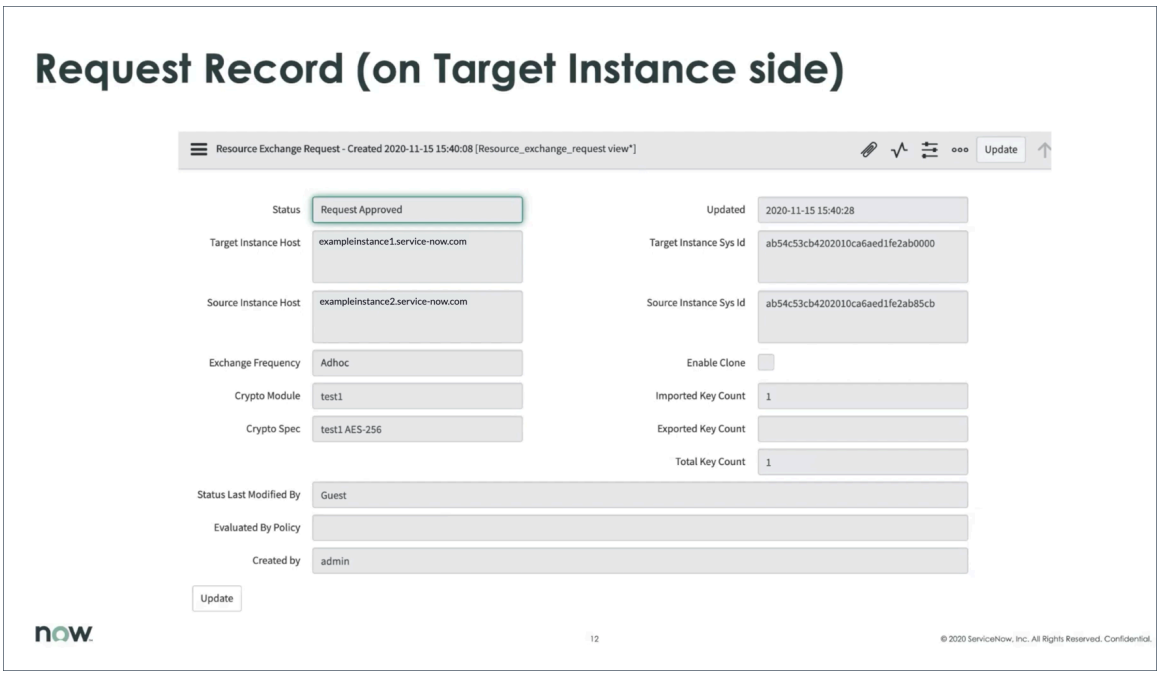
3. Selecione **Enviar**.
   Se for bem-sucedido, uma confirmação será exibida na parte superior do formulário. A tabela Solicitações será atualizada com uma entrada de **Solicitação Pendente** na instância de origem e na instância de destino. Abra o registro de solicitação para exibir o status da solicitação, a contagem de chaves importadas e a contagem total de chaves no host de destino ou de origem.



© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. A solicitação pendente é aceita na instância de origem para concluir a troca.

   No momento da clonagem, a política de acesso ao módulo na instância de origem é invocada para aprovar automaticamente a solicitação e enviar chaves para o destino recém-clonado.



Resultados
Depois de tentar uma troca de chave, sua instância de não produção atualiza a propriedade do sistema *`protected.script.values.kmf.rekeyed`*. Essa propriedade fica visível na tabela Propriedades do Sistema [sys_properties] após uma tentativa de troca de chaves. Se a criptografia que usa a chave trocada for bem-sucedida, esta propriedade terá como valor **verdadeiro**. Caso contrário, a propriedade terá como valor **falso**. Se o valor for falso, a instância tentará criptografar novamente no dia seguinte.

Recriação de chave de texto cifrado com o Key Exchange

O Resource Exchange oferece suporte à redigitação de texto cifrado na instância de destino que foi criptografada com chaves da origem. A atividade de rechaveamento é rastreada no ciclo de vida da chave.

Visão geral

Os administradores que usam o KMF para criptografia no nível de coluna podem usar o Key Exchange para recriar chaves criptográficas entre instâncias de produção ao executar a clonagem de dados. Primeiro, uma chave ativa deve estar disponível na instância de destino para recodificação, pois a recodificação requer uma chave ativa. Um trabalho de criptografia será criado automaticamente e executado pelo sistema para girar e recodificar a chave de origem e criptografar novamente o texto cifrado.

Use o Key Exchange para fazer o seguinte:

- Definir um intervalo de tempo de expiração para a recodificação.

  Se a solicitação tiver expirado, ela será rejeitada e a chave será excluída.

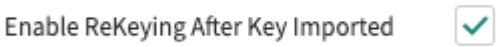
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Automatizar a recriação de chave de texto cifrado que foi criptografado com chaves de instâncias de origem.

  A nova chave de criptografia clonada é usada para criptografar novamente o texto cifrado na instância de destino.

- A finalidade de recriação de chave é configurada durante o processo de clonagem e será automatizada como parte do clone.
- A atividade de recriação de chave é acompanhada na guia **Chave de módulos** do módulo criptográfico. Acesse o estado do ciclo de vida da chave e a versão da chave da atividade. Consulte Girar chaves para obter informações adicionais.

Configure um Key Exchange e marque a caixa de seleção **Habilitar recriação de chave após importação da chave** para ativar. Consulte Configurar troca de chaves para obter detalhes.



Passo a passo para troca de chave recorrente

Use este passo a passo para configurar uma troca de chave recorrente na sua instância usando Resource Exchange.

Antes de Iniciar

Funções necessárias: sn_kmf.cryptographic_manager

Por Que e Quando Desempenhar Esta Tarefa

Este exemplo mostra como uma instância de destino solicita chaves de uma instância de host.

- Antes de executar este procedimento, é necessário clonar uma instância. Consulte Clone do sistema para obter mais informações.
- **Troca automática de chave**: a propriedade do sistema de base *glide_encryption.auto_key_exchange.enabled* é **verdadeira** por padrão, o que significa que a troca automática é ativada ao clonar uma instância. A propriedade é clonada para a instância de destino.
- Desative a troca automática definindo a propriedade como **falsa**.

Procedimento

1. Na instância de origem, crie um módulo de criptografia ou acesse um módulo de criptografia existente usando column_level_encryption e defina as configurações de campo criptografado para a criptografia de texto cifrado para Key Exchange. Consulte e para obter detalhes.

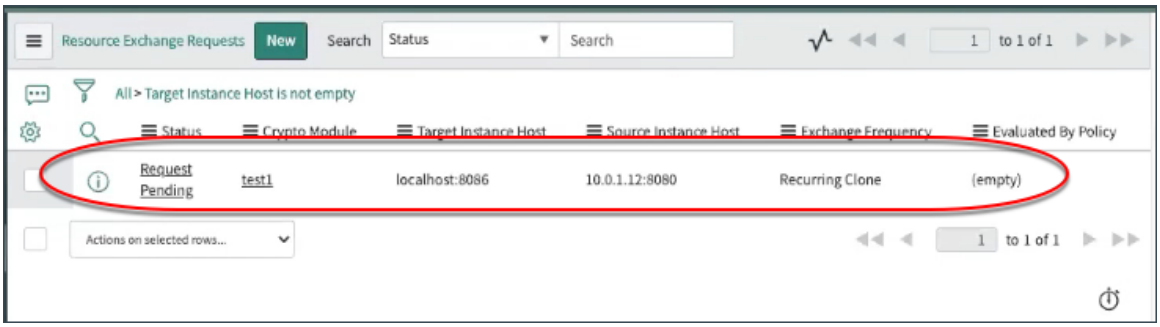
   a. Certifique-se de que as chaves foram geradas no módulo criptográfico.

   Nota: Sua instância cria automaticamente uma política de acesso ao módulo na execução da solicitação de clone.

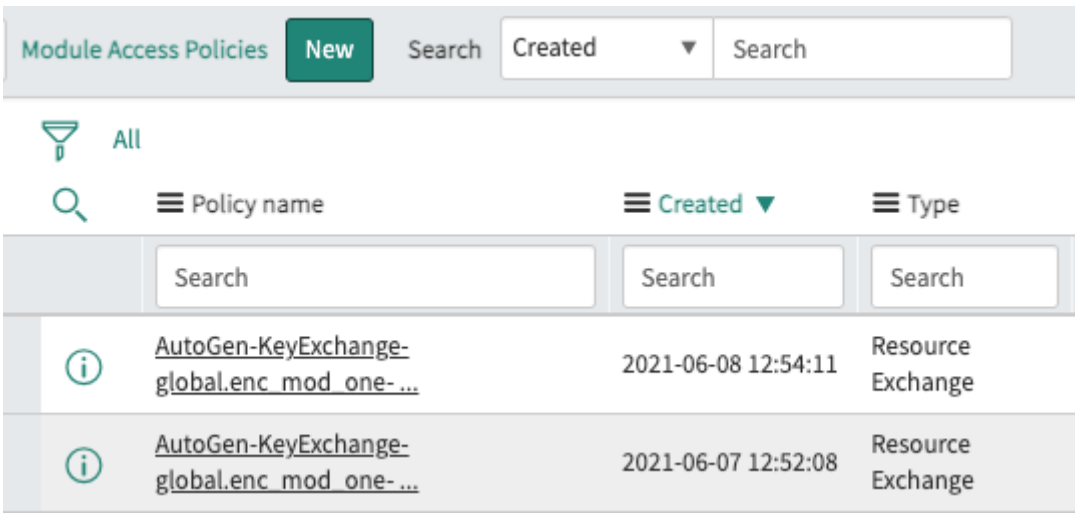
2. Na instância clonada, navegue até **Gerenciamento de chave** > **Solicitações da Troca de recurso** > **Nova**.
3. Preencha o formulário e selecione **Clone recorrente** como a Frequência de troca.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Na instância de destino do clone, navegue até **Gerenciamento de chave** > **Solicitações da Troca de recurso** .
   A solicitação da instância do host será exibida na tabela.

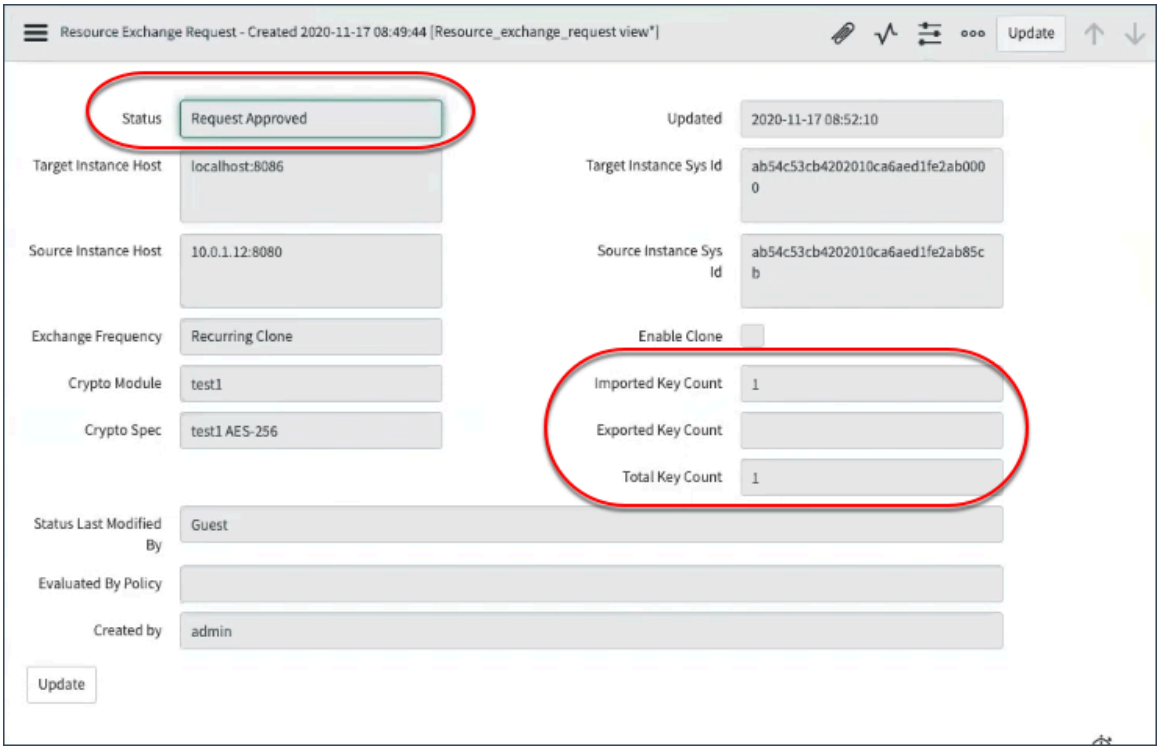


Importante: Para solicitações de clone únicas e recorrentes, sua instância cria automaticamente uma política de acesso ao módulo. Não é necessário configurar uma política manualmente. No momento da clonagem, essa política na instância de origem será invocada para aprovar automaticamente a solicitação e enviar chaves para o destino recém-clonado.

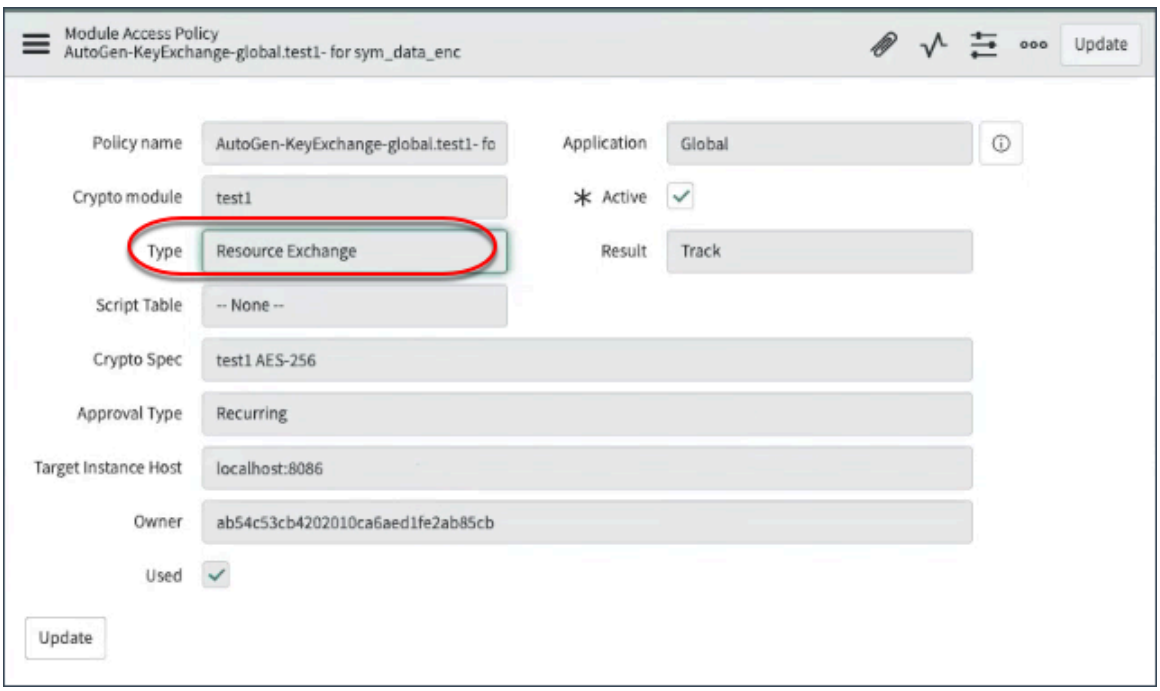


No Formulário de solicitações, o status será atualizado para **Solicitação aprovada** e o campo **Contagem de chaves importadas** aparecerá no registro.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Retorne à instância do host.
6. Exiba o registro de solicitação para ver o número de chaves exportadas.
7. Exiba o registro da Política de acesso ao módulo para conferir se o **Tipo** é Resource Exchange.



Nota: O Resource Exchange também oferece suporte à recriação de chaves de texto cifrado na instância de destino. Consulte para obter detalhes.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resultados
Depois de tentar uma troca de chave, sua instância de não produção atualiza a propriedade do sistema *protected.script.values.kmf.rekeyed*. Esta propriedade fica visível na tabela Propriedades do sistema [sys_properties]. Se a criptografia que usa a chave trocada for bem-sucedida, esta propriedade terá como valor **verdadeiro**. Caso contrário, a propriedade terá como valor **falso**. Se o valor for falso, sua instância tentará criptografar novamente no dia seguinte.

Segurança de infraestrutura

Use as ferramentas de segurança de infraestrutura para criar, carregar e gerenciar certificados usados pela sua instância para criptografar o tráfego do cliente para o servidor.

O plug-in de Segurança de Infraestrutura fornece as ferramentas para gerenciar as cifras de Segurança da Camada de Transporte (TLS) e os certificados. Sua instância usa TLS para criptografar o tráfego do cliente para o servidor.

Selecionar as cifras usadas em sua instância

Usando a **página de TLS**, os administradores podem configurar quais cifras de datacenter serão usadas em sua instância, bem como selecionar a ordem em elas são testadas.

Gere e carregue seus próprios certificados

Use as ferramentas de segurança de infraestrutura para gerar suas próprias solicitações de assinatura de certificado, que podem ser assinados pela autoridade de certificação de sua escolha. Em seguida, você pode usar as ferramentas para carregar o certificado assinado para o balanceador de carga da sua instância.

Monitore o status de suas cifras e certificados

Use as páginas **Configurações de TLS** e **Configurações de SYOC** para exibir o status das mudanças feitas em suas cifras e certificados.

Instale o plug-in de segurança de infraestrutura

Instale o plug-in do ServiceNow Configurações de segurança de infraestrutura (com.glide.infrastructure_security) para começar a usar esses recursos. Para obter detalhes sobre a ativação do plug-in, consulte Ativar um plug-in.

Depois de instalar o plug-in, habilite a funcionalidade Sign Your Own Security (SYOC) definindo a propriedade do sistema *sn_infra_sec.syoc.enabled* como `verdadeira`.

Nota: Se a propriedade *sn_infra_sec.syoc.enabled* não estiver disponível na sua instância, você deverá criá-la. Para detalhes sobre este processo, consulte Adicionar uma propriedade do sistema.

Gerar uma solicitação de assinatura de certificado

Use a página Gerar assinatura de certificado (CSR) para criar uma solicitação de assinatura de certificado e oferecer suporte a certificados assinados pelo cliente do balanceador de carga da instância.

Antes de Iniciar
Função necessária: administrador

É necessário instalar o plug-in Segurança de infraestrutura (com.glide.infrastructure_security) para realizar essas etapas. ConsulteSegurança de infraestrutura para obter detalhes sobre esse plug-in.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para obter informações sobre como usar URLs personalizados com ServiceNow, consulte Definição de Uma URL personalizada como o URL da instância.

Procedimento

1. Navegue até **Todos** > **Configurações de segurança de infraestrutura** > **Gerar CSR**.
2. Adicione um ou mais domínios à sua solicitação.

   a. Clique no botão **Adicionar** sob o título **Domínios**.

   b. Na janela pop-up, insira o domínio e selecione **OK**.

   c. Repita essas etapas conforme necessário para adicionar mais domínios.

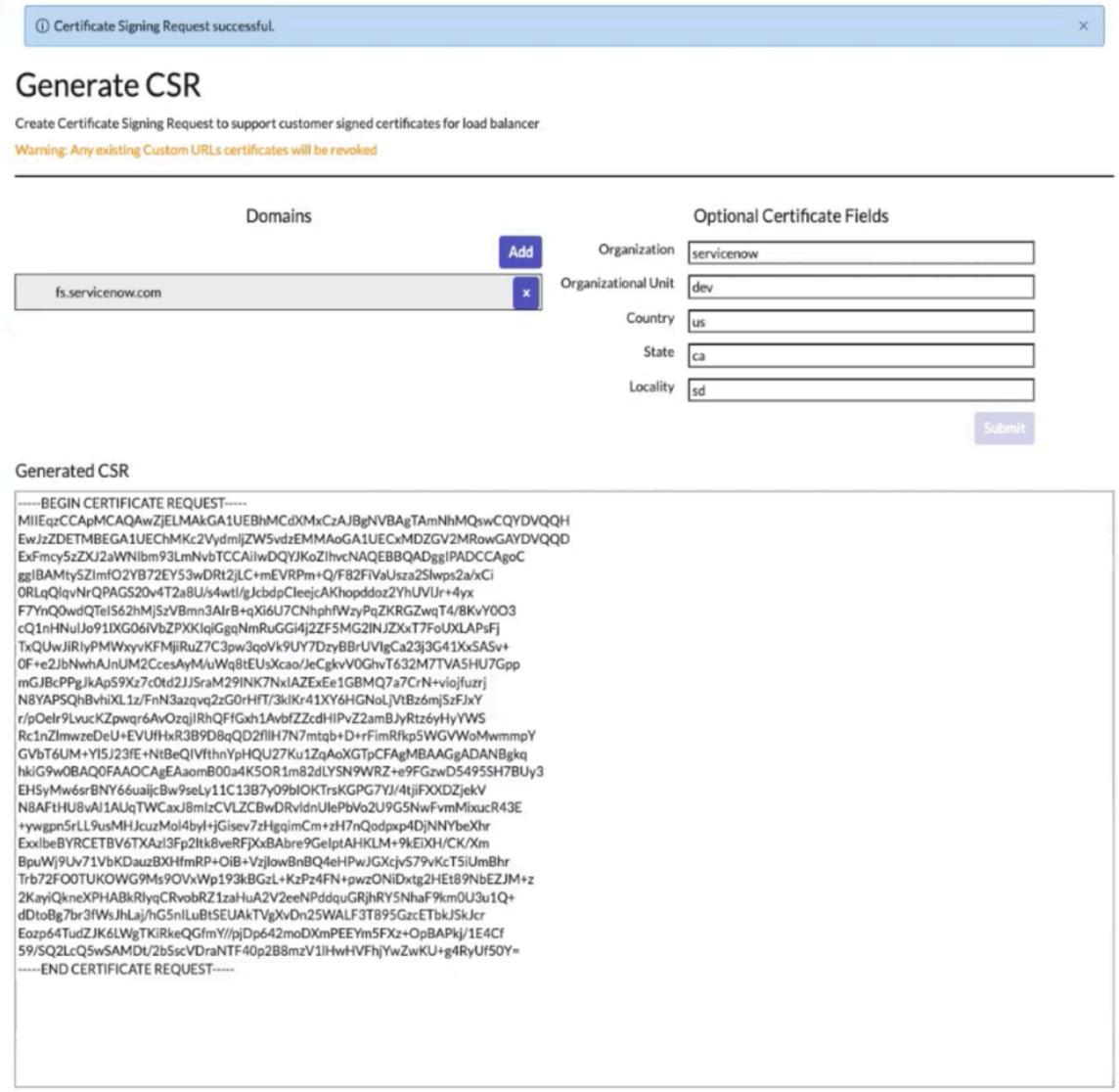
   > **Nota:** Os domínios podem ser removidos selecionando o botão "X" à esquerda de cada entrada de domínio.

3. Insira as informações que você deseja incluir em sua solicitação nos **Campos de certificação opcionais**.
4. Selecione **Enviar**.

   > **Aviso:** Não é possível enviar uma solicitação enquanto outra solicitação está sendo gerada. Se isso ocorrer, será exibido um erro de "Recurso em conflito". Para realizar o processamento, cancele a solicitação atual ou aguarde o processamento da solicitação atual antes de enviar outra.

   Depois de clicar em **Enviar**, sua instância gerará a solicitação de assinatura de certificado. A solicitação será exibida no campo **CSR gerado**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Copie o conteúdo do campo **CSR gerado**.

Criptografia Password2 com o KMF (Key Management Framework, Estrutura de gestão de chaves)

Compatível com Estrutura de gestão principal, o tipo de campo Password2 (criptografia bidirecional) é usado para criptografar e descriptografar campos personalizados com segregação de tarefas, proteção de chave e gerenciamento de ciclo de vida. Ele funciona de acordo com as diretrizes NIST 800-57 e fornece proteção FIPS 140-2-L3.

O Password2 é um campo de texto que armazena senhas com criptografia bidirecional. A criptografia bidirecional armazena senhas como um valor criptografado seguro que pode ser descriptografado na instância.

Dica: A partir da versão Vancouver, os administradores podem descontinuar a criptografia 3DES em campos password2 e dar preferência para o AES (Advanced Encryption Standard) mais atual. Para obter mais detalhes, consulte Descontinuar o uso do GlideEncrypter do 3DES para campos Password2.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

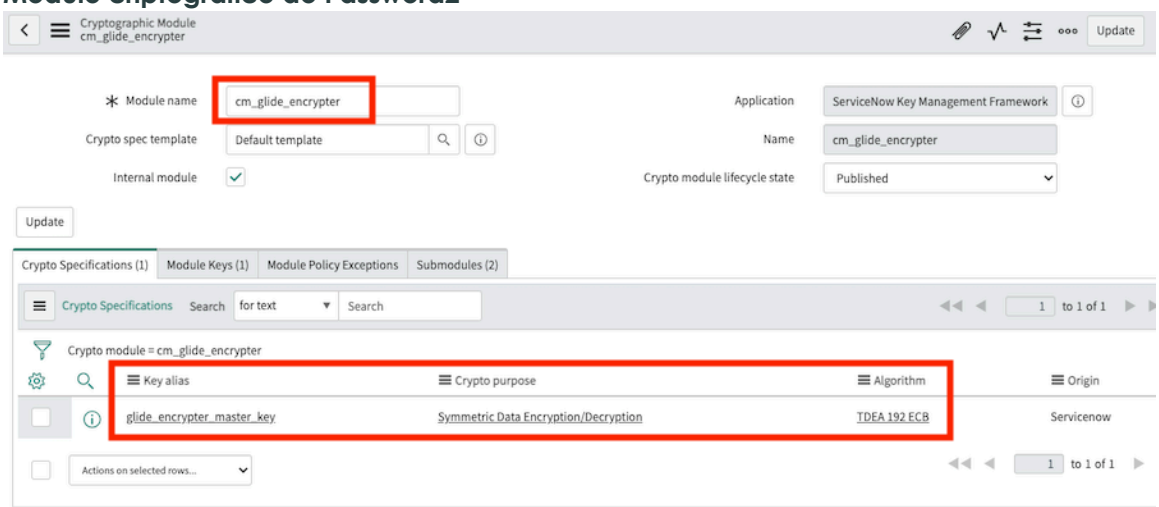
Ativação

A funcionalidade do Password2 está ativa por padrão. Ela é controlada pela propriedade *glide.kmf.encrypter.enabled*, que é definida como **true (verdadeira)** para todas as novas instâncias e upgrades. Não é necessário habilitar o Criptografia em nível de coluna para empresas para usar o Password2.

Entendendo o funcionamento do Password2

O Estrutura de gestão principal fornece um módulo criptográfico primário do sistema base **cm_glide_encrypter**. Esse módulo fornece uma especificação criptográfica e uma chave que pode descriptografar campos legados Password2.

Módulo criptográfico do Password2



Este módulo cm_glide_encrypter pode ter submódulos, cada um com seu próprio módulo de chave e especificação. Se um submódulo estiver presente com o mesmo escopo da aplicação do campo em que o Password2 está, o sistema usará o submódulo. Por exemplo, se uma tabela da aplicação ServiceNow® Atendimento ao cliente tiver um submódulo, e você gravar informações em um campo de Password2 em uma tabela no escopo da aplicação do Atendimento ao cliente, o processo criptográfico chamará o submódulo Atendimento ao cliente. O processo também usa a chave desse submódulo para criptografia e descriptografia com uma chave de criptografia AES 256 GCM exclusiva. É permitido um submódulo por escopo da aplicação. O módulo primário nem sempre é usado para o escopo global. Geralmente, os novos campos usam instance_level_glide_encrypter.

Nota: Não é possível criar seus próprios submódulos na Xanadu. Os submódulos são fornecidos em vários plug-ins de aplicação na Now Platform. Você pode girar chaves em submódulos, mas não no módulo primário cm_glide_encrypter.

Domain separation e clientes no local

O KMF Password2 não é compatível com Domain Separation. Você pode usar o Password2 com instâncias locais.

Password2 herdado e Password2 atual

No Xanadu, o campo Password2 existente foi atualizado.

A implementação atual do Password2:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Usa o Estrutura de gestão principal de acordo com as diretrizes de encapsulamento de chave NIST 800-57 e fornece proteção FIPS 140-2-L3 para toda a hierarquia de chaves.
- Inclui recursos para criar submódulos KMF Password2 dedicados e exclusivos para aplicações específicas, fornecendo controle por meio do escopo da aplicação. Cada submódulo tem sua própria chave de criptografia AES 256 GCM exclusiva.

Campos Password2 em scripts.

Ao acessar campos Password2 com um script, execute o script no mesmo escopo do escopo da tabela. Use `setDisplayValue ()` para criptografar valores Password2 e `getDecryptedValue ()` para descriptografar e ler o valor.

Nota: Não use a API `GlideEncrypter ()` em campos Password2.

Este script de exemplo mostra como criptografar `my@Password` na coluna password2 da tabela 'table_xyz'.

```
var  gr =  new GlideRecord('table_xyz');
gr.setDisplayValue('pwd2column_name', 'my@Password');
gr.insert();
```

Importante: Você não pode usar a API `setValue ()` para o campo Password2.

Este script de exemplo mostra como descriptografar o mesmo campo para recuperar o valor:

```
var  gr =  new GlideRecord('table_xyz');
gr.query();
gr.next();
var ge=gr.getElement('pwd2column_name');
var ged1 = ge.getDecryptedValue();
```

Importante: A API `getDecryptedValue ()` não tem escopo. Ela está disponível globalmente.

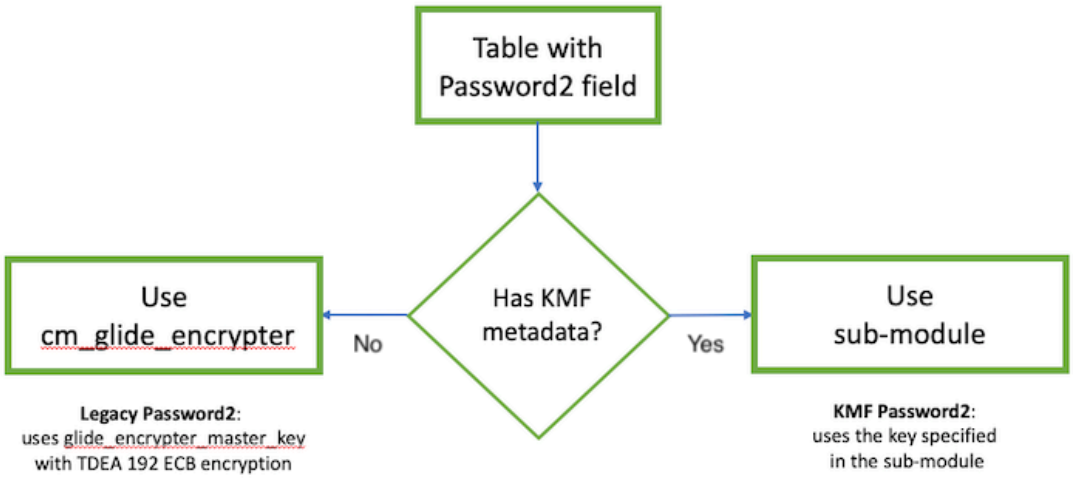
1. Quando você criptografa dados em um campo Password2, o sistema determina o escopo da aplicação em que o campo Password2 reside.
2. O sistema vai procurar um submódulo do módulo primário **cm_glide_encrypter** com o mesmo escopo da aplicação se a propriedade estiver definida como *true*.

   Nota: Se um submódulo com o mesmo escopo estiver presente, ele usará a especificação e a chave do submódulo para executar a criptografia.

Esta ilustração explica como sua instância descriptografa dados em campos Password2 :

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Fluxo de descriptografia do Password2



Trabalho de migração do KMF Password2

Um trabalho de migração é fornecido para clientes que atualizam de versões anteriores. Ele usa os dados criptografados com uma criptografia herdada do Password2 e os criptografa novamente com a chave em uma chave de submódulo KMF Password2. A recriptografia se aplica somente a tabelas com campos Password2 em escopos da aplicação que também têm submódulos criados para esse escopo. Por exemplo, um campo Password2 herdado na aplicação **XYZ_example** (com o escopo da aplicação **XYZ_example**) somente será recriptografado se um submódulo para o escopo da aplicação **XYZ_example** existir no módulo primário cm_glide_encrypter.

As chaves de criptografia KMF Password2 no submódulo são protegidas (criptografia de envelope) na hierarquia de chaves KMF.

Certificados

Sua instância requer certificados para estabelecer conexões seguras e validar assinaturas.

Explorar	Configurar
Aprenda os principais recursos e o valor comercial dos certificados.	Planeje suas configurações principais.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Carregar Planeje e configure a aplicação.	

Explorando certificados

Sua instância requer certificados para estabelecer conexões seguras e validar assinaturas.

Os certificados são usados para recursos como:

- LDAPS
- Autenticação mútua de serviço web de saída
- Segurança de serviços da web
- MID Server

Para usar um certificado, é necessário gerar ou comprar um certificado para o cliente ou servidor protegido e carregá-lo em uma instância.

Certificados LDAP

Um certificado SSL é necessário para que a instância estabeleça uma conexão do protocolo LDAPS (LDAP over SSL) com um servidor LDAP.

A instância aceita dois tipos de certificados LDAP:

Certificado	Tipo	Necessário para
Certificado do servidor LDAP	Qualquer tipo suportado	Todas as configurações LDAP
Certificado do cliente LDAP	Tipo de armazenamento de chaves Java	Autenticação mútua

Se houver vários certificados de servidor, a instância, por sua vez, tentará cada certificado de servidor até que o servidor LDAP permita a conexão. Se usar vários servidores LDAP, certifique-se de incluir o certificado SSL para cada servidor LDAP.

A autenticação mútua exige que o cliente apresente um certificado além do servidor. Se o servidor LDAP requer autenticação mútua, você também deve fornecer o certificado de cliente do servidor LDAP em um certificado Java do tipo de armazenamento de chaves.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Critérios de certificação

Um certificado válido deve atender a estes critérios:

- O certificado pode ter um tamanho de chave de até 2048 bits.
- O certificado deve ter uma destas extensões de arquivo:

Extensão	Descrição
DER	O formato Regras de codificação diferenciadas é uma sintaxe de transferência de mensagens binárias. Este formato também oferece suporte às extensões de arquivo .CER e .CRT.
CER	Extensões do arquivo de certificação para certificados que usam o formato Regras de codificação diferenciadas.
CRT	Extensões do arquivo de certificação para certificados que usam o formato Regras de codificação diferenciadas.
PEM	O formato Privacy Enhanced Mail é um certificado DER codificado por base-64 cercado entre as cadeias de texto "-----BEGIN CERTIFICATE-----" e "-----END CERTIFICATE-----".

Confiança de certificado

Por padrão, sua instância confia somente em certificados de uma autoridade de certificação (CA) reconhecida na JVM (Java Virtual Machine). Certificados autoassinados e assinados pela empresa não são confiáveis.

Nota: Para saber mais sobre as propriedades que afetam o uso de certificados, consulte Comunicações seguras nas Configurações de proteção da segurança de instância.

Geração de certificado do cliente LDPA

Gere um certificado de cliente LDAP para autenticação mútua usando OpenSSL. A saída final é um certificado PKCS#12 armazenado em um armazenamento de chaves Java.

Antes de Iniciar
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa
Consulte a Documentação OpenSSL para obter mais informações sobre a geração de certificados. Essas etapas assumem que você possui acesso ao OpenSSL.

Insira esses comandos em uma interface da linha de comandos.

Procedimento

1. Gere um certificado do cliente auto-assinado.

   Example
   Por exemplo, este comando cria um certificado de cliente test1-cert.crt com base na chave privada test1-key.key.

```
openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout
 test1-key.key -out test1-cert.crt
```

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

2. Converta o arquivo de certificado e a chave privada em PKCS#12 (um arquivo com uma extensão .pfx ou .p12).

   Example
   Por exemplo, este comando converte o certificado do cliente e a chave privada em um certificado PKCS#12 chamado test1-certificate.pfx.

   ```
   openssl pkcs12 -export -out test1-certificate.pfx -inkey test1-key.key
    -in test1-cert.crt
   ```

3. Gere o Java Key Store e importe o arquivo pkcs12 nele.

   Example
   Por exemplo, este comando importa o certificado para o armazenamento de chave test1.jks Java.

   ```
   keytool -importkeystore -srckeystore test1-certificate.pfx
    -srcstoretype PKCS12 -destkeystore test1.jks
   ```

4. Carregue o certificado no arquivo de armazenamento de chave (`test1.jks`) para a instância.

   Nota:

   Se você estiver atualizando em uma instância no local usando um certificado com a extensão .jks e receber um erro dizendo "Nenhum certificado válido encontrado para processar o carregamento da aplicação", use um certificado com a extensão .pfx em seu lugar.

O que Fazer Depois
Carregamento de certificados para uma instância

Geração de certificado de servidor

É possível usar a ferramenta de chave para gerar um novo arquivo de armazenamento de chave Java, criar uma solicitação de assinatura de certificado (CSR) e importar a chave privada, par de certificados público e certificados assinados no armazenamento de chave.

Antes de Iniciar
Função necessária: admin

Por Que e Quando Desempenhar Esta Tarefa
Consulte a Documentação da ferramenta de chave Java para obter mais informações sobre a geração de chaves e CSRs.

Insira esses comandos em uma interface da linha de comandos:

Procedimento

1. Gere um armazenamento de chaves Java e par de chaves.

   Example
   Por exemplo, este comando cria um armazenamento de chaves denominado my.keystore e gera uma chave privada denominada mydomain com o armazenamento de chaves.

   ```
   keytool -genkey -alias mydomain -keyalg RSA -keystore my.keystore
   ```

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

2. Gere um CSR para um armazenamento de chaves Java existente.

   Example
   Por exemplo, este comando gera um CSR denominado mydomain.csr ou a chave mydomain.

   ```
   keytool -certreq -alias mydomain -keystore my.keystore -file
    mydomain.csr
   ```

3. Importe uma autoridade de certificação intermediária ou raiz, ou CA, certificação para o armazenamento de chave Java.

   Example
   Por exemplo, este comando importa a certificação CA para Thawte. Este comando assume que Thwate foi a CA que assinou o CSR.

   ```
   keytool -import -trustcacerts -alias root -file Thawte.crt -keystore
    my.keystore
   ```

4. Importe um certificado primário assinado para o armazenamento de chaves Java.

   Example
   Por exemplo, este comando importa o certificado assinado mydomain.crt para o armazenamento de chaves.

   ```
   keytool -import -trustcacerts -alias mydomain -file mydomain.crt
    -keystore my.keystore
   ```

5. Carregue o certificado no arquivo de armazenamento de chaves (my.keystore) para a instância.

O que Fazer Depois
Carregamento de certificados para uma instância

Carregamento de certificados para uma instância

Adicione um certificado à instância do módulo Certificados.

Carregue um certificado para uma instância

Carregue um certificado para uma instância.

Antes de Iniciar
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa
Quando um certificado é atualizado no servidor ADFS, você também precisa carregar um certificado atualizado para a instância.

Procedimento

1. Navegue até **Todos** > **Definição do sistema** > **Certificados**.
2. Selecione **Novo**.
3. No formulário, preencha os campos.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Nome	Especifique um nome exclusivo para o certificado.
Notificação de expiração	[Opcional] Selecione se deseja enviar uma notificação quando o certificado estiver prestes a espirar.
Ativo	Selecione se a instância deve usar este certificado para comunicações seguras e solicitações de assinatura.
Descrição resumida	[Opcional] Insira uma descrição de texto do certificado, como o solicitante ou o nome do servidor.
Formato	Selecione o formato de certificado. A instância suporta os formatos PEM e DER.
Tipo	Selecione o contêiner de certificado. A instância reconhece os certificados dos armazenamentos de confiança, armazenamento de chaves Java e armazenamentos de chave PKCS#12.
Certificado PEM	Insira o texto formatado por PEM codificado com base-64 que contém o certificado DER. A instância decodifica o certificado para preencher os campos **Válido a partir de**, **Expira**, **Expira em dias**, **Emissor** e **Assunto**.

4. Selecione **Enviar**.

   Durante o carregamento, o módulo extrai e exibe as propriedades somente leitura do certificado nestes campos:

   - Data inicial válida
   - Data de vencimento
   - Emissor
   - Assunto do Certificado

5. Selecione **Validar Stores/Certificados** para verificar se o certificado está correto.
   Se a instância encontrar erros com o certificado ou armazenamento de chaves, será exibida uma mensagem de erro.

Carregamento de um certificado de servidor confiável

Ao carregar o certificado do servidor confiável do provedor de serviço, a instância assegura que está se conectando a um serviço seguro e válido.

Antes de Iniciar

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

A instância valida as chamadas de serviço da web de saída usando o certificado fornecido pelo provedor de serviços.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Crie um novo registro Certificado com o tipo **Trust Store Cert**.
2. Execute uma das seguintes ações:
   - Anexe o certificado formatado de DER do provedor de serviço.
   - Copie e cole o certificado de formato de PEM do provedor de serviço no campo **Certificado PEM**.

Criptografia em nível de coluna

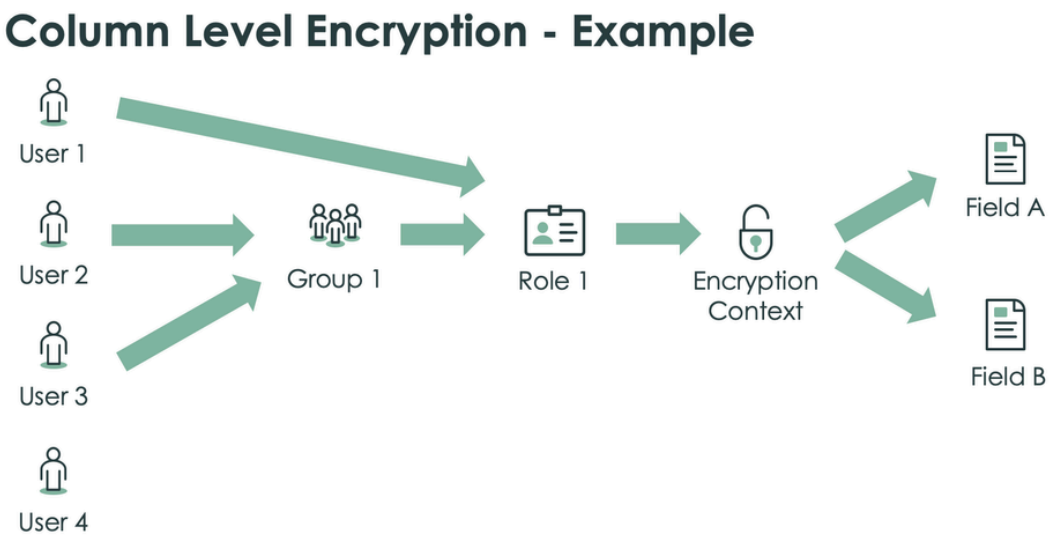
A CLE (Column Level Encryption, criptografia em nível de coluna) permite e recusa o acesso a dados criptografados com base na função do usuário. Ela inclui gestão básica de chaves usando módulos de criptografia.

Visão geral

Com a Criptografia em nível de coluna, é possível criptografar colunas de dados específicas em suas tabelas, em vez de criptografar toda a tabela ou todo o banco de dados. Use esse método para garantir que seus dados confidenciais permaneçam protegidos sem a necessidade de criptografar uma tabela inteira. A capacidade de criptografar somente as partes das tabelas que exigem isso ajuda a reduzir o tempo gasto na criptografia e descriptografia de dados.

A CLE concede acesso a dados criptografados com base na função de um usuário. Por causa dessa abordagem, para exibir dados criptografados pela CLE, os usuários devem estar associados a uma função. É possível associar os usuários a uma função diretamente ou designá-los a um grupo que está associado a uma função. Essa abordagem baseada em função simplifica o processo de garantir que os dados fiquem visíveis somente aos usuários que precisam deles.

Exemplo de criptografia baseada em função



Nesse exemplo, é possível ver quatro usuários que estão tentando acessar dados armazenados em dois campos de um formulário. Esses campos são criptografados por um contexto de criptografia, que só pode ser acessado por usuários associados a uma função específica (Função 1).

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- O usuário 1 é um membro da Função 1, que oferece acesso ao módulo de criptografia 1. O usuário 1 pode ver o conteúdo do Campo A e do Campo B.
- O Usuário 2 e o Usuário 3 são membros do Grupo 1. O Grupo 1 é um membro da Função 1, o que permite que todos no Grupo 1 acessem o módulo de criptografia 1 e permite que o Usuário 2 e o Usuário 3 vejam o conteúdo do Campo A e do Campo B.
- O Usuário 4 não é membro de nenhum grupo ou função e não tem acesso ao módulo de criptografia 1. Portanto, além de não ter acesso ao Campo A nem ao Campo B, ele também nem vê esses campos em um formulário. Em uma exibição de lista, esses campos estão visíveis, mas os valores estão vazios.

Iniciar

Explorar	Configurar	Usar
Conheça os benefícios das edições Standard e Enterprise da Criptografia em nível de coluna.	Saiba como ativar e configurar a Criptografia em nível de coluna para empresas e gerenciar a migração do Suporte de criptografia	Use a Criptografia em nível de coluna para gerenciar o acesso aos dados criptografados em suas instâncias

Solucionar problemas e obter ajuda

- Fórum da comunidade ServiceNow
- Pesquisar artigos de erros conhecidos no portal de erros conhecidos
- ContatoSuporte e atendimento ao cliente

Exploração da criptografia em nível de coluna

Saiba mais sobre a Criptografia em nível de coluna.

Visão geral da Criptografia em nível de coluna

CLE (Column Level Encryption, Criptografia em nível de coluna) é um recurso básico do sistema que permite a criptografia de dados armazenados em uma instância usando AES128 ou AES256.

A CLE permite criptografar campos selecionados de banco de dados e arquivos armazenados usando contextos de criptografia. Nesses contextos, você define o que é criptografado, escolhe qual algoritmo usar e informa a chave de criptografia, que é armazenada em sua instância.

Após a criação do contexto, é possível associá-lo a uma função do usuário. Os usuários atribuídos a essa função, diretamente ou por meio de um grupo, podem acessar os dados criptografados.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Como a CLE baseia o acesso aos dados na atribuição de função, é importante estar familiarizado com a administração de funções em sua instância. Para obter mais informações, consulte Gestão de funções.

Fluxo de trabalho da Criptografia em nível de coluna

Benefícios da Criptografia em nível de coluna

Benefício	Recurso	Funções necessárias
Configure o acesso aos dados criptografados com base nas funções do usuário atribuídas.	Acesso aos dados criptografados com base em função	administrador de segurança
Proteja dados usando o AES (Advanced Encryption Standard, padrão de criptografia avançada). É possível optar por usar os algoritmos de criptografia AES-128 ou AES-256.	Criptografia AES	administrador de segurança
Crie até cinco módulos e MAPs (Module Access Policies, políticas de acesso a módulos) usando a versão padrão da CLE. As MAPs expandem o acesso baseado em função a fim de permitir considerações para: • Usuários do sistema • Scripts • Troca de recursos KMF A CLE para empresas oferece suporte a MAPs adicionais.	Suporte a até cinco módulos e MAPs	administrador de segurança
Criptografe tipos de campo comuns usando a versão padrão da CLE. A CLE para empresas oferece suporte a tipos de campo adicionais.	Criptografia de textos de cadeias de caracteres, campos de data e data/hora, anexos e URLs	administrador de segurança
Escolha entre a criptografia padrão e de preservação da igualdade. Quando ativada, a criptografia de preservação da igualdade garante que o valor criptografado de um campo seja o mesmo quando o valor do campo permanece o mesmo. Esse tipo de criptografia proporciona comparações de igualdade e operações de agrupamento em um campo. **Nota:** Não há suporte à criptografia não determinística.	Suporte à criptografia de preservação de igualdade	administrador de segurança

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Benefício	Recurso	Funções necessárias
Use as APIs `getDisplayValue()` e `setDisplayValue()` para exibir valores em texto simples e inserir dados criptografados para os campos criptografados.	APIs `getDisplayValue()` e `setDisplayValue()`	administrador de segurança, desenvolvedor

Benefícios da Criptografia em nível de coluna para empresas

A Criptografia em nível de coluna para empresas se baseia na estrutura existente de CLE e oferece estes recursos adicionais depois que você adquire uma assinatura.

Benefício	Recurso	Funções necessárias
Criptografe tipos de campo adicionais.	Suporte a tipos de campo adicionais: • HTML • Diário • Traduzido	administrador de segurança
A CLE para empresas dá suporte a mais de cinco módulos e políticas de acesso a módulos para oferecer mais opções de acesso a dados protegidos.	Suporte a MAPs e módulos adicionais	administrador de segurança
É possível fazer rodízio das chaves de um cofre de chaves com base em um cronograma que você configurar. O uso do rodízio automático de chaves pode melhorar a segurança e reduzir a sobrecarga administrativa.	Rodízio automático e configurável de chaves	administrador de segurança
Gerencie o ciclo de vida completo de suas chaves de criptografia de dados. Também é possível trocar as chaves de criptografia de dados geradas em seu ambiente com segurança.	Chaves fornecidas pelo cliente	administrador de segurança
Chaves efêmeras são chaves criptográficas geradas para cada execução de um processo criptográfico. Essas chaves são mais seguras porque são geradas para uso em uma só sessão.	Chaves criptográficas efêmeras	administrador de segurança
As APIs `setDisplayValue()` e `setDisplayValue()` atualizadas podem inserir dados criptografados para campos criptografados.	APIs `getDisplayValue()` e `setDisplayValue()` atualizadas	administrador de segurança, desenvolvedor

Tour guiado do Criptografia em nível de coluna

O tour fornece uma visão geral em resumo da configuração do Criptografia em nível de coluna (CLE) necessária para criptografar campos de tabela ou anexos. Aborda também as etapas para a criação de módulos de Edge Encryption, políticas de acesso ao módulo e

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

configurações de campo criptografado. O tour inclui links para documentação detalhada e o curso de Visão Geral da Criptografia em nível de coluna do Now Learning.

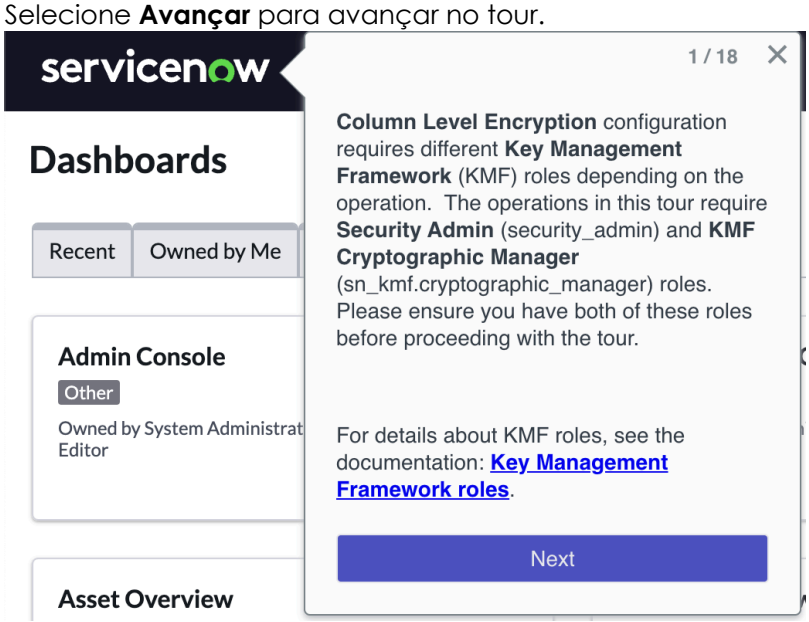
Antes de Iniciar

Função necessária: sn_kmf.cryptographic_manager ou security_admin

Nota: O tour guiado ainda não está disponível quando o Next Experience estiver habilitado.

Procedimento

1. Navegue até a página de IU **$pa_dashboards_overview.do** em sua instância. Por exemplo: `http://yourcompany.servicenow.com/nav_to.do?uri=%2F$pa_dashboards_overview.do` Substitua `yourcompany` pelo nome da instância.
2. Abra o ícone **Exibir ajuda** ( ) no canto superior esquerdo.
3. Selecione **Fazer um tour** na parte inferior da barra lateral.
4. Selecione **Avançar** para avançar no tour.



Configuração da criptografia em nível de coluna

Saiba como ativar e configurar a Criptografia em nível de coluna e gerenciar a migração do Suporte de criptografia.

Ativação

Criptografia em nível de coluna

O plug-in de Criptografia em nível de coluna (com.glide.encryption) não requer uma assinatura e pode ser ativado em sua instância por um administrador. Para obter detalhes sobre a instalação do plug-in, consulte Ativar um plug-in.

Criptografia em nível de coluna para empresas

A Criptografia em nível de coluna para empresas é uma versão aprimorada da aplicação base e requer uma assinatura.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Para obter detalhes sobre o produto, consulte Criptografia em nível de coluna para empresas.
- Para obter detalhes de instalação da Criptografia em nível de coluna para empresas, consulte Ativação do Criptografia em nível de coluna para empresas.

Migração do suporte de criptografia

Use os Trabalhos agendados para migrar suas chaves e seus dados criptografados do Suporte de criptografia legado para a Criptografia em nível de coluna para empresas. Veja os detalhes desse processo em Migração para o Criptografia em nível de coluna para empresas

Como mudar as configurações de criptografia de anexos

Aumente a segurança impedindo que usuários anexem arquivos não criptografados. Para obter detalhes, consulte Impedir que usuários anexem arquivos não criptografados.

Ativação do Criptografia em nível de coluna para empresas

Com a assinatura do Criptografia em nível de coluna para empresas, um administrador pode ativar o plug-in com.glide.now.platform.encryption.

Antes de Iniciar

Função necessária: administrador

Para adquirir uma assinatura, entre em contato com o seu gerente de contas ServiceNow. O gerente de contas pode providenciar para que o plug-in seja ativado nas instâncias de produção e não produção da organização, geralmente dentro de alguns dias.

Por Que e Quando Desempenhar Esta Tarefa

A ativação do plug-in Criptografia em nível de coluna para empresas (`com.glide.now.platform.encryption`) faz as seguintes mudanças na instância:

- O plug-in do Suporte de Criptografia (com.glide.encryption) também está ativado.

  Nota: O plug-in do Estrutura de gestão principal (com.glide.kmf.global) já está ativo por padrão.

- A propriedade `glide_encryption.set_value_support_cle.disabled` será definida como **falsa**, o que ativa o recurso SetValue. O suporte ao SetValue permite que as APIs `setDisplayValue ()` e `setValue ()` ofereçam suporte a dados criptografados. Ele também permite que `getDisplayValue ()` e `getValue ()` retornem valores de texto não criptografado.
- Dois trabalhos agendados estão habilitados:

  - **autoKeyMigration**: migra chaves de contexto de criptografia para chaves de módulo criptográficoEstrutura de gestão principal (KMF).
  - **autoDataMigration**: migra os dados que você já criptografou para usar a chave do módulo criptográfico KMF.

  Os administradores podem modificar quando eles são executados e podem pausá-los ou reiniciá-los a qualquer momento.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegue até **Todos** > **Aplicações do sistema** > **Todas as aplicações disponíveis** > **Todas**.
2. Encontre o plug-in *Criptografia da plataforma - com.glide.now.platform.encryption* usando os critérios de filtro e a barra de pesquisa. Pesquise o plug-in pelo nome ou ID. Se não conseguir encontrar um plug-in, talvez seja necessário solicitá-lo ao pessoal ServiceNow.
3. Selecione **Instalar** e, na caixa de diálogo Ativar plug-in, selecione **Ativar**.

> **Nota:** Quando a separação de domínio e o administrador delegado estão habilitados em uma instância, o usuário administrativo deve estar no domínio **global.** Caso contrário, será exibido o seguinte erro: `A instalação do aplicativo não está disponível porque há outra operação em execução: ativação de plug-in para <plugin name>.`

Migração para o Criptografia em nível de coluna para empresas

Os trabalhos agendados migram suas chaves e dados criptografados do Suporte de criptografia para o Criptografia em nível de coluna para empresas.

Você pode revisar os trabalhos agendados navegando até **Segurança do sistema** > **Configurações de alta segurança** > **Trabalhos de segurança**:

- **autoKeyMigration**: migra chaves de contexto de criptografia para chaves de módulo criptográficoEstrutura de gestão principal (KMF).
- **autoDataMigration**: migra os dados que você já criptografou para usar a chave do módulo criptográfico KMF.

Você pode modificar quando eles são executados e pausá-los ou reiniciá-los a qualquer momento.

Verifique se as configurações de campo criptografado estão usando as chaves do módulo recém-migradas, navegando até **Segurança do sistema** > **Edge Encryption** > **Configurações de campo criptografado**. Procure os seguintes itens:

- O campo **Método** é **Módulo único**.
- O campo **Módulo de criptografia** está preenchido com o nome do módulo criptográfico que o sistema cria automaticamente. Você pode revisar esse módulo e a política de acesso ao módulo, ambos ativos e publicados.

Criptografia em nível de coluna para empresas e clones do sistema

Se o Criptografia em nível de coluna Enterprise estiver instalado em sua instância, uma nova chave de criptografia do módulo de Edge Encryption será gerada automaticamente na instância do clone de destino como parte do processo de clonagem. Essas chaves são geradas para todos os módulos aos quais o usuário tem acesso que ainda não têm uma chave.

Por isso, os módulos de Edge Encryption na instância do clone de destino podem ter duas chaves de criptografia de módulo:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

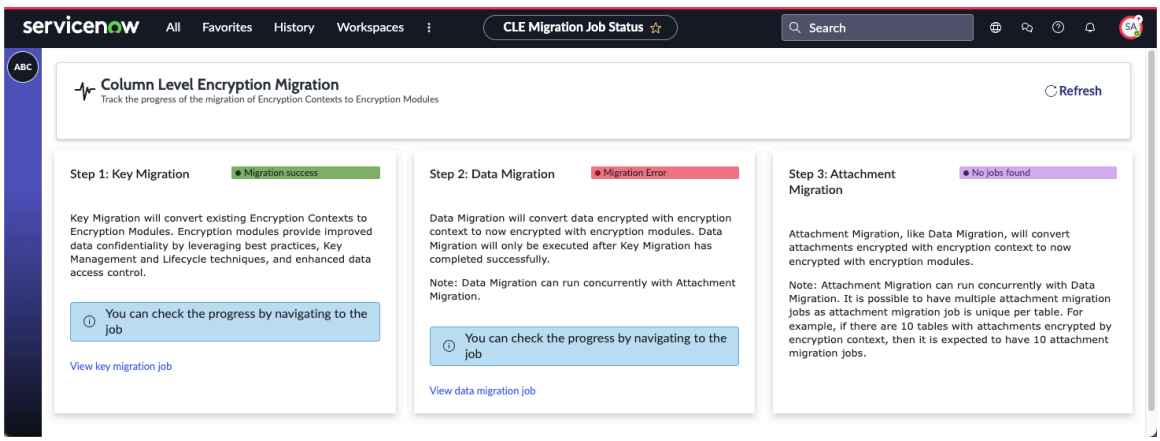
- Uma chave de criptografia do módulo ativo. Esta é a nova chave gerada após a clonagem, contanto que o módulo esteja acessível para o usuário e não tenha chaves anteriores.
- Uma chave do módulo de criptografia desativada (da transferência de troca de chave automatizada

  A chave de criptografia do módulo ativo é usada para criptografar os dados inseridos conforme necessário na instância do clone de destino. O módulo desativado é usado para descriptografar dados existentes que foram clonados como parte do clone do sistema.

  Para usar uma única chave para descriptografar e criptografar todos os dados, você pode executar um trabalho de recriação de chaves do módulo. Para obter mais informações sobre trabalhos de rechaveamento de módulo, consulte Programar trabalhos de criptografia, descriptografia e rechaveamento em massa.

Página de status de migração do Criptografia em nível de coluna

Use a página de status de migração para rastrear a migração de contextos de criptografia para módulos de criptografia.

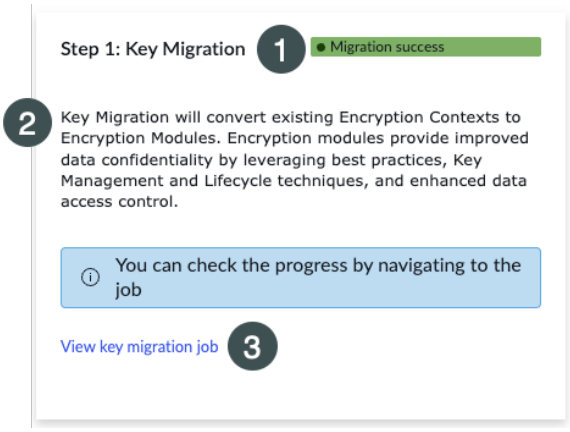


A página Migração do Criptografia em nível de coluna exibe o status das etapas envolvidas na migração de contextos de criptografia para módulos de criptografia. Cada uma das três seções exibe o status de uma etapa específica do processo.

Cartões de seção de página

A página contém três cartões que representam as etapas no andamento da migração. Esses cartões exibem:

- (1) O status da etapa atual. Esse status será exibido se a etapa tiver sido concluída com sucesso ou se não houver trabalhos para processar.
- (2) Uma descrição da etapa listada.
- (3) Um link para o registro de trabalho de criptografia relevante [sys_mass_encryption_job].



© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Impedir que usuários anexem arquivos não criptografados

Modifique a propriedade com.glide.encryption.enable_attachment_key_ui para permitir que usuários com acesso a uma chave de módulo de criptografia anexem anexos não criptografados.

Antes de Iniciar
Função necessária: security_admin

Você deve elevar para a função security_admin ao executar essas etapas. Para obter instruções, consulte Elevar para uma função privilegiada.

Por padrão, os usuários com acesso a uma chave do módulo de criptografia não podem carregar anexos não criptografados. Atualize a propriedade do sistema *com.glide.encryption.enable_attachment_key_ui* para mudar este comportamento.

Ao anexar, os usuários veem o seletor de IU em registros com configuração de campo criptografado de módulos múltiplos. Quando esta propriedade é definida como falsa, os usuários não veem mais uma opção para não criptografar um anexo.

Procedimento

1. Navegue até **Todas** > **Propriedades do sistema** > **Todas as propriedades**.
2. Na lista de propriedades do sistema, localize e abra a propriedade do sistema.
3. Defina o **valor** da propriedade é definido como `falso`.

Uso da Criptografia em nível de coluna

Use a Criptografia em nível de coluna para gerenciar o acesso aos dados criptografados em suas instâncias.

Informações relacionadas

- Criação de um módulo criptográfico do Criptografia em nível de coluna.
- Usando vários módulos de criptografia
- Criação de uma especificação criptográfica do Criptografia em nível de coluna
- Configuração de algoritmos avançados para o Criptografia em nível de coluna para empresas
- Configurar propriedades de chaves fornecidas pelo cliente
- Como criptografar campos e anexos
- Exemplos da Criptografia em nível de coluna para empresas

Criação de um módulo criptográfico do Criptografia em nível de coluna.

Crie um módulo criptográfico do Criptografia em nível de coluna para definir os mecanismos usados para operações criptográficas.

Antes de Iniciar
Funções necessárias: sn_kmf.cryptographic_manager ou sn_kmf_admin, security_admin e administrador

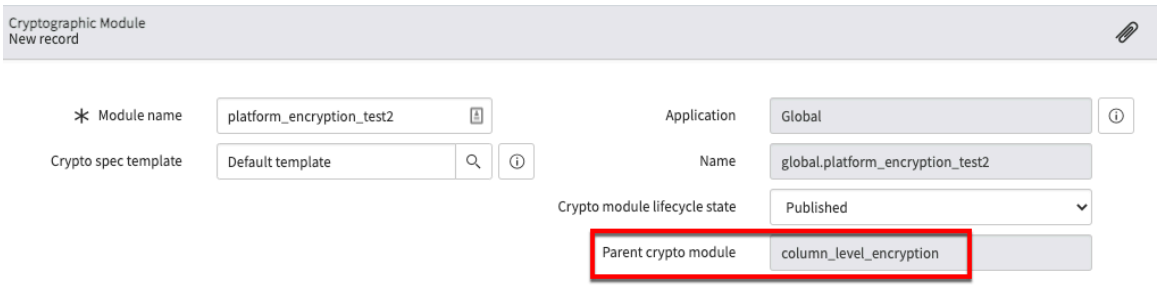
Por Que e Quando Desempenhar Esta Tarefa
Este procedimento descreve as opções disponíveis com o Criptografia em nível de coluna (CLE) com o sistema de base e opções de configuração adicionais que se tornam

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

disponíveis com a funcionalidade Criptografia em nível de coluna para empresas (CLE_Ent). Criptografia em nível de coluna para empresas está disponível com uma assinatura paga. Consulte Pacote de assinatura do Gerenciamento de criptografia e chaves para conhecer os recursos suportados e as opções disponíveis com cada oferta. Consulte Ativação do Criptografia em nível de coluna para empresas para obter mais informações sobre como obter Criptografia em nível de coluna para empresas.

Procedimento

1. Navegue até **Todos** > **Segurança do sistema** > **Módulos de Edge Encryption** > **Novo**.



2. No formulário, preencha os campos.

Formulário do Módulo criptográfico

Campo	Descrição
Nome do módulo	Cadeia de caracteres alfanuméricos a ser referenciada ao executar scripts.
Modelo de especificação de criptografia	Modelo padrão usado para criar o módulo criptográfico que contém mapeamentos de várias finalidades de criptografia para especificações de criptografia e algoritmos recomendados.
Aplicação	O escopo da aplicação selecionado
Nome	O nome do módulo de criptografia é anexado ao nome do escopo da aplicação para evitar conflito com outras aplicações com escopo na criação do módulo. Por exemplo, se você criar um módulo com o nome `my_crypto_module` no escopo da aplicação global, o nome será salvo como `global.my_crypto_module`.
Estado do ciclo de vida do módulo de criptografia	O termo ciclo de vida se refere à criação, uso e desativação de um módulo criptográfico. Defina como **Rascunho** inicialmente durante a configuração. Ao usar o módulo, defina-o como **Publicado**. O modelo Padrão é definido automaticamente como **Publicado**.
Módulo de criptografia primário	O módulo primário é preenchido automaticamente como **column_level_encryption**.

3. Clique em **Enviar**.

   Após o envio bem-sucedido, seu módulo criptográfico será listado na tabela Módulos criptográficos.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Aviso:

Para usuários de suporte a criptografia legada:

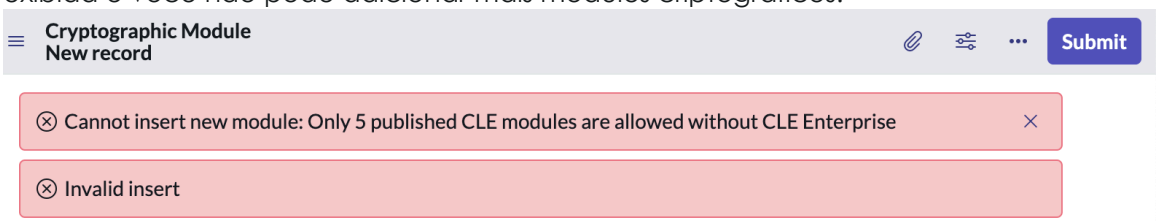
Se estiver usando a versão não Enterprise de Criptografia em nível de coluna, há um limite de cinco módulos. Se você excedeu esse limite, o seguinte aviso será exibido:

Esta inserção excede o limite de módulos publicados para o Criptografia em nível de coluna#disponíveis com a assinatura do produto. A assinatura Enterprise para o Criptografia em nível de coluna é necessária para outros módulos. Entre em contato com sua equipe de conta.

Uma especificação de criptografia padrão será criada com a finalidade de criptografia definida como criptografia/ descriptografia de dados simétrica e o algoritmo como AES 256 CBC. Selecione o algoritmo para atualizações.

4. Para abrir as opções de configuração, clique no módulo criptográfico recém-criado.

Nota: São permitidos no máximo cinco módulos da criptografia em nível de coluna antes da atualização para o Criptografia em nível de coluna para empresas. Uma mensagem de erro será exibida e você não pode adicionar mais módulos criptográficos.



O que Fazer Depois

Criação de uma especificação criptográfica do Criptografia em nível de coluna.

Usando vários módulos de criptografia

Múltiplos módulos de criptografia permitem que os dados sejam criptografados com mais de um módulo de criptografia. Se cada módulo tiver sua própria política de acesso com base em uma função, por exemplo, usuários com funções diferentes podem criptografar dados na mesma tabela, mas ainda podem ser impedidos de visualizar os dados criptografados uns dos outros.

Antes de Iniciar

Função necessária: sn_kmf.cryptographic_manager ou sn_kmf.admin

Por Que e Quando Desempenhar Esta Tarefa

Nota: Somente a criptografia em colunas é compatível com múltiplos módulos. A criptografia de anexos não é compatível. A criptografia em massa não está disponível ao usar o método de múltiplos módulos de criptografia.

Não é possível alterar um campo que usa módulos múltiplos de criptografia para usar um único módulo de criptografia.

O campo é criptografado pelo módulo de criptografia do primeiro usuário a inserir dados. Como o módulo de criptografia é definido por registro, os campos em uma lista podem ter módulos de criptografia diferentes. Em um único registro, o campo pode ser criptografado por apenas um módulo.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

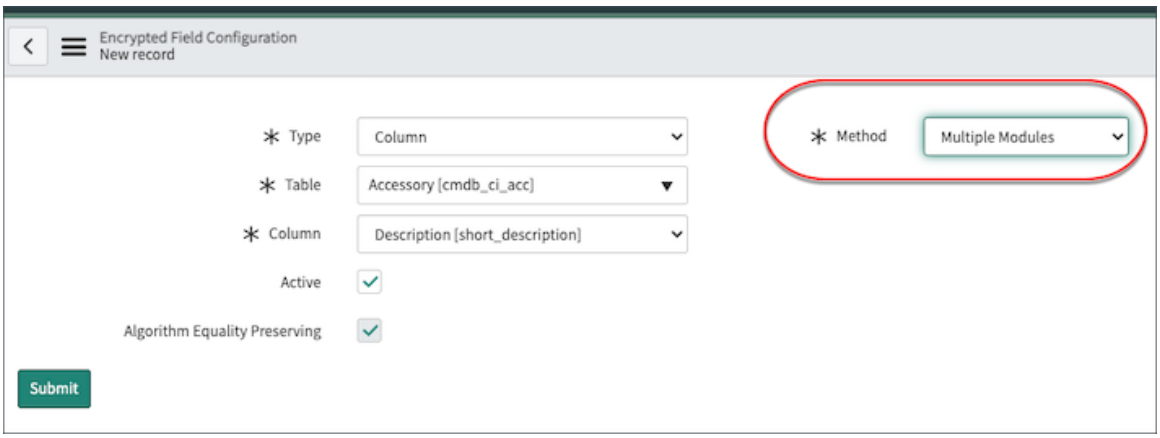
1. Criação de módulos criptográficos múltiplos e uma política de acesso para cada um.

   Certifique-se de conceder funções diferentes aos diferentes módulos criptográficos por meio das políticas de acesso.

2. Navegue até **Segurança do sistema** > **Edge Encryption** > **Configurações de Edge Encryption**

   Se precisar de mais informações sobre configurações de campo criptografado, consulte Definição das configurações de campo criptografado.

3. No campo **Tipo**, selecione **Coluna**.
   A criptografia de anexo não é compatível com módulos múltiplos.
4. Selecione **Módulos múltiplos** no campo **Método**.



5. Selecione a **Tabela** e a **Coluna** na tabela que você deseja criptografar.
6. Clique em **Enviar**.

Resultados

Os dados recém-criados para o campo especificado são criptografados com a chave do módulo relevante. Quando um usuário com a função especificada na política de acesso do módulo A grava na tabela especificada, os dados são criptografados com a chave do módulo A. Somente usuários com a mesma função podem ler os dados.

Example:

Como criptografar a coluna Descrição resumida na tabela Incidente. Você deve fazer o seguinte:

1. Criar dois módulos criptográficos A e B.
2. Criar uma política de acesso ao módulo para cada módulo.

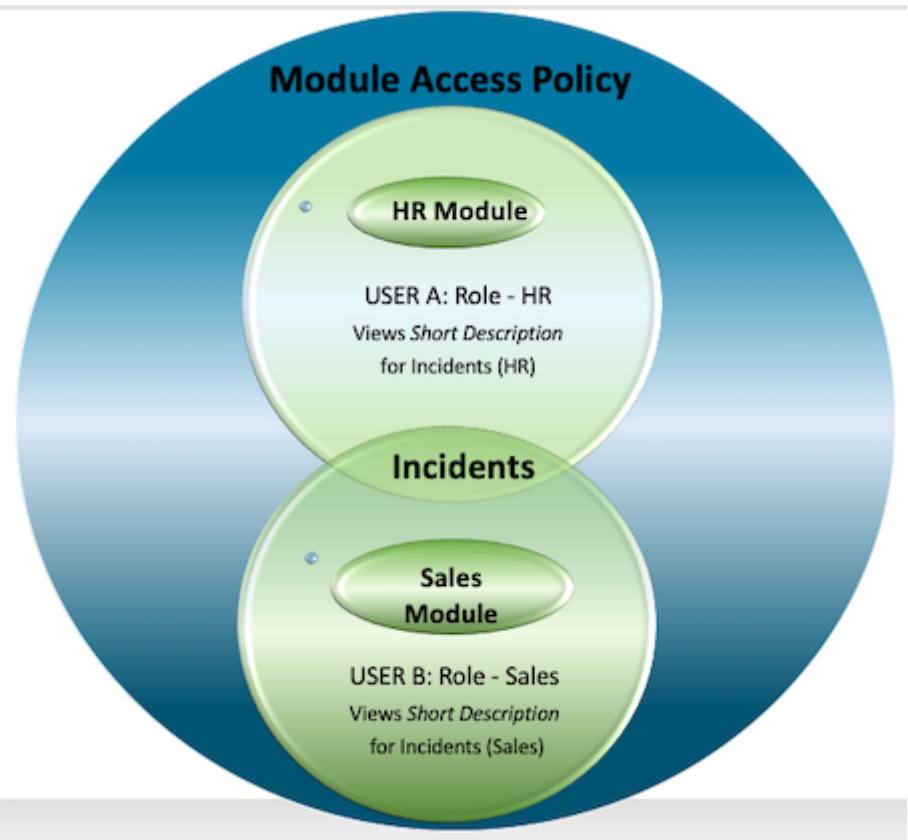
   Para o módulo A, conceda acesso aos usuários com uma função de RH. Para o módulo B, conceda acesso aos usuários com uma função de Vendas.

3. Crie um registro de Configuração de campo criptografado especificando a coluna Descrição resumida na tabela Incidente e certifique-se de selecionar **Módulos múltiplos** no campo **Método**.
4. Faça com que dois usuários, um com a função de RH (usuário A) e um com a função de Vendas (usuário B), criem um incidente com uma descrição resumida e, em seguida, faça com que ambos os usuários vejam a lista de incidentes.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A descrição resumida do incidente criado pelo usuário com a função de RH é criptografada pela chave do módulo A. Da mesma forma, a descrição resumida do incidente criado pelo usuário com a função de vendas é criptografada pela chave do módulo B.

Embora todos os usuários com as funções de RH e Vendas tenham acesso a incidentes, somente um usuário com a função de RH pode descriptografar e exibir a descrição resumida dos incidentes criados pelo usuário A, que tinha a função de RH. Da mesma forma, apenas os usuários com a função de Vendas podem descriptografar e visualizar as descrições resumidas dos incidentes criados pelo usuário B, que tinha a função de Vendas.



Criação de uma especificação criptográfica do Criptografia em nível de coluna

Depois de criar um módulo criptográfico, acesse a especificação criptográfica correspondente para definir o algoritmo.

Antes de Iniciar

Funções necessárias: sn_kmf.cryptographic_manager or sn_kmf_admin and security_admin or admin

Por Que e Quando Desempenhar Esta Tarefa

Este procedimento descreve as opções que estão disponíveis com o Criptografia em nível de coluna (CLE) com o sistema base e opções de configuração adicionais que se tornam disponíveis com a funcionalidade Criptografia em nível de coluna para empresas (CLE_Ent). A funcionalidade Criptografia em nível de coluna para empresas está disponível com uma assinatura paga. Consulte Pacote de assinatura do Gerenciamento de criptografia e chaves para conhecer os recursos suportados e as opções disponíveis com cada oferta.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Consulte Ativação do Criptografia em nível de coluna para empresas para obter mais informações sobre como obter Criptografia em nível de coluna para empresas.

Uma especificação criptográfica será criada pelo sistema quando você criar um módulo criptográfico para a criptografia do Criptografia em nível de coluna.

.

Procedimento

1. Navegue até **Segurança do sistema** > **Módulos de Edge Encryption** > **Todo**.
2. Selecione o módulo criptográfico para abrir as opções de configuração.
   As informações do módulo criptográfico são exibidas na parte superior da tela.
   Uma especificação de criptografia/descriptografia de dados simétricos é criada automaticamente com um algoritmo AES 256 CBC.
3. Selecione a especificação de criptografia na tabela para abrir a definição do algoritmo.
   Para Criptografia em nível de coluna para empresas consulte Configuração de algoritmos avançados para o Criptografia em nível de coluna para empresas.
4. Clique em **Avançar** para acessar o Ciclo de vida da chave.

O que Fazer Depois

Execute uma das seguintes operações:

- Selecione uma entrada na tabela Ciclo de vida da chave para definir o comportamento do ciclo de vida da chave. Consulte Configuração de estados do ciclo de vida da chave para obter detalhes para concluir a definição do ciclo de vida da chave.
- Clique em **Avançar** para criar uma chave criptográfica. Para obter detalhes sobre este processo, consulte Geração de uma chave criptográfica da ServiceNow.

Configuração de algoritmos avançados para o Criptografia em nível de coluna para empresas

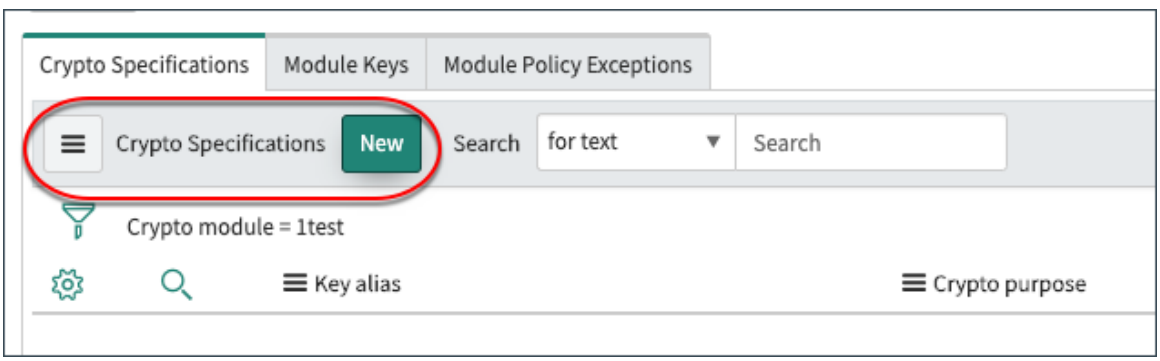
Crie uma especificação criptográfica para definir os algoritmos de um módulo criptográfico Personalize as especificações de criptografia com opções avançadas que estão disponíveis para o Criptografia em nível de coluna para empresas.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Na guia **Especificações de criptografia (#)**, clique em **Novo**.



2. No formulário, preencha os campos.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formulário de Definição de algoritmo

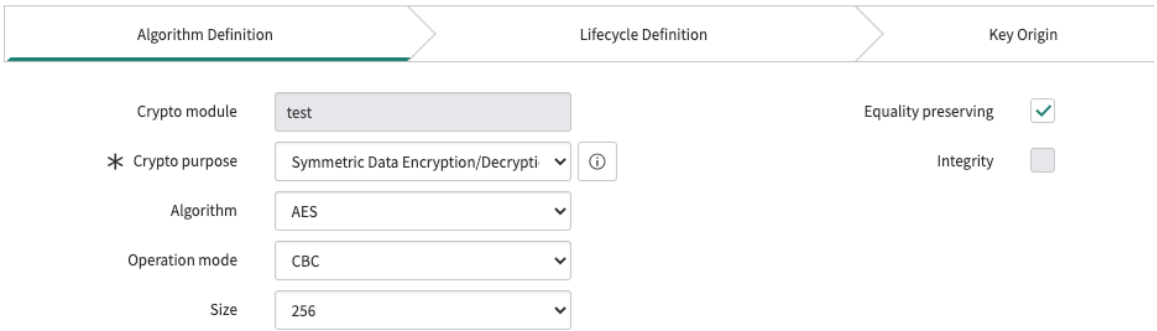
Campo	Descrição
Módulo de criptografia	O nome do módulo criptográfico selecionado é preenchido.
Finalidade da criptografia	O valor é **Criptografia/Descriptografia de dados simétrica** para o Criptografia em nível de coluna para empresas.
Algoritmo	O valor é **AES** para o Criptografia em nível de coluna para empresas.
Modo de operação	O valor é **CBC** para o Criptografia em nível de coluna para empresas.
Tamanho	Os valores possíveis são **256** e **128**. **Nota:** O tamanho de 256 bits é mais seguro para criptografia e é usado para Criptografia/descriptografia de dados simétrica em Criptografia em nível de coluna para empresas.
Preservação de Igualdade	Opção para habilitar a criptografia determinística. **Nota:** Selecionar esta opção significa que o valor criptografado de um campo deve ser o mesmo quando o valor do campo permanecer o mesmo. Opção para habilitar a **Criptografia/ descriptografia de dados simétrica** com o **AES** no modo de **Cipher Block Chaining (CBC)**.
Integridade	Opção para fornecer integridade na operação de GCM e não se aplica à funcionalidade Criptografia em nível de coluna para empresas.

3. Clique em **Enviar**.

O exemplo a seguir mostra a criptografia AES CBC-256. Quando Criptografia em nível de coluna para empresas está ativo e o módulo primário é column_level_encryption, somente se aplica criptografia/descriptografia de dados simétrica AES CBC-256 como a

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

finalidade da criptografia. Consulte Finalidade criptográfica, algoritmos e informações de chave para obter detalhes.



O que Fazer Depois

Execute uma das seguintes operações:

- Selecione uma entrada na tabela Ciclo de vida da chave para definir o comportamento do ciclo de vida da chave. Consulte Configuração de estados do ciclo de vida da chave para obter detalhes para concluir a definição do ciclo de vida da chave.
- Clique em **Avançar** para criar uma chave criptográfica. Consulte uma das tarefas a seguir para geração de chaves:
  - Geração de uma chave criptográfica da ServiceNow.
  - Configurar propriedades de chaves fornecidas pelo cliente.
  - Importação do par de chaves de encapsulamento/desencapsulamento.

Usar chaves fornecidas pelo cliente com a Criptografia em nível de coluna para empresas

Você pode usar sua própria chave fornecida pelo cliente em vez de usar as chaves geradas pelo sistema ServiceNow®.

Importante: Esses tópicos somente aplicam instâncias usando Criptografia em nível de coluna para empresas, que só está disponível com o plug-in `com.glide.now.platform.encryption`. Consulte Ativação do Criptografia em nível de coluna para empresas para mais informações sobre como obter este plug-in.

Com a Criptografia em nível de coluna para empresas, você pode usar suas próprias chaves para criptografia. Os administradores têm a opção de usar chaves fornecidas pela ServiceNow® ou suas próprias chaves fornecidas pelo cliente (CSK) para criptografia no Now Platform.

Importante: Para usar a opção de chave fornecida pelo cliente, você deve ter sua própria chave criptográfica.

Depois de ter sua chave, você pode usá-la em suas instâncias seguindo as etapas a seguir.

1. Configurar propriedades de chaves fornecidas pelo cliente

   Três propriedades do sistema definem o tamanho, o algoritmo de preenchimento e o período de validade do par de chaves de encapsulamento RSA. Revise essas propriedades e ajuste seus valores se os padrões não atenderem às suas necessidades.

2. Encapsule sua chave fornecida pelo cliente

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Use uma ferramenta criptográfica para encapsular sua chave, como o OpenSSL, para encapsular a chave simétrica a ser usada para criptografia com a chave pública baixada.

Configure e carregue a chave fornecida pelo cliente

Carregue sua chave encapsulada fornecida pelo cliente e configure o módulo criptográfico para começar a usar sua chave para criptografia em sua instância.

Configurar propriedades de chaves fornecidas pelo cliente

Se o plug-in Criptografia em nível de coluna para empresas estiver habilitado, você poderá usar as propriedades do sistema para definir o preenchimento da chave, o tamanho do par de chaves efêmero e um período de validade para as chaves fornecidas pelo cliente.

O Criptografia em nível de coluna para empresas com Key Management permite que você gerencie todo o ciclo de vida de suas chaves de criptografia de dados. Também é possível trocar as chaves de criptografia de dados geradas em seu ambiente com segurança.

A Criptografia da plataforma com a Gestão de chaves permite que você gerencie todo o ciclo de vida de suas chaves de criptografia de dados. Também é possível trocar as chaves de criptografia de dados geradas em seu ambiente com segurança.

Propriedades do sistema para definir atributos de par de chaves

Ao fornecer sua própria chave, você deve encapsulá-la com a chave pública RSA. Três propriedades definem o tamanho, o algoritmo de preenchimento e o período de validade do par de chaves de encapsulamento RSA:

- *glide.kmf.ephemeral_key.key_padding* controla o esquema de preenchimento de chave da chave efêmera. O esquema padrão é OAEP SHA256, mas SHA1 também é compatível.
- *glide.kmf.ephemeral_key.key_size* controla as dimensões de chave do par de chaves efêmeras. O padrão é 4096 bits, mas 2048 bits também são compatíveis.
- *glide.kmf.ephemeral_key.key_validity_period* define o período de validade do par de chaves efêmeras. O valor padrão é 2 horas.

Depois que a chave de criptografia de dados for importada para a instância, uma chave de encapsulamento segura protegerá as novas chaves do módulo na instância. A chave de encapsulamento é uma chave de criptografia de instância (IKEK) gerada por um módulo de segurança de hardware (HSM) no SafeNet KeySecure. Consulte Chaves de nível de instância na estrutura de gerenciamento de chave para obter detalhes sobre os tipos de chave.

Continuar para Encapsule sua chave fornecida pelo cliente.

Encapsule sua chave fornecida pelo cliente

Encapsule a chave simétrica a ser usada para criptografia com a chave pública baixada.

Antes de Iniciar

Nota: Este procedimento descreve as opções que estão disponíveis com o sistema de base KMF e as opções a serem usadas com a funcionalidade Criptografia em nível de coluna para empresas. A funcionalidade Criptografia em nível de coluna para empresas estará disponível somente quando o plug-in *com.glide.now.platform.encryption* estiver ativo. Consulte Ativação do Criptografia em nível de coluna para empresas para obter mais informações sobre como obter Criptografia em nível de coluna para empresas.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Algumas das etapas neste documento exigem o uso de uma ferramenta criptográfica instalada no seu dispositivo local. Os exemplos nesta tarefa usam a ferramenta OpenSSL. Para obter mais informações sobre essa ferramenta, consulte https://www.openssl.org. Se estiver usando outras ferramentas criptográficas, como LibreSSL ou GnuTLS, consulte a documentação desses produtos para obter etapas semelhantes.

- Modifique as propriedades opcionais que controlam o tamanho, o algoritmo de preenchimento e o período de validade da chave. Consulte Configurar propriedades de chaves fornecidas pelo cliente.

- Você deve ter sua chave simétrica (.BIN) para criptografia.

  Importante: Sua chave deve estar no formato binário. Se outro formato for usado, será `exibida uma mensagem de erro informando. Anexe novamente o token não modificado.` que a validação do token falhou.

- Você deve ter uma ferramenta criptográfica para encapsular sua chave. Este exemplo usa o OpenSSL 1.1.

Função necessária: sn_kmf.cryptographic_manager ou sn_kmf.admin

Procedimento

1. Navegue até **Todos** > **Key Management Framework** > **Módulos Criptográficos** > **Todos**.
2. Selecione o módulo criptográfico criado para a chave fornecida pelo cliente na lista relacionada Especificações de criptografia.
3. Você será direcionado para a etapa de **Criação de chave**.
4. Se ainda não tiver baixado a chave de encapsulamento, clique no link para baixar o arquivo *token_publickey<id>.zip* e salve-o no mesmo local de sua chave.

   Nota: Não renomeie o arquivo *token_publickey<id>* baixado.

5. Descompacte o arquivo em sua rede local.
   O arquivo zip contém dois arquivos, um token de importação e um certificado `.PEM` de chave pública. Encapsule sua chave simétrica com a chave pública para criptografá-la.
6. Copie o nome do arquivo *token_publickey* para a área de transferência.
7. Em uma linha de comando, use o nome do arquivo *token_publickey* copiado para abrir a pasta dos arquivos descompactados como um espaço reservado para a chave encapsulada.
8. Edite este script substituindo os exemplos pelos nomes de seus arquivos de criptografia.

```
"downloads user.name$ cd token_publickey_<token>
openssl pkeyutl -encrypt -pubin -inkey publickey_<keyname>.PEM
-in <keyname.bin>
-out wrapped_key_material -pkeyopt rsa_padding_mode:oaep -pkeyopt
 rsa_oaep_md:sha<128 or 256> "
```

   Revise os comandos de encapsulamento de chave na tabela a seguir para obter mais informações.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Comandos de encapsulamento de chave

Direções	Comando	Exemplo
Abra o diretório do arquivo no qual você baixou o token de encapsulamento.	`cd`	`cd token_publickey123456789`
Cole o nome do certificado `publickey.PEM`.	`openssl pkeyutl -encrypt -pubin -inkey`	`publickey_586798643ffff.PEM`
Cole o nome da sua chave aqui.	`-in`	`mykey.bin`
Insira o comando <-out> e especifique se a chave é de 128 bits ou 256 bits.	`-out wrapped_key_material -pkeyopt rsa_padding_mode:oaep -pkeyopt rsa_oaep_md:sha256`	N/D

9. Execute o comando:
   Uma mensagem do sistema exibe `token_publickey_<keynumber>`. A chave será gerada e um arquivo *`wrapped_key_material`* adicionado ao diretório.
10. Carregue a chave encapsulada.

O que Fazer Depois

Retorne para Configure e carregue a chave fornecida pelo cliente para carregar sua chave encapsulada.

Configure e carregue a chave fornecida pelo cliente

Você pode usar sua própria chave fornecida pelo cliente em vez de usar as chaves geradas pelo sistema ServiceNow®.

Antes de Iniciar

Funções necessárias: security_admin e sn_kmf.cryptographic_manager

Se você NÃO estiver fornecendo suas próprias chaves, não precisará executar este procedimento. Para criar um módulo criptográfico com chaves ServiceNow®, vá para Criação de um módulo criptográfico ou Criação de um módulo criptográfico do Criptografia em nível de coluna..

Nota: Este procedimento se aplica apenas à funcionalidade Criptografia em nível de coluna para empresas. Para obter mais informações, consulte Ativação do Criptografia em nível de coluna para empresas.

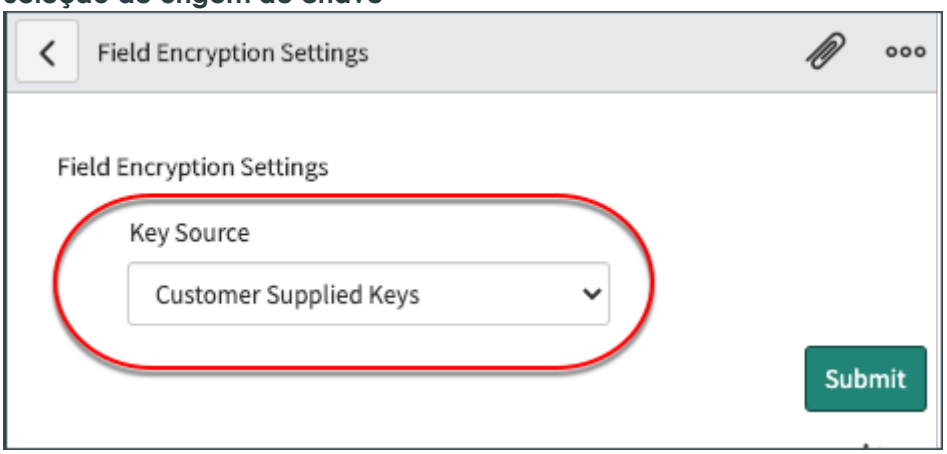
Importante: Você não pode revogar uma chave fornecida pelo cliente.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

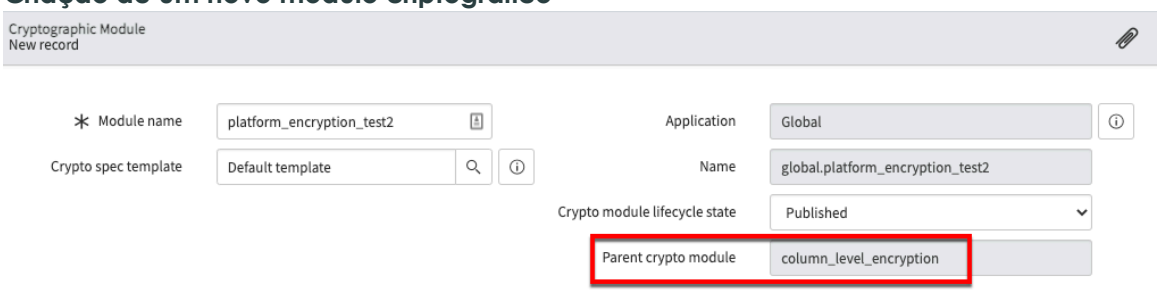
1. Navegue até **Todos** > **Segurança do sistema** > **Configurações de Edge Encryption** e verifique se **Chaves fornecidas pelo cliente** está selecionado.

Seleção de origem de chave



2. Selecione **Enviar**.
3. Retornar para **Segurança do sistema** > **Módulos de Edge Encryption** > > **Criar novo**.

Criação de um novo módulo criptográfico



4. Preencha o formulário do Módulo criptográfico da seguinte forma:

Campos do Módulo criptográfico

Campo	Descrição
Nome do módulo	Insira um nome para o módulo.
Modelo de especificação de criptografia	O modelo criptográfico padrão foi selecionado.
Nome	Preenche automaticamente de acordo com o nome do módulo e o adiciona ao escopo para garantir qual aplicação está sendo aplicada. Nesse caso, foi aplicado o escopo global.
Estado do ciclo de vida do módulo de criptografia	Selecione **Publicado** para ativar o módulo de criptografia.

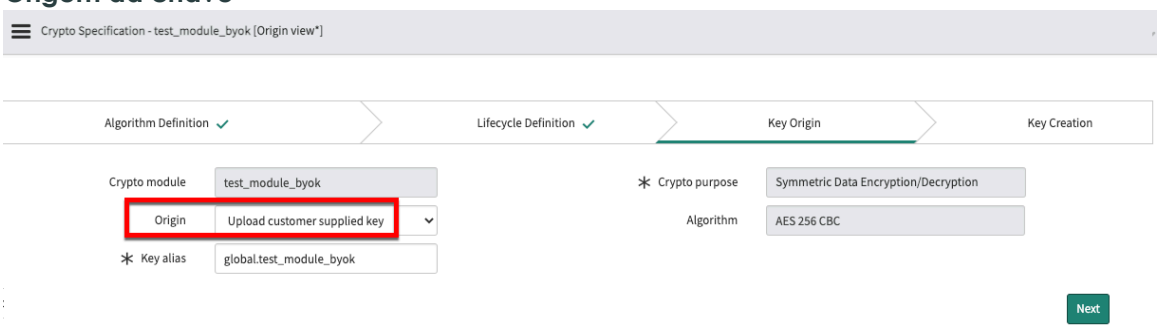
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Módulo de criptografia primário	O módulo primário **column_level_encryption** é selecionado automaticamente ao usar chaves fornecidas pelo cliente e módulos de criptografia.

5. Selecione **Enviar**.
6. Selecione o módulo criptográfico recém-criado na tabela.
   Na lista relacionada **Especificações de criptografia**, clique no alias de chave gerado automaticamente com o algoritmo AES 256 CDB.

   O sistema preenche a Finalidade da criptografia e o Algoritmo do CLE automaticamente e passa para o estágio de **Origem da chave**.
7. Observe que **Carregar chave fornecida pelo cliente** é a **Origem** e que o **Alias da chave** já está preenchido.

Origem da chave



8. Selecione **Avançar** para ir para o estágio **Criação de chave**.

   Existem dois links:

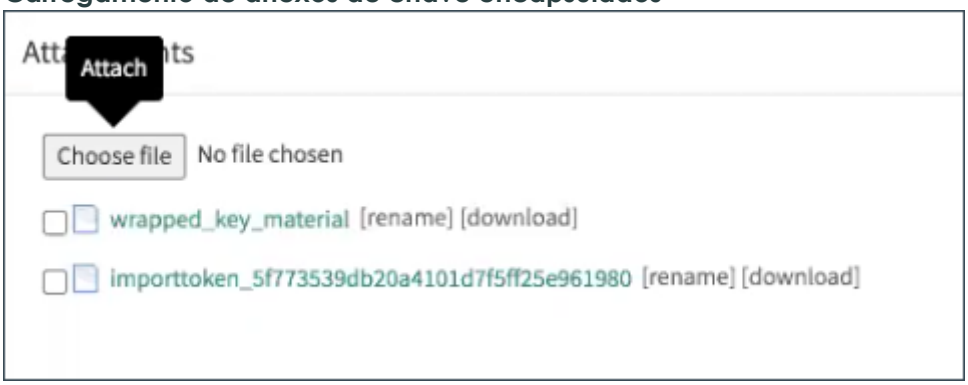
   - **Baixar chave de encapsulamento** baixa a chave em um arquivo zip que contém um token de importação e um certificado de chave pública, arquivo `.PEM`. Use o token de importação para verificar se o encapsulamento da chave foi bem-sucedido de acordo com a especificação de segurança para a instância. Use o arquivo `.PEM` de certificação de chave pública para encapsular a chave fornecida pelo cliente com segurança antes de carregá-la junto com o token.
   - **Carregar chave fornecida pelo cliente** abre o navegador de arquivos para seleção do token e da chave criptografada que você encapsulou.

Links de carregamento de criação de chave

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

9. Selecione **Fazer download da chave de encapsulamento** para salvar o token.
   Salve o token no mesmo local de destino em que a chave foi salva no sistema. Não renomeie o token baixado.
10. Execute o comando BYOK em um terminal para encapsular a chave.
    Para obter mais informações, consulte Encapsule sua chave fornecida pelo cliente.
11. Selecione **Carregar chave fornecida pelo cliente**.
12. Clique em **Navegar** para selecionar os dois arquivos, a chave encapsulada e o arquivo de token.
    A janela Anexos exibe os dois arquivos.

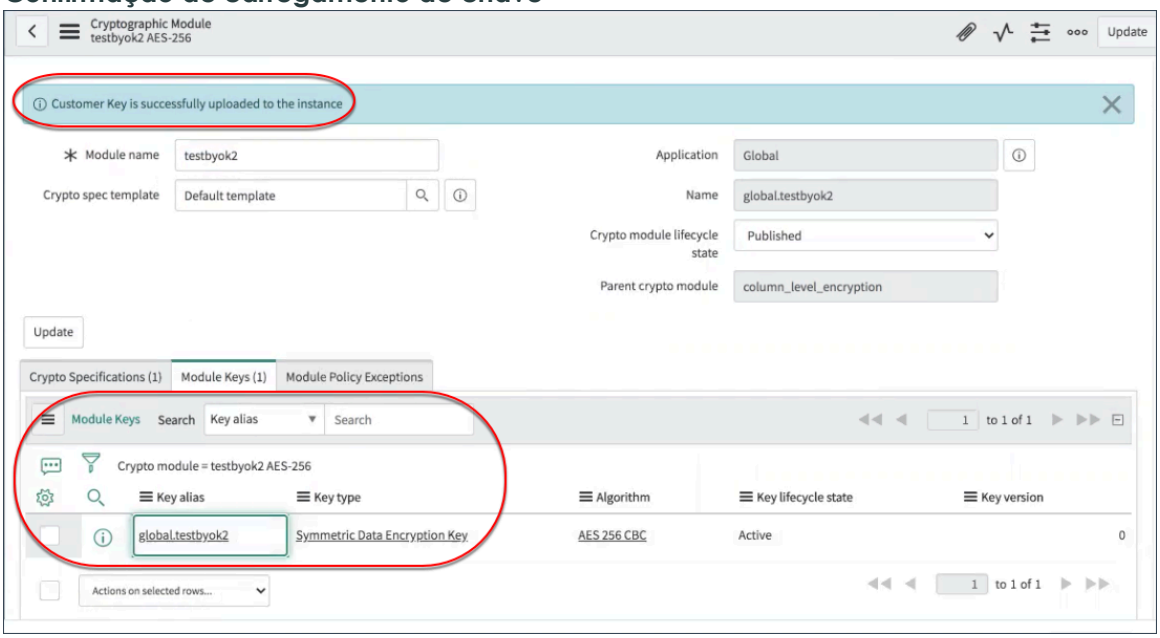
Carregamento de anexos de chave encapsulados



Selecione um arquivo para remover e carregar novamente, se necessário.

13. Selecione **OK**.
    Você retornou à tela do Módulo criptográfico. Uma mensagem de confirmação será exibida caso o carregamento da chave do cliente tenha sido bem-sucedido. A chave também será listada na lista relacionada de chaves de módulo.

Confirmação de carregamento de chave



O que Fazer Depois

Agora que concluiu a configuração do módulo criptográfico com a chave fornecida pelo cliente, prossiga para Criação de uma política de acesso ao módulo

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Como criptografar campos e anexos

Depois de criar seus módulos criptográficos, crie configurações de campo criptografado e especifique se deseja criptografar um campo em uma tabela ou criptografar anexos.

Como criptografar campos

Nota: Campos criptografados não são auditados por natureza. Este comportamento não é configurável.

1. Especifique a origem da chave: chaves geradas pelo sistema ou chaves fornecidas pelo cliente (traga sua própria chave) em **Segurança do sistema** > **Configurações de Edge Encryption**.
2. Depois de especificar a origem da chave, crie um novo módulo criptográfico ou use um módulo criptográfico existente. Comece com Criação de um módulo criptográfico para obter instruções.

   Nota: Caso use chaves fornecidas pelo cliente, siga as instruções em Criação de um módulo criptográfico do Criptografia em nível de coluna. e Configurar propriedades de chaves fornecidas pelo cliente.

3. Crie uma configuração de campo criptografado, onde especificará a tabela na qual a criptografia será realizada e a coluna na tabela ou os anexos na tabela a serem criptografados. Consulte Definição das configurações de campo criptografado para começar.

Nota: Consulte Exemplos da Criptografia em nível de coluna para empresas, que ilustra como criptografar campos e anexos usando chaves fornecidas pelo cliente.

Definição das configurações de campo criptografado

Configure quais as colunas de tabela ou anexos o sistema vai criptografar usando um módulo criptográfico pré-configurado.

Antes de Iniciar

Funções necessárias: sn_kmf.cryptographic_manager e security_admin ou eleve a função para administrador de segurança.

Por Que e Quando Desempenhar Esta Tarefa

Verifique se você está no escopo da aplicação correto para ver as tabelas nesse escopo.

Somente usuários com acesso ao módulo criptográfico usado nessa configuração de campo criptografado podem ler os dados na coluna da tabela criptografada ou acessar o anexo.

- Se um usuário tiver acesso de gravação, mas não de leitura, o campo será exibido no modo de edição e os dados inseridos serão exibidos como asteriscos.
- Se um usuário tiver acesso de leitura, mas não de gravação, o campo exibirá os dados descriptografados no modo somente leitura.
- Se um usuário tiver acesso total, as funcionalidades de leitura/gravação estarão disponíveis no campo criptografado.

Veja Criação de um módulo criptográfico ou Criação de um módulo criptográfico do Criptografia em nível de coluna. para começar.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Importante:

Depois de criptografar uma coluna, todos os novos dados inseridos nela são criptografados automaticamente. No entanto, os dados que existiam na coluna antes de a criptografia estar ativa não são criptografados automaticamente.

Para criptografar dados que existiam antes da criptografia da coluna, você deve executar um trabalho de criptografia em massa separado. Saiba mais sobre criptografia em massa em Execução de criptografia ou descriptografia em massa.

Procedimento

1. Navegue até **Tudo** > **Segurança do sistema** > **Edge Encryption** > **Configurações de Edge Encryption** > **Novo**.
2. Selecione **Novo**.
3. Preencha o formulário.

Campo	Descrição
Tipo	**Coluna** para criptografar uma coluna de tabela ou **Anexo** para criptografar todos os anexos de uma tabela. Os tipos de dados criptografados são: ◦ Texto de cadeia de caracteres (UTF-8 completo) ◦ Anexos ◦ Data, Data/Hora: **Nota:** Você pode criar configurações de campo criptografado para criptografar os campos de Data e Data/Hora existentes. Você pode adicionar uma nova configuração de criptografia somente a uma tabela primária. Você não pode adicionar uma nova configuração de criptografia a uma tabela secundária. ◦ URL ◦ Criptografia em nível de coluna para empresas também é compatível com os seguintes tipos de campo: ▪ HTML ▪ Diário ▪ Traduzido
Tabela	Tabela cujos campos ou anexos devem ser criptografados.
Coluna	Coluna (campo) a ser criptografada se você selecionou o tipo **coluna**.
Ativo	Selecione para marcar a configuração ativa. Desmarque se a configuração ainda não estiver em uso.
Módulo criptográfico	O módulo criptográfico ao qual a configuração de campo criptografado se aplica.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Método	Selecione **Módulo único** para definir a configuração de campo em um módulo. Selecione **Módulos múltiplos** para acesso baseado em função que se estende por mais de um módulo criptográfico. Módulo único Use esta opção para criptografar todos os anexos usando um único módulo. Seus usuários precisam de acesso a esse módulo; caso contrário, não poderão carregar anexos. Módulos Múltiplos Use esta opção para permitir que os usuários escolham um módulo ao carregar anexos. Usuários com acesso a pelo menos um módulo podem selecionar um módulo a ser usado para criptografia. Usuários sem acesso ao módulo podem carregar anexos não criptografados.
Preservação de algoritmo criptografado [read-only] (somente leitura)	Indica se o módulo de criptografia selecionado já está configurado para oferecer suporte à criptografia não determinística. Isso significa que se os mesmos dados forem criptografados mais de uma vez, a criptografia será diferente a cada vez.

4. Selecione **Enviar**.

Acesso de script para módulos criptográficos

Os scripts podem ser executados para acessar uma política de módulo criptográfico de uma finalidade criptográfica.

No caso do Estrutura de gestão principal, as políticas podem ser os scripts baseados. Quando uma política de acesso é acionada para acesso ao script, o script de back-end pode executar as ações de política do módulo a partir do script.

Os módulos criptográficos podem oferecer suporte a uma ou mais finalidades de criptografia, como descriptografia de dados assimétrica e descriptografia de dados simétrica. Cada finalidade criptográfica requer a geração de uma chave de criptografia e a definição de uma finalidade criptográfica.

Considere o seguinte ao executar uma solicitação de script de criptografia:

- A finalidade criptográfica referenciada deve ser definida no módulo criptográfico.
- Deve existir uma chave ativa gerada para o módulo criptográfico.
- O tipo de Política de acesso ao módulo deve ser definido como **script**.

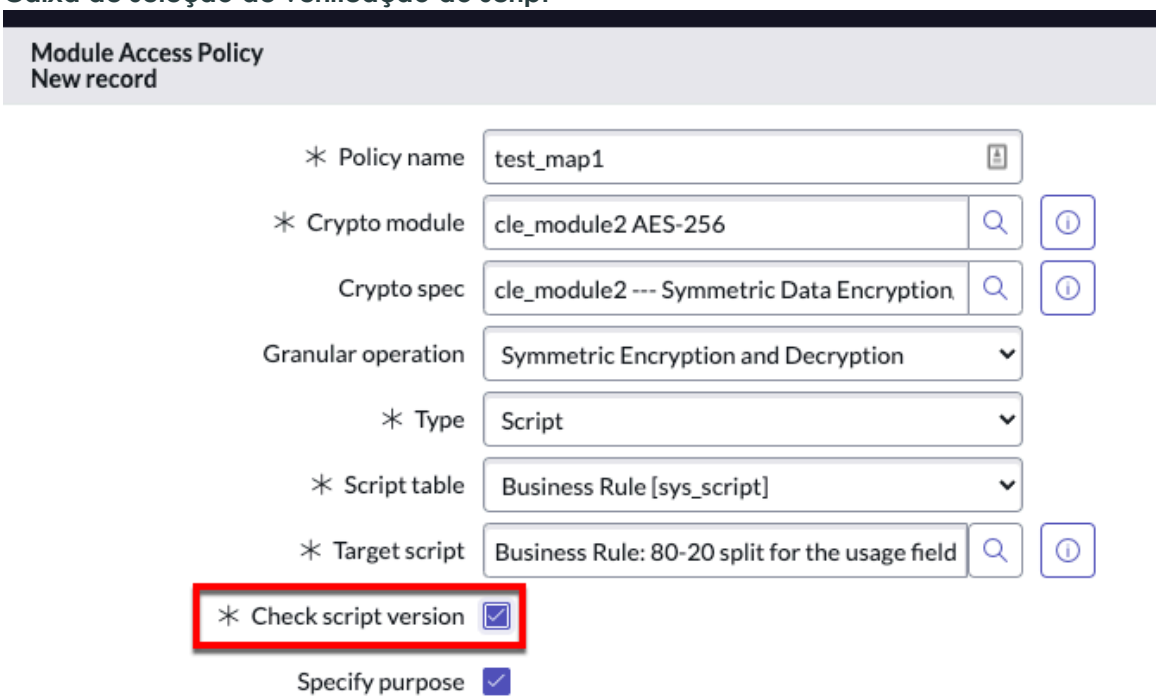
Verificação de versão de script

Ao criar uma política de acesso ao módulo definida como tipo script, há uma opção disponível para validar a integridade da versão do script que está sendo acessada. Somente a versão atribuída do script tem permissão para acessar os módulos de criptografia. Quando a caixa de seleção **Verificar versão do script** estiver marcada na

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

política de acesso ao módulo, sempre que o script for executado, o sistema executará uma comparação de versão. Se o script tiver sido alterado, o usuário será notificado.

Caixa de seleção de verificação do script



Configuração de acesso do script a dados criptografados

Execute um script para executar a política do módulo criptográfico de uma finalidade criptográfica. O acesso específico de leitura (descriptografia/desencapsulamento) ou de gravação (criptografia, encapsulamento) pode ser definido com base na granularidade da operação da política de acesso ao módulo.

Antes de Iniciar

Função necessária: sn_kmf.cryptographic_manager

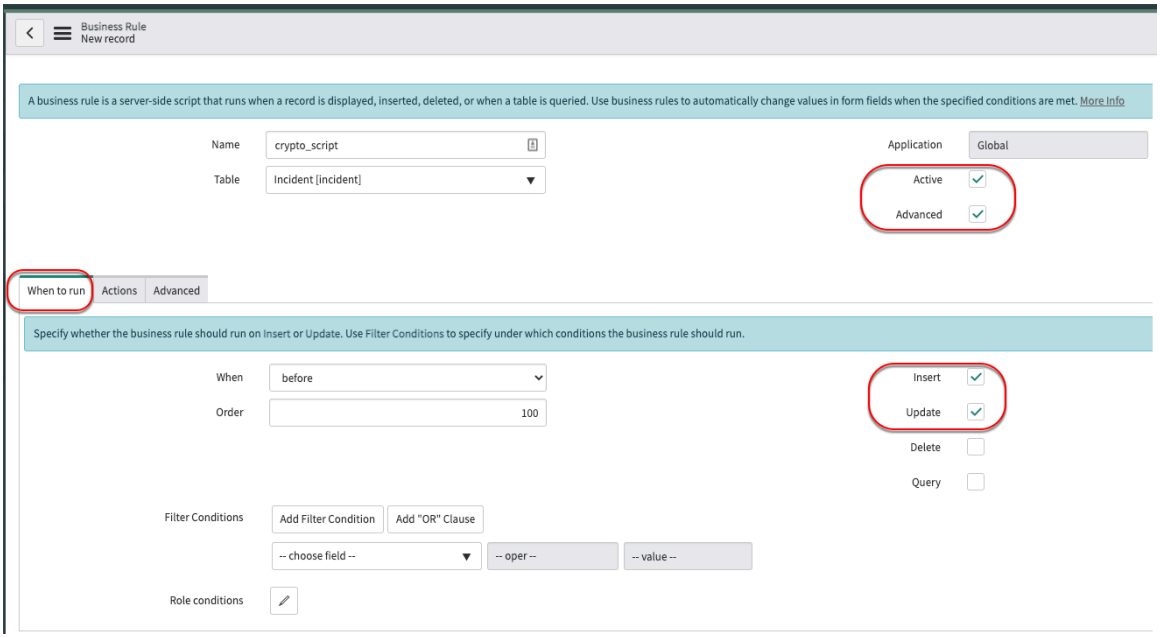
Por Que e Quando Desempenhar Esta Tarefa

Regras de negócios e Inclusões de script são exemplos de usos. Este procedimento usa um script para Regras de negócio.

Procedimento

1. Crie um módulo criptográfico com o algoritmo de criptografia/ descriptografia de dados simétrica.
   Consulte Criação de um módulo criptográfico para saber detalhes. O acesso específico aos dados ou ao anexo é controlado com uma política de acesso ao módulo com as seguintes características:
   - Criptografia simétrica: o script pode criptografar dados, mas não pode descriptografar os dados.
   - Descriptografia simétrica: o script pode descriptografar dados criptografados carregados, mas não pode criptografar os dados ou anexos.
   - Criptografia e descriptografia simétricas: o script pode criptografar e descriptografar dados ou anexos.
2. Navegue até **Definições do sistema** > **Regras de negócio**.
3. Clique em **Novo**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



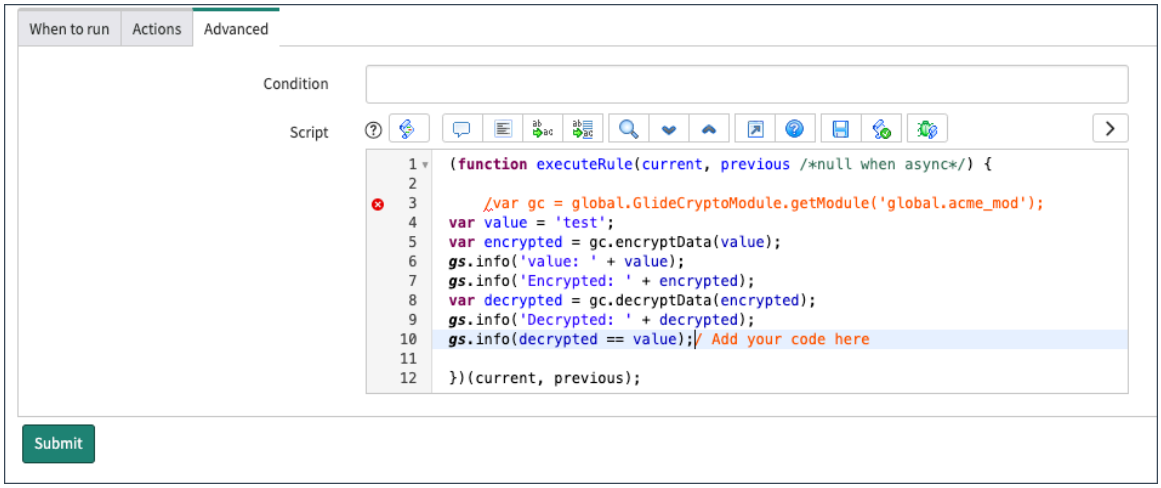
4. Preencha o formulário na guia **Quando executar** e insira o script na guia **Avançado** :

Campos da Regra de negócio

Campo	Descrição
Nome	Insira um nome para a regra de negócio.
Tabela	Selecione **Incidente [incidente]**na lista suspensa.
Aplicação	**Global** está selecionado por padrão.
Ativo	Marque a regra como **Ativa**.
Avançado	Marque a caixa de seleção para exibir opções avançadas.
Guia Quando executar	Na guia **Quando executar**, habilite os campos **Inserir** e **Atualizar**.

Guia Avançado	Na guia **Avançado**, cole o seguinte texto de script na linha 3:
	`//`
	`var gc = global.GlideCryptoModule.getModule('global.acme_mod');`
	`var value = 'test';`
	`var encrypted = gc.encryptData(value);`
	`gs.info('value: ' + value);`
	`gs.info('Encrypted: ' + encrypted);`
	`var decrypted = gc.decryptData(encrypted);`
	`gs.info('Decrypted: ' + decrypted);`
	`gs.info(decrypted == value);`
	Nota: Consulte a imagem "Guia avançada de regras de negócio" para obter detalhes.

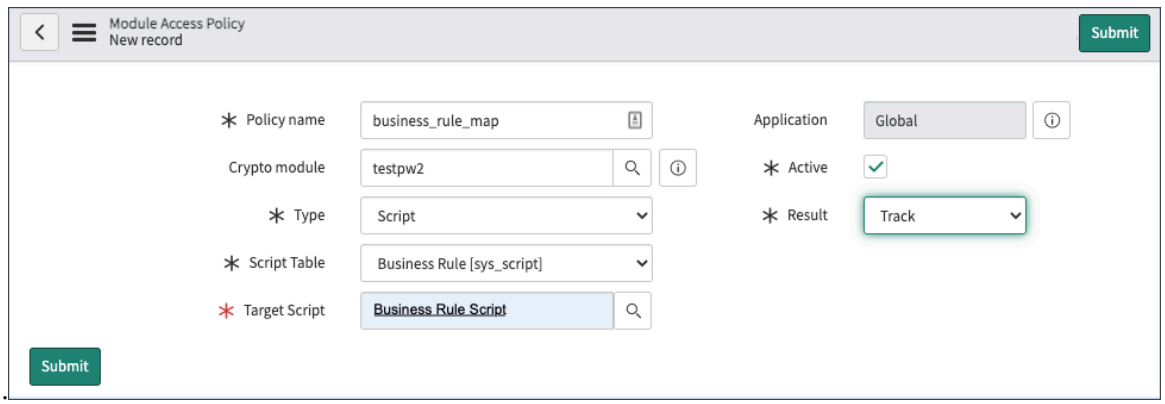
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Clique em **Enviar**.
6. Navegue até **Gerenciamento de chave** > **Políticas de acesso ao módulo** > **Todas**.

> **Nota:** Para obter informações adicionais, consulte Criação de uma política de acesso ao módulo.

7. Clique em **Novo**.
8. Preencha o formulário.



Campos de Políticas de acesso ao módulo

Campo	Descrição
Nome da política	Insira um nome para a política.
Módulo criptográfico	Clique no ícone de pesquisa para selecionar um módulo com o algoritmo de criptografia/descriptografia de dados simétrica.
Tipo	Selecione **Script** para controlar o acesso por script.
Tabela de Scripts	Selecione um valor na lista suspensa da tabela de scripts. Para este exemplo, selecione **Regra de negócio [sys_script]**.
Scripts de destino	Selecione o documento de script para a política. Selecione o **Nome da tabela** e o documento relacionado à política. Nes-

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	te exemplo, selecione a regra de negócio que você criou nas etapas anteriores.
Ativo	Selecione para ativar a política.
Resultado	Para conceder ao script acesso ao módulo, selecione **Acompanhar** no campo **Resultado**.

9. Clique em **Enviar**.
   A política de acesso ao módulo do script ficará agora disponível no sistema.

Exibir solicitações de uso do módulo criptográfico recusadas

Exibir módulos criptográficos que rejeitaram solicitações de criptografia feitas por scripts devido a mecanismos de criptografia incompatíveis.

Antes de Iniciar
Função necessária: sn_kmf.cryptographic_manager

Por Que e Quando Desempenhar Esta Tarefa
Os módulos criptográficos podem oferecer suporte a uma ou mais finalidades de criptografia, como descriptografia de dados assimétrica e descriptografia de dados simétrica. Os dados criptografados só podem ser acessados com base na política de acesso ao módulo. Se um script tentar usar um módulo criptográfico para uma finalidade não definida no módulo, não poderá acessar os dados criptografados.

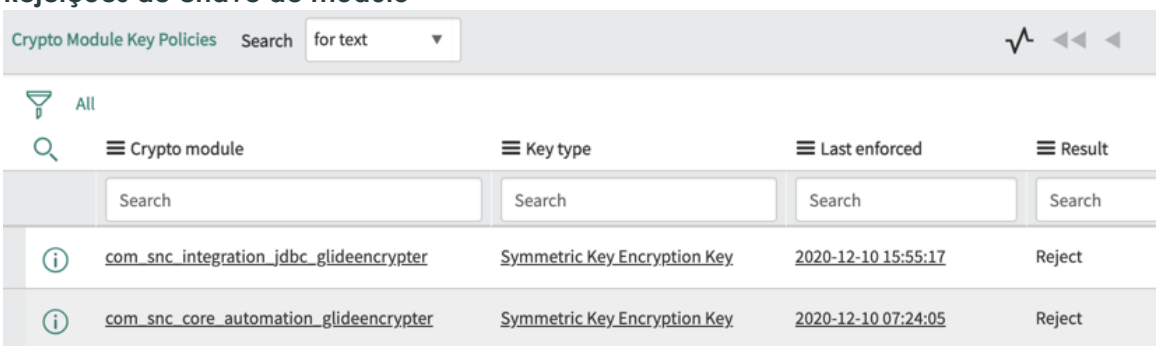
No exemplo a seguir, uma finalidade criptográfica foi atribuída a um módulo criptográfico, mas nunca foi gerada uma chave ele.

Procedimento

Navegue até **Todos** > **Gerenciamento de chave** > **Políticas de chave do módulo** > **Rejeições de chave do módulo** .

Será exibida uma lista de módulos criptográficos que rejeitaram solicitações junto com a chave de criptografia usada no script correspondente.

Rejeições de chave de módulo



Nota: Se um script diferente tentar usar o mesmo módulo criptográfico usando o mesmo tipo de chave, o valor de **Imposto pela última vez** será atualizado. Não será gerada outra linha.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Neste exemplo, em 2020-02-10_15:55:17, o primeiro módulo rejeitou uma solicitação porque a chave do módulo1 foi comprometida. Em 2020-02-10_07:24:05, o segundo módulo rejeitou uma solicitação porque a chave do segundo módulo estava suspensa.

Para conceder a permissão para que os scripts usem o módulo de criptografia na próxima vez em que forem executados, crie uma política de acesso ao módulo para a criptografia de script. Para obter mais informações, consulte Configuração de acesso do script a dados criptografados.

Programação de criptografia em massa, descriptografia e trabalhos de recriação de chaves

Programe trabalhos de criptografia, descriptografia e recriação de chaves para serem executados no horário mais adequado à sua instância.

Antes de Iniciar

Os trabalhos de criptografia, descriptografia e recriação de chaves podem consumir muito tempo e recursos. Portanto, considere programá-los em horários que não sejam de pico. Certifique-se também de que o usuário que programa o trabalho tenha o acesso apropriado para cada trabalho.

Função necessária: sn_kmf.cryptographic_manager

Por Que e Quando Desempenhar Esta Tarefa

A criptografia e a descriptografia em massa também estão disponíveis no formulário Configurações de campo criptografado. Consulte Execução de criptografia ou descriptografia em massa para obter instruções.

Procedimento

1. Navegue até **Todos** > **Segurança do sistema** > **Configurações de alta segurança** > **Trabalhos de segurança**.
2. Clique em **Nova**.
3. Preencha o formulário de programação.

Campo	Descrição
Nome	Nome do trabalho de criptografia, descriptografia ou recriação de chave.
Tipo	Tipo de trabalho: ◦ **Migração de chave de contexto para módulo:** migração em massa de chaves de contexto de criptografia para módulos de criptografia, incluindo a criação de registros de políticas de acesso ao módulo para controles de acesso nos módulos de criptografia ◦ **Contexto de migração de dados para módulo**: migra dados criptografados por contextos de criptografia para módulos de criptografia ◦ **Anexo de descriptografia em massa**: descriptografa todos os anexos criptografados em registros para uma única tabela definida no campo **Tabela**. ◦ **Anexo de criptografia em massa**: criptografa todos os anexos criptografados em registros para uma única tabela definida no campo **Tabela**. ◦ **Módulo de criptografia em massa**: criptografa qualquer valor preexistente na coluna/campo definido usado na Configuração de Edge Encryption

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	◦ **Módulo de descriptografia em massa**: descriptografa qualquer valor preexistente na coluna/campo definido usado na Configuração de Edge Encryption com o módulo único. ◦ **Módulo múltiplo de descriptografia em massa**: descriptografa qualquer valor preexistente na coluna/campo definido usado na Configuração de Edge Encryption com módulos múltiplos. ◦ **Módulo de recriação de chaves**: criptografa novamente qualquer valor preexistente na coluna/campo definido usado na configuração de Edge Encryption usando a chave ativa atual do módulo. ◦ **Migração de contexto de anexo para módulo**: criptografa qualquer anexo pré-existente na tabela definida na configuração de Edge Encryption. Qualquer anexo criptografado anteriormente com um contexto é criptografado novamente com o módulo.
Estado	O estado inicial do trabalho é Novo. Após sua execução conforme programado, o estado será atualizado de acordo.
Início da janela de tempo	Hora de início do trabalho no formato 24h.
Término da janela de tempo	Hora de finalização do trabalho no formato 24h.
Tabela	Tabela a ser criptografada ou descriptografada.
Campo	Campo a ser criptografado ou descriptografado.
Resumo	Informações de status do trabalho quando ele estiver em execução, for concluído ou apresentar erros.

Nota: Por causa da sobrecarga do sistema, você deve programar a execução de trabalhos de criptografia, descriptografia e recriação de chaves em massa em horários fora de pico. O Now Platform executa o trabalho entre o **Início da janela de tempo** e o **Término da janela de tempo**. Se o trabalho não for concluído em uma janela de processamento, ele continuará durante a próxima janela de processamento especificada até que todo o processamento seja concluído.

4. Clique em **Enviar**.
5. Depois de programar um trabalho, é possível pode fazer o seguinte.
   - Clicar em **Cancelar trabalho** para cancelar um trabalho em execução.
   - Clicar em **Iniciar** para iniciar um trabalho imediatamente.
   - Clicar em **Atualizar** para salvar quaisquer mudanças feitas na programação do trabalho.
   - Clicar em **Excluir** para excluir o trabalho agendado.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Execução de criptografia ou descriptografia em massa

Você pode executar a criptografia em massa em configurações de criptografia, bem como uma descriptografia em massa para descriptografar valores anteriormente criptografados.

Antes de Iniciar
Função necessária: security_admin

Por Que e Quando Desempenhar Esta Tarefa
Você também pode criar trabalhos agendados de criptografia e descriptografia em massa. Consulte Programação de criptografia em massa, descriptografia e trabalhos de recriação de chaves para obter instruções.

A criptografia e a descriptografia em massa estão disponíveis somente quando uma configuração de campo criptografado usa o módulo criptográfico único. A descriptografia em massa está disponível para os métodos de criptografia único e múltiplo.

Nota: A criptografia e a descriptografia em massa devem ser executadas apenas fora dos horários de pico porque as operações consomem muitos recursos e tempo.

Procedimento
1. Navegue até **Todos** > **Segurança do sistema** > **Edge Encryption** > **Configurações de campo criptografado**.
2. Abra a configuração de campo criptografado do campo que deseja criptografar ou descriptografar em massa.
3. Em Links relacionados, selecione uma opção disponível.
   - **Programar trabalho de descriptografia em massa**
   - **Programar trabalho de criptografia em massa**
4. Confirme sua seleção na caixa de diálogo.

Resultados
Se estiver executando uma criptografia em massa, todos os valores serão criptografados tendo o módulo de criptografia definido no registro de configuração do campo criptografado. Se uma descriptografia em massa estiver sendo executada, somente os campos criptografados com um módulo de criptografia ao qual você tem acesso serão descriptografados.

Exemplos da Criptografia em nível de coluna para empresas

Estes exemplos orientam você na criptografia de campos e anexos usando chaves fornecidas pelo cliente.

Tutorial de Edge Encryption

Este passo a passo mostra como criptografar um campo em sua instância usando o Criptografia em nível de coluna para empresas com o Estrutura de gestão principal (KMF). Ele também mostra como usar sua própria chave.

Antes de Iniciar

Nota: Este procedimento se aplica apenas à funcionalidade Criptografia em nível de coluna para empresas. Consulte Ativação do Criptografia em nível de coluna para empresas para obter mais informações sobre como obter Criptografia em nível de coluna para empresas.

Função necessária: admin ou security_admin

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: security_admin é uma função privilegiada, para obter detalhes sobre como usar funções privilegiadas, consulte Elevar para uma função privilegiada.

Por Que e Quando Desempenhar Esta Tarefa

Este passo a passo começa com uma instância em que você já criou e carregou sua chave criptográfica pessoal. Você pode usar a chave da ServiceNow, mas este exemplo usa uma chave fornecida pelo cliente.

Depois que a chave foi armazenada em um módulo criptográfico, comece a configurar campos em sua instância com acesso limitado de determinados usuários, como salário ou número de CPF. Em Configuração de campo criptografado, especifique qual equipe autorizada pode acessar dados confidenciais.

Esta tarefa demonstra dois cenários. Um exemplo criptografa o campo **Descrição resumida** em um incidente para usuários que não estão autorizados a exibir os dados confidenciais.

Os anexos também podem ser criptografados e visíveis somente para usuários com acesso, ou ficar visíveis para todos os usuários que não estejam impedidos de visualizar os dados. Consulte Tutorial de criptografia de anexo para criptografar um anexo.

Procedimento

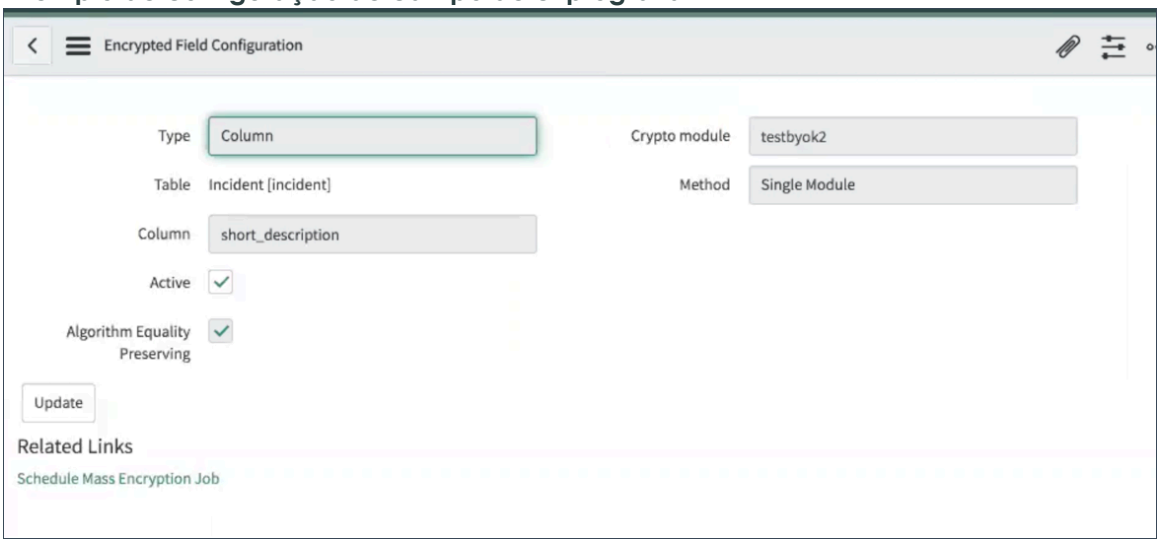
1. Certifique-se de que o Criptografia em nível de coluna para empresas esteja habilitado.
2. Crie um módulo criptográfico para column_level_encryption.
   Consulte Criação de um módulo criptográfico do Criptografia em nível de coluna. Criação de um módulo criptográfico para obter mais informações.
3. Navegue até **Segurança do sistema** > **Configurações de campo criptografado**.
4. Clique em **Novo**.
5. No formulário, preencha os campos.

Formulário de Configuração de campo criptografado

Campo	Descrição
Tipo	A **coluna** é necessária para usar sua chave pessoal.
Tabela	Tabela que armazena as informações confidenciais. Para este exemplo, selecione **Incidente [incidente]**.
Coluna	Coluna ou informações específicas que representam os dados confidenciais a serem criptografados. Para este exemplo, selecione **short_description**.
Ativo	Opção de marcar como **Ativo** para usar a configuração do campo.
Preservação de igualdade de algoritmo	A opção é selecionada automaticamente.
Módulo de criptografia	Módulo criado para usar com a chave pessoal.
Método	A opção **Módulo único** é usada para aplicar as políticas para um módulo. **Vários módulos** é usado para aplicar as políticas em vários módulos.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exemplo de configuração de campo de criptografia



6. Clique em **Enviar**.

   Estabeleça uma política de acesso ao módulo para atribuir acesso ao módulo criptográfico. Consulte Criação de uma política de acesso ao módulo para obter informações adicionais.

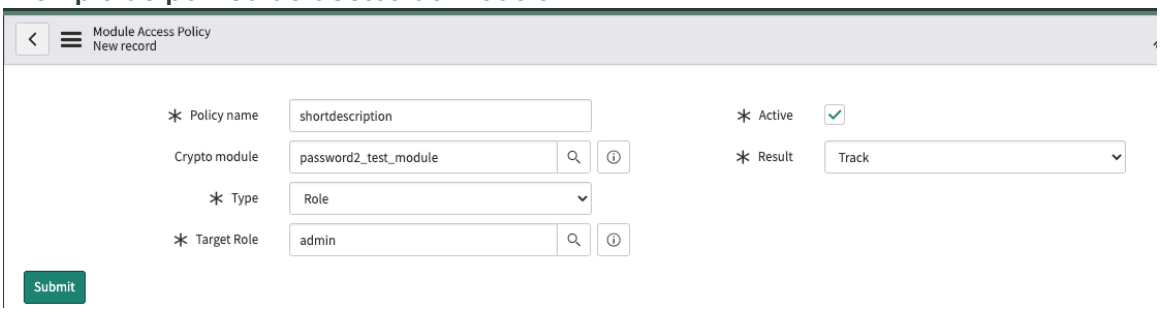
7. Navegue até **Gestão de chave** > **Políticas de acesso ao módulo** > > **Criar nova** > .
8. No formulário, preencha os campos.

Formulário de política de acesso ao módulo

Campo	Descrição
Nome da política	Nome da política, como `descrição resumida`.
Módulo de criptografia	Módulo de criptografia criado para criptografar sua chave.
Tipo	Tipo de designação de acesso à política de criptografia. Use **Função** para conceder acesso ao campo criptografado somente aos usuários que tenham a função atribuída.
Função de destino	A função que tem acesso ao campo criptografado. Para este exemplo, selecione **Administrador**.
Ativo	Opção para ativar a Política de acesso ao módulo.
Resultado	A opção **Rastrear** permite o acesso ao campo para a função selecionada. (Para restringir o acesso a esse campo para a função selecionada, selecione **Rejeitar** ou**Rejeitar estritamente**.)

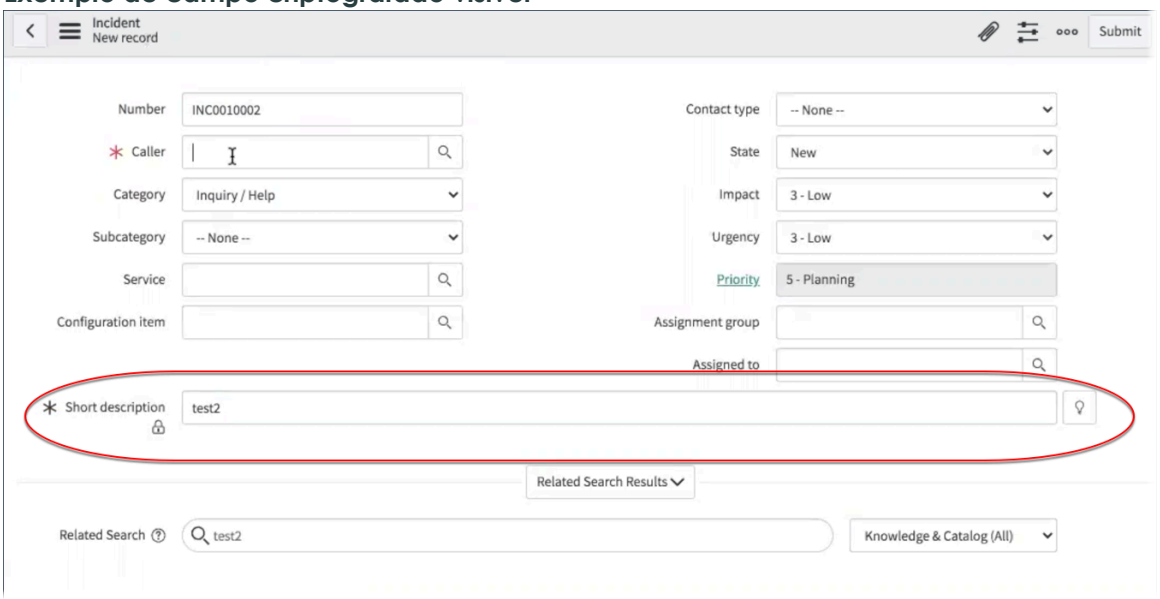
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exemplo de política de acesso ao módulo



9. Clique em **Enviar**.
10. Como um usuário com a função sn_kmf.admin, navegue até **Incidente** > **Novo**.

Exemplo de campo criptografado visível



Agora é possível exibir o campo Descrição resumida com base na configuração da política de acesso ao módulo.

Nota: A função sn_kmf.admin recebeu acesso de usuário ao campo criptografado e Descrição resumida, definindo a política de acesso ao módulo como **Rastrear**.

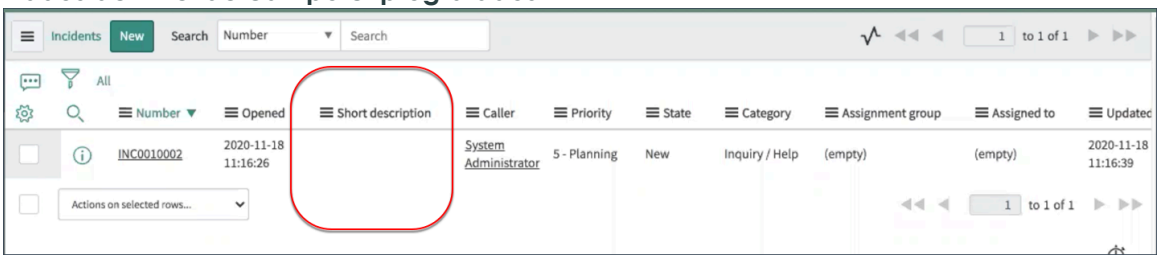
Observe o ícone de cadeado ( ) abaixo do nome do campo indicando que o campo é um campo criptografado.

Agora você pode acessar o módulo **Incidentes** como um usuário final para testar a configuração do campo criptografado.

11. Faça o login como um usuário que deve ser impedido de exibir os dados criptografados no campo configurado.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Dados de nível de campo criptografados



Quando você acessa o número do incidente, os dados na Descrição resumida não ficam visíveis.

Resultados

Você usou com sucesso sua chave simétrica para controlar o acesso a um campo específico usando o Criptografia em nível de coluna para empresas.

Tutorial de criptografia de anexo

Este passo a passo mostra como criptografar um campo em sua instância usando o Criptografia em nível de coluna para empresas com o Estrutura de gestão principal (KMF). Ele também mostra como usar sua própria chave.

Antes de Iniciar

Nota: Este procedimento se aplica apenas à funcionalidade Criptografia em nível de coluna para empresas. Consulte Ativação do Criptografia em nível de coluna para empresas para obter mais informações sobre como obter Criptografia em nível de coluna para empresas.

Função necessária: kmf cryptographic manager

Por Que e Quando Desempenhar Esta Tarefa

Este passo a passo começa com uma instância que você já tenha criado e carregado a sua chave criptográfica pessoal. Você pode usar a chave da ServiceNow®, mas este exemplo usa uma chave fornecida pelo cliente.

Carregue anexos confidenciais em sua instância e limite o acesso de determinados usuários. Use a Configuração de campo criptografado para especificar a equipe autorizada que pode acessar dados confidenciais.

Mostramos como criptografar anexos para ficarem visíveis somente para usuários com acesso, ou ficarem visíveis para todos os usuários que não estejam impedidos de visualizar os dados. Neste exemplo, restringimos uma determinada função de acessar um anexo no módulo **Incidentes**.

Nota: Embora seja possa usar vários módulos com criptografia de coluna, a criptografia de anexo deve usar módulos únicos.

Procedimento

1. Certifique-se de que o Criptografia em nível de coluna para empresas esteja habilitado.
2. Crie um módulo criptográfico.
   Consulte Criação de um módulo criptográfico do Criptografia em nível de coluna. para obter mais informações.
3. Navegue até **Segurança do sistema** > **Configurações de campo criptografado**.
4. Clique em **Nova**.

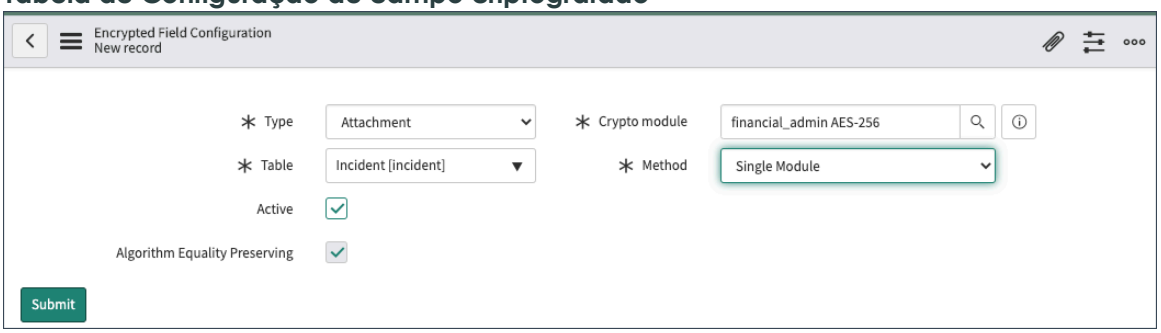
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Preencha o formulário:

Campos da Configuração de campo criptografado

Campo	Descrição
Tipo	Selecione **Anexo** para usar sua chave pessoal para criptografar um anexo da **Tabela** selecionada. Para este exemplo, selecione **Incidente**.
Tabela	Selecione a tabela para acessar as informações confidenciais. Para este exemplo, selecione **Incidente [incidente]**.
Ativo	Marque como **Ativo** para poder usar a configuração do campo.
Preservação de igualdade de algoritmo	Ao selecionar o Criptografia em nível de coluna, este campo ficará visível com base na tabela selecionada.
Módulo de criptografia	Selecione o módulo criado para usar com a chave pessoal.
Método	A opção **Módulo único** é usada para aplicar as políticas para um módulo. **Vários módulos** é usado para aplicar as políticas em vários módulos.

Tabela de Configuração de campo criptografado



6. Clique em **Enviar**.

   Estabeleça uma Política de acesso ao módulo para atribuir acesso ao módulo criptográfico. Consulte Criação de uma política de acesso ao módulo para obter informações adicionais.

7. Navegue até **Gerenciamento de chave** > **Políticas de acesso ao módulo** > **Todas**.
8. Clique em **Nova**.
9. Preencha o formulário:

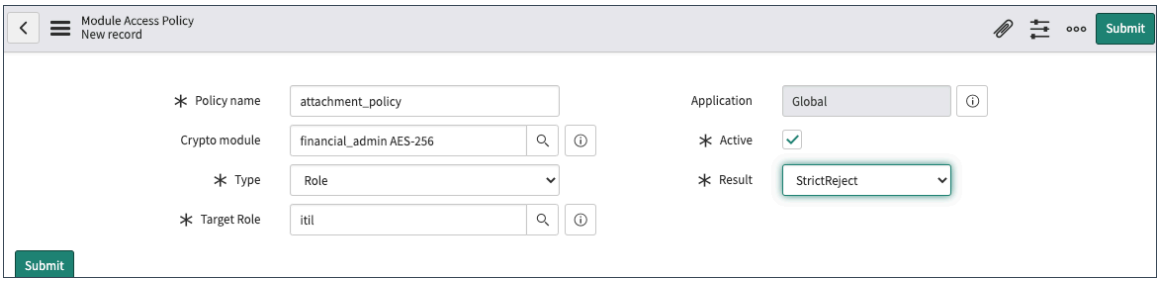
Campos de Política de acesso ao módulo

Campo	Descrição
Nome da política	Insira um nome para a política, como "Política de anexo".
Módulo de criptografia	Selecione o módulo de criptografia criado para criptografar sua chave.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

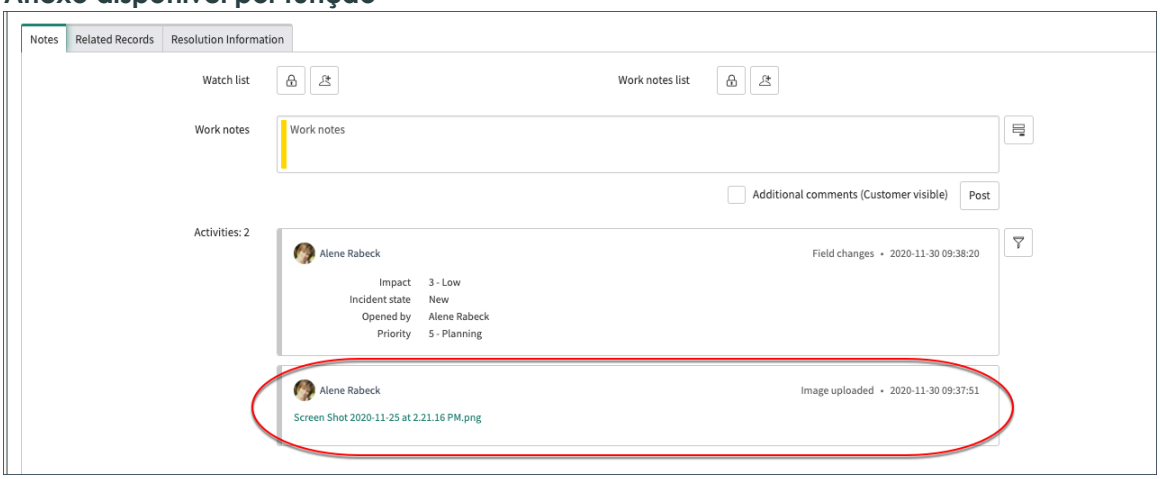
Campo	Descrição
Tipo	Selecione **Função** para restringir o acesso ao campo criptografado de usuários com a função atribuída.
Função de destino	Selecione a função que tem acesso ao campo criptografado. Para este exemplo, selecione **itil**.
Ativo	Marque esta caixa de seleção para poder usar a Política de acesso ao módulo.
Resultado	Selecione **Rejeitar estritamente** para controlar o acesso ao anexo da função selecionada. (Para conceder acesso à função selecionada, selecione **Rastrear**.)

Formulário de Política de acesso ao módulo



10. Clique em **Enviar**.
11. Como administrador ou como uma pessoa que criou o incidente, navegue até **Incidentes** e adicione um anexo às **Atividades** na lista relacionada de **Anotações**.

Anexo disponível por função



12. Faça login como um usuário com acesso restringido ao anexo criptografado.
13. Abra o incidente e role até a seção **Atividades:**.
    O link para abrir o anexo não poderá ser acessado por usuários com a função restrita.
14. A chave fornecida pelo cliente foi usada com sucesso para controlar o acesso a um anexo específico usando criptografia em nível de coluna.

Criptografia em nível de coluna para empresas

A CLE (Criptografia em nível de coluna para empresas, criptografia em nível de coluna para empresas) utiliza a KMF (Estrutura de gestão principal, Estrutura de gestão de chaves)

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

para permitir que você personalize e gerencie a forma de criptografia e descriptografia de campos e anexos em sua instância. É necessária uma assinatura para utilizar o Criptografia em nível de coluna para empresas.

Importante: Este tópico cobre a versão Enterprise da criptografia em nível de coluna. Para obter informações sobre a versão padrão do CLE ou para aprender as diferenças entre as duas versões, consulte Exploração da criptografia em nível de coluna.

A Criptografia em nível de coluna para empresas se baseia na CLE (Column Level Encryption, Criptografia em nível de coluna) e usa a Estrutura de gestão principal e seu suporte total a funções de gestão de chaves. A Criptografia em nível de coluna para empresas oferece proteção de chaves e gestão do ciclo de vida das chaves, proporcionando criptografia de campo em nível de aplicação. Todas as chaves são protegidas com uma hierarquia de encapsulamento de chave enraizada em módulos de segurança de hardware (HSM) FIPS 140-2-L3.

O Criptografia em nível de coluna para empresas oferece a capacidade de gerenciar como os campos compatíveis são criptografados e descriptografados de acordo com as práticas do NIST 800-57. Ele também usa a versão mais atualizada da criptografia em nível de campo, incluindo a integração para proteção e gerenciamento de chave apropriados.

Especificamente, o Criptografia em nível de coluna para empresas utiliza os módulos de criptografia doKMF, concedendo a você mais controle da criptografia do lado do servidor. OKMF garante a proteção da chave de criptografia de dados usando a hierarquia de chaves e a criptografia de envelope. Sua instância criptografa os dados por meio de módulos criptográficos que você configura. É possível criar uma política de acesso para cada módulo e, em seguida, configurar as especificações criptográficas e as políticas de acesso e controlar a gestão do ciclo de vida das chaves.

O Criptografia em nível de coluna para empresas oferece suporte a políticas de acesso ao módulo com base em:

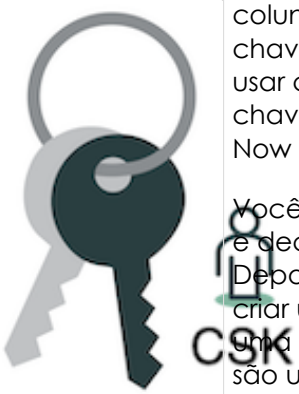
- Escopo
- Função
- Script
- Troca de recursos
- Usuário do Sistema

Consulte Criação de uma política de acesso ao módulo para obter informações adicionais.

Nota: Para obter detalhes sobre os recursos compatíveis com a Criptografia em nível de coluna e como fazer upgrade e assinar o direito ao Criptografia em nível de coluna para empresas, consulte Pacote de assinatura do Gerenciamento de criptografia e chaves.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Termos de criptografia

Termo	Descrição
Gerenciamento de chave	Suporte para gerenciamento de chave O KMF (Key Management Framework) é fundamental para o Criptografia em nível de coluna para empresas Obtenha os seguintes recursos: • Gestão do ciclo de vida das chaves. • Rotação de chave. Consulte Girar chaves para obter detalhes. • Proteção de chave e geração de chave com módulos de segurança de hardware (HSMs) FIPS 140-2-L3. • Separação de funções e deveres. • A transferência segura de chaves de criptografia de dados entre instâncias, como instâncias de produção e não produção. • Chaves fornecidas pelo cliente (CSK) com quebra de chave. • Criptografia não determinística. • Criptografia/descriptografia em massa • Auditoria de acesso/uso de chave. Consulte Noções básicas sobre a estrutura de gerenciamento de chaves para obter detalhes.
Chave fornecida pelo cliente 	Suporte para chaves fornecidas pelo cliente Um dos maiores benefícios do Criptografia em nível de coluna para empresas é que você pode usar suas próprias chaves de criptografia. Os administradores têm a opção de usar chaves fornecidas pela ServiceNow ou suas próprias chaves fornecidas pelo cliente (CSK) para criptografia no Now Platform®. Você também pode gerenciar o ciclo de vida da chave e decidir quando revogar, girar e desativar as chaves. Depois de habilitar as chaves fornecidas pelo cliente e criar um módulo criptográfico, é preciso baixar um token e uma chave efêmera pública. O token e a chave pública são usados para encapsular sua chave e carregá-la na instância. Para usar chaves fornecidas pelo cliente, consulte Definição das configurações de Edge Encryption para selecionar o tipo de chave e Usar chaves fornecidas pelo cliente com a Criptografia em nível de coluna para empresas.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Termo	Descrição
Criptografia em nível de coluna	Suporte para Edge Encryption e criptografia de anexo A Edge Encryption e a criptografia de anexo utilizam módulos criptográficos e políticas de acesso por meio de configurações de campo criptografado. O formulário de Configuração de campo criptografado é usado para a escolha de um tipo de criptografia de coluna ou de anexo. Consulte Definição das configurações de campo criptografado para obter mais informações e os tipos de campo compatíveis.
Criptografia não determinística	Suporte para criptografia não determinística. O Criptografia em nível de coluna para empresas é compatível com a criptografia não determinística para maior segurança. Se o sistema criptografar os mesmos dados mais de uma vez, os textos cifrados serão diferentes a cada vez. A criptografia não determinística está disponível com a criptografia AES com Cipher Block Chaining (CBC). Você pode habilitar este recurso por meio da opção Preservação de igualdade na fase de Definição de algoritmo da especificação criptográfica. Crie uma especificação criptográfica para um módulo criptográfico e defina um algoritmo de criptografia e gere uma chave. Consulte Criação de um módulo criptográfico para definir os mecanismos usados para operações criptográficas e para obter mais informações sobre como habilitar a criptografia não determinística.
Resource Exchange	Resource Exchange Criptografia em nível de coluna para empresas chave de instância para instância de maneira segura usando as APIs criptográficas KMF para fornecer confidencialidade, integridade, autenticação e não recusa. Resource Exchange é um recurso KMF que oferece a capacidade de trocar recursos entre instâncias de maneira segura. Consulte Troca de recursos do Key Management Framework para obter detalhes.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Se você optar por não ativar a Criptografia em nível de coluna para empresas, ainda poderá usar a criptografia em nível de coluna. Consulte Exploração da criptografia em nível de coluna para obter informações.

O Criptografia em nível de coluna para empresas oferece suporte a clientes no local. Ele não é compatível com a Separação de domínios.

Suporte para módulos adicionais e políticas de acesso ao módulo

A versão padrão do Criptografia em nível de coluna é limitada a 5 módulos e políticas de acesso ao módulo (MAP). O Criptografia em nível de coluna para empresas oferece suporte a um número maior de módulos e MAPs.

Informações sobre campo compatíveis

Os seguintes tipos de campo podem ser criptografados:

- Anexos
- Data
- Data/Hora
- E-mail
- HTML
- Diário
- Entrada de Diário
- Lista de Diários
- Telefone
- Texto de cadeia de caracteres
- Campo Traduzido
- HTML Traduzido
- Texto Traduzido
- URL

Criptografia de anexo

Criptografia de anexo por padrão

Para clientes que usam a Criptografia em nível de coluna, por padrão os anexos são criptografados em tabelas que têm um tipo de EFC (Encrypted Field Configuration, Configuração de campo criptografado) ativo de *`Attachment`*.

Essa criptografia padrão definida pela configuração EFC significa que os administradores não precisam declarar manualmente que um anexo deve ser criptografado no carregamento dessas tabelas.

Os administradores podem proibir os usuários de anexar arquivos não criptografados

Para obter detalhes, consulte Impedir que usuários anexem arquivos não criptografados.

Recusar criptografia padrão

Se você não quiser que os anexos sejam criptografados por padrão com base na configuração EFC, é possível recusar essa opção entrando em contato com o suporte da ServiceNow.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para recusar este recurso, crie um caso junto ao suporte da ServiceNow e inclua esta declaração no comentário do registro do caso:

"Eu [nome do cliente] entendo que estou solicitando que a ServiceNow desative uma prática recomendada de segurança para anexos, e que a [empresa do cliente] assume qualquer risco adicional relacionado à configuração e ao uso de anexos não criptografados na aplicação ServiceNow."

Suporte de API

O Criptografia em nível de coluna para empresas atualiza as APIs `setDisplayValue()` e `setValue()` para que possam inserir dados criptografados de campos criptografados. Ele também permite que `getDisplayValue()` e `getValue()` retornem valores de texto não criptografado.

O script a seguir ilustra essas mudanças de API quando a descrição resumida do incidente é criptografada:

```
var gr = new GlideRecord('incident'); //creates a new incident
gr.setValue('short_description','test123'); //sets the value to test123
var sys_ID = gr.insert(); //inserts the record in the Incident table.
gs.info(gr.getValue('short_description')); //displays the unencrypted
 value
```

Ao usar `getValue()` para obter texto criptografado, o script não retorna mais o texto cifrado. O script exibe o texto sem formatação, supondo que o usuário tenha acesso ao módulo criptográfico. Para usuários que não têm acesso ao módulo criptográfico, `getValue()` exibe o texto cifrado.

Criptografia da nuvem com gerenciamento de chave

O ServiceNow® Criptografia da nuvem oferece armazenamento criptografado para o banco de dados usando criptografia de bloco, junto com gerenciamento de chave aprimorado. O Criptografia da nuvem está disponível com o pacote de assinatura da Criptografia da plataforma ServiceNow®.

O Criptografia da nuvem oferece:

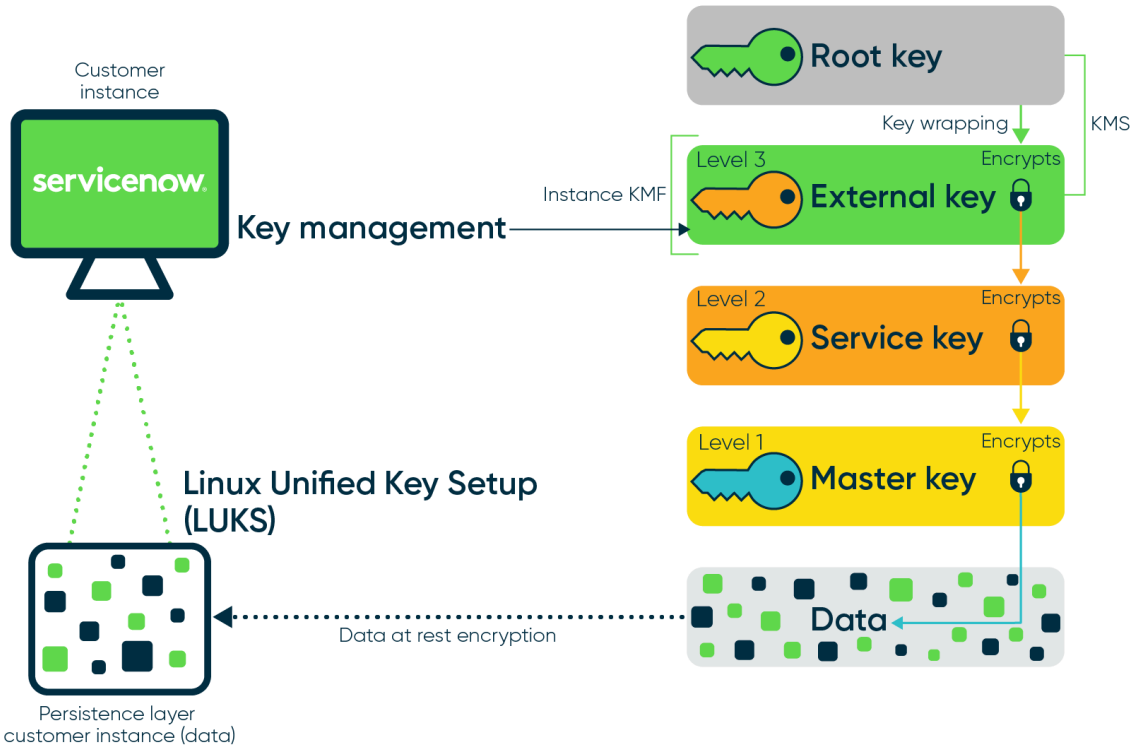
- Separação de trabalhos.
- Rotação de chaves gerenciadas pela ServiceNow.
- Opção de chaves gerenciadas pelo cliente.

> **Nota:** Considere essa opção se sua organização exigir o uso de material de chaves gerado por suas próprias bibliotecas ou ferramentas criptográficas, um sistema corporativo de gestão de chaves ou um HSM (Hardware Security Module, módulo de segurança de hardware). Consulte Operações de gerenciamento de chaves para obter detalhes.

O diagrama a seguir mostra como o Criptografia da nuvem funciona:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Visão geral da Criptografia da nuvem



O módulo de gerenciamento de chaves do Criptografia da nuvem consiste nos seguintes submódulos:

- Operações de gerenciamento de chaves:
  - Acesse a lista de chaves.
  - Execute operações de rotação de chave.
  - Retire chaves gerenciadas pelo cliente.
- Transações de gestão de chaves:

  Faça referência a todas as transações que ocorreram nas chaves que foram usadas.

  Use sua própria chave gerenciada pelo cliente para criptografia.

Em determinadas circunstâncias, ao usar chaves gerenciadas pelo cliente, é possível optar por uma solicitação de retirada de chave. Para fazer isso, você deve licenciar a SKU do complemento opcional Retirada e Reabastecimento da Criptografia da nuvem e solicitar que um membro da equipe Suporte e atendimento ao cliente ative a funcionalidade de retirada.

A opção "Configurações de política de controle de quórum" ficará disponível após a ativação do recurso de retirada. Caso contrário, o módulo não ficará visível no menu. Somente é possível ativar esse recurso ao usar chaves gerenciadas pelo cliente. Essa política permite a definição de configurações em relação ao quórum quando há a ativação do recurso de retirada. Para obter mais detalhes sobre o recurso, consulte Política de controle de quórum.

A Criptografia da nuvem é compatível com instâncias de produção e não produção dos bancos de dados MariaDB e RaptorDB. A Criptografia da nuvem é compatível com o ServiceNow Commercial Cloud, o GCC (Government Customer Cloud) pod 101 e a SPP-AU (ServiceNow Protected Platform – Austrália).

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Licenciamento e habilitação de Criptografia da nuvem

Para obter informações sobre o licenciamento de Criptografia da nuvem, consulte Pacote de assinatura do Gerenciamento de criptografia e chaves.

Para clientes licenciados com novas instâncias, o novo provisionamento de instância incluirá Criptografia da nuvem.

Para que os clientes licenciados com instâncias existentes solicitem que uma instância seja movida para a Criptografia da nuvem, siga as instruções em KB1117369. Você deve ter a função de administrador de cliente ou de administrador de parceiro para solicitar o item do Catálogo de serviços para Habilitar a Criptografia da nuvem em sua instância. A habilitação deste recurso exige uma janela de manutenção de uma hora.

IU da Criptografia da nuvem

Quando a Criptografia da nuvem está habilitada, a IU (User Interface, interface do usuário) dela fica visível para o usuário security_admin quando ele tem a função sn_kmf.admin.

Para acessar a IU da Criptografia da nuvem, pesquise por **Gestão da chave de criptografia da nuvem** na barra de navegação. Navegue até a seção **Operações de gestão de chaves** para ver informações sobre chaves de criptografia, como detalhes da chave ativa, e se a Criptografia da nuvem está habilitada para a instância.

Operações de gerenciamento de chaves

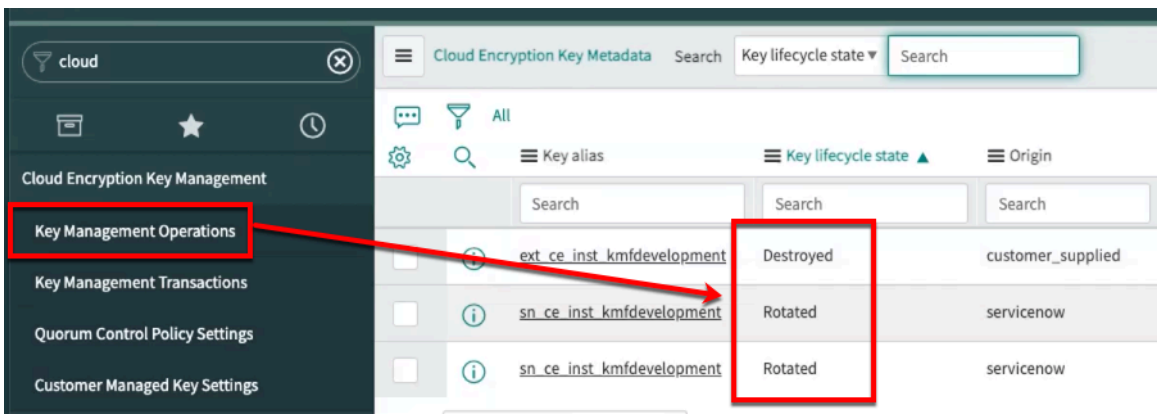
O submódulo de Operações de gerenciamento de chave fornece acesso para exibir e gerenciar todas as chaves de criptografia usadas com o ServiceNow Criptografia da nuvem.

Introdução à Criptografia da nuvem

Estados do ciclo de vida da chave

Em qualquer momento, haverá apenas uma chave ativa no sistema. Ao selecionar uma chave, você acessa a atividade da chave selecionada, como quais chaves foram giradas ou retiradas e o carimbo de data/hora correspondente.

O estado do ciclo de vida da chave é atualizado de acordo com a operação de gerenciamento de chave realizada.



Consulte Girar uma chave gerenciada pela ServiceNow ou Girar uma chave gerenciada pelo cliente para obter detalhes.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: O processo de rotação de chave pode levar até 20 minutos para ser concluído.

Girar uma chave gerenciada pela ServiceNow

Gire a chave gerenciada pela Criptografia da nuvem ServiceNow ativa.

Antes de Iniciar

Funções necessárias: sn_kmf.admin ou sn_kmf.cryptographic_manager

Importante: Se você estiver usando chaves gerenciadas pelo cliente, consulte Girar uma chave gerenciada pelo cliente.

Procedimento

1. Navegue até **Todos** > **Gerenciamento de chaves do Criptografia da nuvem** > **Operações de gerenciamento de chaves**.
   A lista de Metadados da chave da Criptografia da nuvem será carregada. Todas as chaves usadas em sua instância serão listadas. Somente uma chave pode estar ativa em um determinado momento.

   Se estiver acessando o módulo do Criptografia da nuvem pela primeira vez, as entradas de chave ficarão disponíveis após a execução de uma rotação de chave inicial. Uma chave gerenciada pela ServiceNow é o padrão no sistema.
2. Selecione a chave ativa na tabela.
   A tabela Definição de chave será exibida com informações gerais sobre a chave gerada pela ServiceNow.
3. Selecione o botão **Girar chave**.
   Será exibida uma notificação com a opção de continuar a rotação da chave ou de cancelar a operação.
4. Selecione **OK** para girar a chave.
   Uma mensagem de confirmação será exibida na parte superior da página de Definição de chave.
5. Retorne à tela Operações de gerenciamento de chaves para atualizar a tabela Metadados de chave da Criptografia da nuvem.
   Serão listadas as entradas para a chave ativa atual e a chave que está sendo gerada para girar no lugar da chave ativa atual. Consulte Estados do ciclo de vida da chave do Key Management Framework para os diferentes estados disponíveis.

   A chave ativa será listada com uma versão de chave `0` e a chave gerada terá uma versão de `1`.
6. Abra a entrada da chave original para exibir as Transações de gerenciamento de chave. Para obter mais informações, consulte Transações de gestão de chaves.
   A chave anteriormente ativa, versão `0`, será atualizada para o estado do ciclo de vida da chave de `Rotação` e a nova chave, versão `1`, estará `Ativa`.

Preparação da sua chave gerenciada pelo cliente

Siga estas etapas para preparar sua chave gerenciada pelo cliente para carregar em sua instância.

Antes de Iniciar

Funções necessárias: sn_kmf.admin ou sn_kmf.cryptographic_manager

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

Para uma chave gerenciada pelo cliente, você pode usar qualquer biblioteca criptográfica ou HSM para gerar sua chave. Esta chave deve ser uma chave AES de 256 bits e ser encapsulada por um certificado de encapsulamento de Criptografia da nuvem com um esquema de criptografia RSAES_OAEP_SHA_256.

Nota:

Se você optar por usar a ferramenta criptográfica OpenSSL para gerar sua chave, a versão do OpenSSL deverá ser 1.1.1x ou posterior.

Se estiver criando e encapsulando sua chave gerenciada pelo cliente usando o Windows, será necessário gerar a chave encapsulada por meio de aplicações de suporte de shell do Bash, como o Git Bash.

Procedimento

1. Gere um valor aleatório para usar como sua chave simétrica AES-256 usando o OpenSSL.

   Por exemplo, usando o openSSL, é possível gerar essa chave com o comando `openssl rand 32`.

   Para ter compatibilidade, sua chave simétrica deve possuir os seguintes atributos:

Atributo	Valor
Tipo de chave	Chave simétrica baseada em algoritmo Padrão de criptografia avançada (AES).
Tamanho da chave	256 bits (32 bytes)
Requisito de encapsulamento de chave	◦ Algoritmo de criptografia RSA ◦ Preenchimento de criptografia assimétrica ideal (OAEP) ◦ Função de hash SHA-256 (RSAES_OAEP_SHA_256) ◦ Codificação usando o algoritmo Base64

2. Salve a chave em um arquivo.
   Por exemplo, o comando `openssl rand 32 > plaintext_key.bin` do openSSL gera uma chave de 32 bytes e a salva em um arquivo chamado `plaintext_key.bin`.

   Importante: Salve esse arquivo com segurança para referência futura. Essa chave será encapsulada com a chave pública para carregamento.

3. Extraia a chave pública do arquivo de certificado de encapsulamento baixado da sua instância:

```
openssl x509 -pubkey -noout -in wrapping_cert.pem > public_key.pem
```

   Nota: Consulte para obter informações sobre como baixar o certificado de encapsulamento.

4. Encapsule a chave gerada com a chave pública baixada com o certificado de encapsulamento usando o algoritmo RSAES_OAEP_SHA_256:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

```
cat plaintext_key.bin | openssl pkeyutl -encrypt -inkey public_key.pem
 -pubin -pkeyopt rsa_padding_mode:oaep -pkeyopt rsa_oaep_md:sha256 |
 openssl base64 -A -out wrapped_key.txt
```

Um arquivo especificado nesse comando contém uma chave gerenciada pelo cliente que pode ser fornecida à SN para o processo do CMK.

Alternância entre a ServiceNow e as chaves gerenciadas pelo cliente

Alterne entre chave gerenciada pelo cliente ou chaves gerenciadas pela ServiceNow para uso no ServiceNow Criptografia da nuvem.

Por padrão, sua instância está configurada para usar chaves gerenciadas pela ServiceNow e a geração de chave de criptografia do ServiceNow está ativa. No entanto, os administradores podem optar por usar chaves gerenciadas pelo cliente. Também podem optar por retornar para chaves gerenciadas pela ServiceNow.

Girar uma chave gerenciada pelo cliente

Gire a chave gerenciada pelo cliente de sua instância depois de encapsular a chave gerenciada do cliente para Criptografia da nuvem.

Antes de Iniciar

Funções necessárias: sn_kmf.admin ou sn_kmf.cryptographic_manager

Procedimento

1. Navegue até **Todos** > **Gerenciamento de chaves do Criptografia da nuvem** > **Operações de gerenciamento de chaves**.
   A lista de **Metadados da chave do Criptografia da nuvem** será carregada. Todas as chaves que foram usadas em sua instância serão listadas.
2. Na lista de **Metadados de chave do Criptografia da nuvem**, abra o registro da sua chave ativa.
   Se tiver várias chaves, selecione aquela com o estado `Ativo` no **Estado do ciclo de vida da chave**. Só existe uma chave ativa na sua instância.
3. No registro de definição de chave, selecione o botão **Girar chave**.
4. Na janela **Carregar chave gerenciada do cliente**, execute as etapas listadas.

   a. Selecione **Baixar certificado de encapsulamento**.
   O *`zip public_certificate ....`* será baixado para sua máquina local e usado para encapsular sua chave gerenciada pelo cliente.

   > ⚠ **Aviso:** Evite possíveis problemas relacionados a certificados baixando o certificado de encapsulamento sempre que girar ou alternar para uma chave gerenciada pelo cliente.

   b. Selecione **Procurar** para carregar sua chave gerenciada pelo cliente e, em seguida, localize e selecione sua chave de criptografia encapsulada.
   Para escolher um arquivo diferente, selecione-o e clique em **Remover**.

   c. Feche a janela Anexos.

   d. Clique em **OK** para carregar sua chave.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Se a chave estiver no formato correto, será exibida uma mensagem de confirmação. Caso contrário, será exibida uma mensagem de erro. O arquivo de chave será anexado ao registro de definição de chave.

Na tabela Transações de gerenciamento de chave, as etapas de download do certificado e de carregamento da chave são listadas. Consulte Transações de gestão de chaves para obter detalhes sobre as etapas de solicitação.

5. Navegue até **Todos** > **Gerenciamento de chaves do Criptografia da nuvem** > **Operações de gerenciamento de chaves** para visualizar a lista de chaves.
   Na lista de chaves, você poderá ver um novo registro para sua chave gerenciada pelo cliente. Essa nova chave terá um valor de **Origem** de **customer_supplied** e estará no estado **Ativo**. Sua chave anterior estará no estado **Rotacionado**.

Alternar para uma chave gerenciada pelo cliente

Use sua chave gerenciada pelo cliente no ServiceNow Criptografia da nuvem.

Antes de Iniciar

Função necessária: sn_kmf.admin ou sn_kmf.cryptographic_manager

Para alternar para uma chave gerenciada pelo cliente, é necessário que você tenha uma chave gerenciada pelo cliente encapsulada para carregar como parte dessas etapas. Para obter detalhes sobre como preparar essa chave para carregá-la, consulte Preparação da sua chave gerenciada pelo cliente. Depois de carregar sua chave, esse processo inicializará uma rotação de chave para sua nova chave.

Procedimento

1. Navegue até **Todos** > **Gerenciamento de chaves de Criptografia da nuvem** > **Operações de gerenciamento de chaves**.
2. Na lista de **Metadados de chave da Criptografia da nuvem**, abra o registro da sua chave ativa.
   Se tiver várias chaves, selecione aquela com o estado `Ativo` no **Estado do ciclo de vida da chave**. Só existe uma chave ativa na sua instância.
3. Na seção **Links relacionados** do formulário, clique no link **Alternar para chave gerenciada pelo cliente**.
4. Na caixa de diálogo **Alternar para chave gerenciada pelo cliente**, clique no botão **Carregar chave gerenciada**.
5. Na caixa de diálogo **Carregar chave gerenciada** pelo cliente execute os passos listados.

   a. Selecione **Baixar certificado de encapsulamento**.

   > ⚠ **Aviso:** Evite possíveis problemas relacionados a certificados baixando o certificado de encapsulamento sempre que girar ou alternar para uma chave gerenciada pelo cliente.

   b. Selecione **Navegar** e siga as instruções para selecionar e carregar a chave do seu dispositivo.

   c. Selecione **Alternar para chave gerenciada pelo cliente**.

   Uma solicitação para alternar para a chave gerenciada do cliente será gerada pela instância. No formulário atual, será possível ver que o **estado do ciclo** de vida da chave originalmente ativa foi alterado para **Girado**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

6. Navegue até **Todos** > **Gerenciamento de chaves de Criptografia da nuvem** > **Operações de gerenciamento de chaves** para visualizar a lista de chaves.
   Na lista de chaves, você poderá ver um novo registro para sua chave gerenciada pelo cliente. Essa nova chave terá um valor de **Origem** de **customer_supplied** e estará no estado **Ativo**.

Resultados

Sua instância agora usará sua chave gerenciada pelo cliente noServiceNow Criptografia da nuvem.

> **Importante:** Certifique-se de que uma cópia de sua chave de criptografia esteja sempre disponível em um local seguro para operações de gerenciamento de chaves. Sem essa chave, sua instância pode ficar inacessível.

Alternância para uma chave gerenciada da ServiceNow

Alterne uma chave gerenciada pelo cliente de volta para uma chave gerenciada pela ServiceNow Criptografia da nuvem.

Antes de Iniciar

Função necessária: sn_kmf.admin ou sn_kmf.cryptographic_manager

Procedimento

1. Navegue até **Todos** > **Gerenciamento de chaves do Criptografia da nuvem** > **Operações de gerenciamento de chaves**.
2. Na lista de **Metadados de chave da Criptografia da nuvem**, abra o registro da sua chave ativa.
   Se tiver várias chaves, selecione aquela com o estado `Ativo` no **Estado do ciclo de vida da chave**. Só existe uma chave ativa na sua instância.
3. Na seção **Links relacionados** do formulário, clique no link **Alternar para chave gerenciada pela ServiceNow**.
4. Na caixa de diálogo **Alternar para chave gerenciada pela ServiceNow**, clique no botão **Alternar para chave gerenciada pela ServiceNow**.
   Uma solicitação para alternar para a chave gerenciada pela ServiceNow será gerada pela instância. No formulário atual, será possível ver que o **estado do ciclo** de vida da chave originalmente ativa foi alterado para **Girado**.
5. Navegue até **Todos** > **Gerenciamento de chaves da Criptografia da nuvem** > **Operações de gerenciamento de chaves** para visualizar a lista de chaves.
   Na lista de chaves, você poderá ver um novo registro para sua chave gerenciada pela ServiceNow. Essa nova chave terá um valor de **Origem** de **ServiceNow** e estará no estado **Ativo**.

Programar rotação de chaves

Defina uma programação para a rotação automática das chaves gerenciadas por ServiceNow. Este processo desativa automaticamente uma chave de criptografia e substitui a chave antiga por uma chave criptográfica recém-gerada. Se você estiver usando uma chave gerenciada pelo cliente, esta programação pode fornecer um lembrete para girar suas chaves personalizadas manualmente.

Antes de Iniciar

Função necessária: sn_kmf.admin

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegue até **Tudo** > **Gerenciamento de chaves de Criptografia da nuvem** > **Configurações de rotação de chave programada**.
2. Marque a caixa de seleção **Habilitar rotação de chave programada**.
3. Preencha os campos restantes com base em suas necessidades de negócios.

Configurações de rotação de chave programada

Campo	Descrição
Número de meses entre as rotações de chaves (máximo de 60 meses)	Número de meses entre as rotações de chaves. Esse valor é `12` por padrão e pode ter um máximo de `60` meses.
Dia da semana para executar a rotação de chaves	Dia da semana em que a rotação de chaves é feita.
Hora do dia para executar a rotação de chaves	Hora do dia em que a rotação de chaves é feita.
Data e hora da próxima rotação de chaves	Data e hora da próxima rotação programada de chaves. Esse valor não é editável diretamente e é calculado automaticamente com base em suas escolhas.
Número de dias antes da rotação de chaves para enviar o lembrete (máximo de 15 dias)	Número de dias antes da data da rotação de chaves em que sua instância envia notificações.
As notificações por e-mail são enviadas para a seguinte lista de administradores de segurança aprovados	Lista de usuários que recebem notificações para rotação de chaves. O **administrador do sistema** está nesta lista por padrão.

4. Selecione **Enviar**
   Depois de selecionar Enviar, você verá uma notificação na parte superior do formulário. As notificações confirmam a rotação de chaves e a programação de notificação.

⚠ Aviso:

Cada rotação de chave programada tem uma assinatura exclusiva, que garante a integridade do trabalho e detecta qualquer modificação não autorizada. A assinatura de um trabalho agendado é exclusiva em cada instância. Ao clonar um trabalho de rotação de chave programada de uma instância de origem A para uma instância de destino B, o trabalho agendado na instância B falhará na validação de assinatura. Se isso ocorrer, você pode recriar a assinatura desmarcando e marcando novamente a caixa de seleção **Habilitar rotação de chave programada**. Para obter mais detalhes sobre esse problema, consulte KB1247113.

Retirar uma chave gerenciada pelo cliente

Depois que a funcionalidade de retirada de chave gerenciada pelo cliente for ativada, uma operação de retirada se tornará disponível na página Operações de gerenciamento de chaves. As operações de retirada de chave e de aprovação de quórum também podem ser gerenciadas.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Funções necessárias: sn_kmf.admin ou sn_kmf.cryptographic_manager

Esta seção se aplica somente se você tiver licenciado a Retirada e o Reabastecimento da Criptografia da nuvem, um complemento opcional para Criptografia da nuvem.

Procedimento

1. Navegue até **Todos** > **Gerenciamento de chaves de Criptografia da nuvem** > > **Operações de gerenciamento de chaves**.
2. Selecionar a chave gerenciada pelo cliente ativa da tabela.
   A tabela de definição de chaves exibe informações gerais sobre a chave do cliente. Uma função de chave de retirada agora está disponível.
3. Selecione a **Retirar chave** para acionar o processo de retirada.

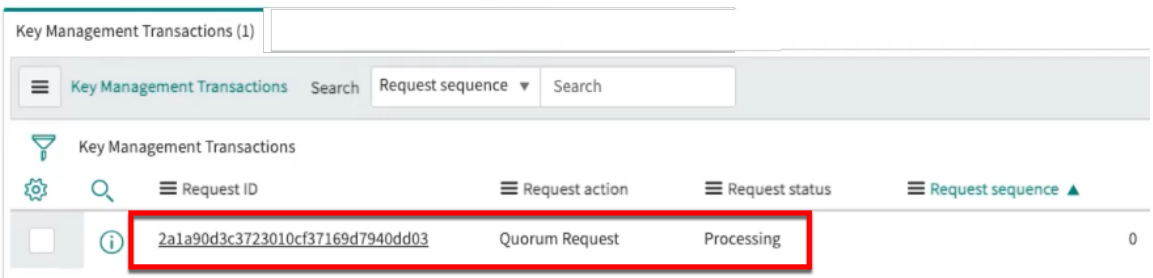
Aviso:

Será exibida uma mensagem de aviso de Retirar chave. A retirada da chave acionará o desligamento da sua instância até que uma operação de restauração seja realizada com a chave retirada.

PERIGO: Você só pode executar uma operação de restauração com a mesma chave que foi retirada. Se você quiser rotacionar para outra chave, faça isso depois de restaurar a chave que foi retirada.

Se a chave gerenciada pelo cliente retirada não for restaurada dentro do intervalo de tempo no qual ServiceNow retém backups (consulte o POP [Procedimento operacional padrão] de backup e restauração para obter mais detalhes), os backups de banco de dados da instância ficarão inacessíveis. Os dados de backup perdidos dessa forma não são recuperáveis.

4. Selecione **OK** para retirar a chave.
   Selecione **Cancelar** se houver alguma dúvida sobre a função de retirada da chave. Você retornará para a tela Definição de chave e será exibida uma mensagem de confirmação.
5. Atualize a página Definição de chave para exibir a solicitação de retirada pendente.



Se a política de controle de quórum tiver sido ativada, o fluxo de trabalho de aprovação deverá ser concluído com sucesso para concluir a retirada da chave. Consulte Gerenciar controle de quórum para obter detalhes.

Reabastecer uma chave gerenciada pelo cliente

Depois que uma operação de retirada de chave for concluída, a chave gerenciada pelo cliente deverá ser reabastecida em sua instância.

Antes de Iniciar
Função necessária: sn_kmf.admin ou sn_kmf.cryptographic_manager

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Esta seção se aplica somente se você tiver licenciado a Retirada e o Reabastecimento da Criptografia da nuvem.

Procedimento

1. Vá para Now Support e navegue até **Catálogo de serviços** > **Catálogo** > **Gerenciamento de instância** > **Restauração de instância - Reabastecimento de chave gerenciada**.
2. Clique em **Solicitar**.
3. Na janela **Restauração de instância - Reabastecer chave gerenciada**, selecione sua instância na lista suspensa **Selecionar instância**.
4. Baixe o certificado de encapsulamento clicando no texto do **certificado de encapsulamento**.

   Aviso: Você deve baixar um novo certificado de encapsulamento sempre que girar ou carregar uma chave gerenciada pelo cliente.

5. Prepare sua chave para upload.
   Para obter detalhes sobre este processo, consulte Preparação da sua chave gerenciada pelo cliente.
6. Na seção **Etapa 4**, clique em **Procurar e carregar** para carregar sua chave encapsulada a partir do dispositivo local.
   Depois que a chave for carregada, você poderá vê-la em **Arquivo abaixo carregado com sucesso**. Se precisar carregar novamente a chave, clique em **Remover arquivo** e carregue a chave novamente conforme descrito nas etapas anteriores.
7. Clique em **Girar chave** para concluir o reabastecimento.

Política de controle de quórum

A Política de controle de quórum especifica o número mínimo de aprovações necessárias entre o número total de aprovadores selecionados para atingir o quórum de retirada de chave gerenciada pelo cliente.

Aviso: Você deve assinar um adendo jurídico para ativar a funcionalidade de retirada de chave. A opção Configurações da política de controle de quórum ficará disponível quando o recurso de retirada for habilitado. Caso contrário, o módulo não estará visível no menu da app. Após a retirada da chave, sua instância não estará mais disponível até que a chave de criptografia seja reabastecida e esteja ativa novamente.

Em determinadas circunstâncias, convém criar uma retirada de chave. Você deve primeiro solicitar a funcionalidade de retirada de chave do Suporte e atendimento ao cliente e preencher um adendo jurídico.

A Política de controle de quórum especifica o número mínimo de aprovações necessárias entre o número total de aprovadores selecionados para atingir o quórum de retirada de chave gerenciada pelo cliente. Por exemplo, há um total de cinco aprovadores, mas somente quatro aprovações são necessárias para atingir o quórum. Quando quatro aprovações são obtidas, a solicitação de retirada é processada e a chave retirada.

Sempre que uma operação de retirada é realizada em um grupo habilitado para aprovação de quórum, um fluxo de trabalho para aprovação de quórum é acionado. Uma notificação por e-mail é enviada a todos os usuários que podem conceder aprovação. As tarefas também são geradas nas contas dos aprovadores, que eles veem no painel ao fazer login em sua conta da ServiceNow.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Os usuários podem conceder aprovações da instância, do e-mail ou da página Operações de gerenciamento de chaves. A operação de retirada de chave é bloqueada até que o quórum seja atendido.

Quando o número mínimo de aprovadores for atingido, o quórum será atingido e a retirada da chave será acionada. A retirada é realizada e registrada, incluindo os nomes dos usuários que aprovaram a solicitação.

Consulte Configurar as definições de política de controle de quórum para obter detalhes da configuração.

Configurar as definições de política de controle de quórum

Siga estas etapas para configurar as definições de política de controle de quórum

Antes de Iniciar

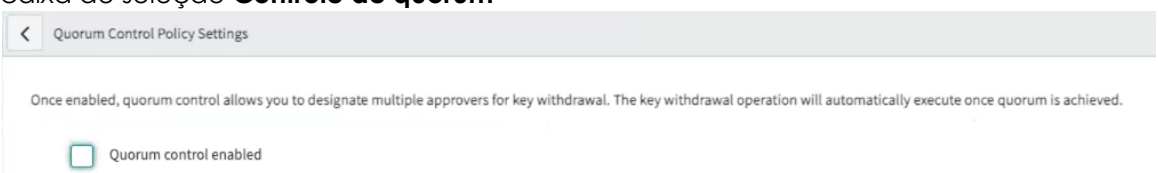
Funções necessárias: sn_kmf.admin

Por Que e Quando Desempenhar Esta Tarefa

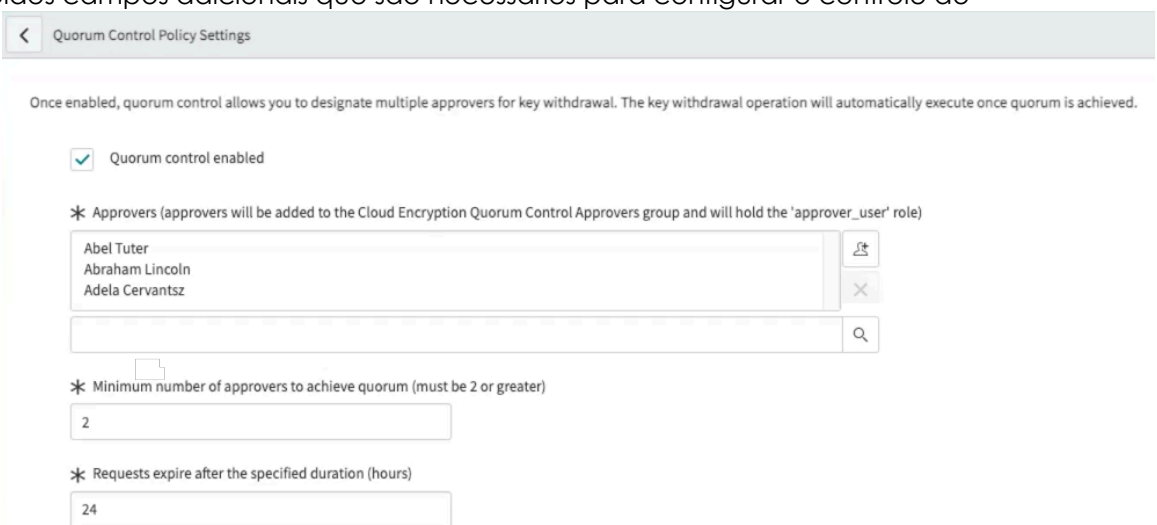
⚠ **Aviso:** Você deve assinar um adendo jurídico para ativar a funcionalidade de retirada de chave. A opção Configurações da política de controle de quórum ficará disponível quando o recurso de retirada for habilitado. Caso contrário, o módulo não estará visível no menu do app. Após a retirada da chave, sua instância não estará mais disponível até que a chave de criptografia esteja ativa novamente.

Procedimento

1. Solicite a funcionalidade de retirada de chave do Suporte e atendimento ao cliente.
2. Navegue até **Gerenciamento de chave da Criptografia da nuvem** > **Definições da política de controle de quórum**.
3. Marque a caixa de seleção **Controle de quórum habilitado**.



São exibidos campos adicionais que são necessários para configurar o controle de quórum.



4. Preencha os campos para completar o formulário.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Aprovadores	Designe os membros do quórum na lista de usuários. Selecione o ícone de cadeado para abrir o diretório do usuário. Não há limite para o número de aprovadores que podem ser selecionados.
Número mínimo de aprovadores para atingir o quórum	Defina o número mínimo de aprovadores exigido para atingir o quórum. Por exemplo, se houver nove aprovadores selecionados, um mínimo de cinco poderá ser configurado para o quórum. Quando cinco aprovações forem recebidas no sistema, o quórum será atingido e a operação de retirada será iniciada. **Nota:** O número mínimo de aprovadores necessários é dois.
As solicitações expiram após a duração especificada (horas)	Defina um valor numérico em horas que seja a alocação de tempo máxima para o número mínimo de aprovações a ser obtido. Depois que o intervalo de tempo expira, as solicitações de quórum também expiram. Uma nova solicitação de quórum é necessária para continuar com uma solicitação de retirada.

5. Clique em **Enviar**.
   Uma mensagem de confirmação será exibida.

O que Fazer Depois
As ações de retirada estão disponíveis em Operações de gerenciamento de chaves.

Gerenciar controle de quórum

Depois que um fluxo de trabalho de operação de retirada for acionado, as ações de quórum poderão ser gerenciadas na página Operações de gerenciamento de chaves. A operação de retirada de chave é bloqueada até que o quórum seja atendido.

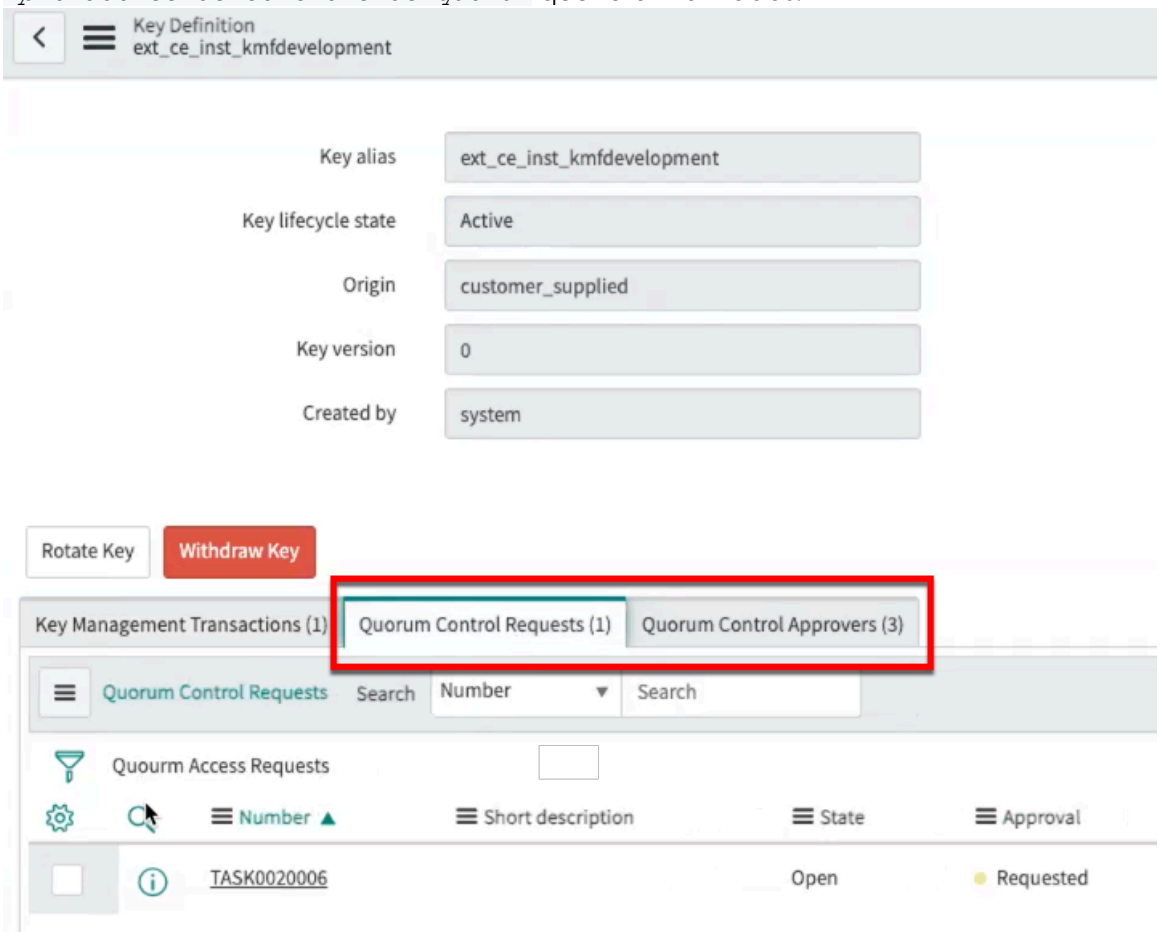
Antes de Iniciar
Função necessária: sn_kmf.admin ou sn_kmf.cryptographic_manager

Quando o quórum for aprovado ou rejeitado, o solicitante da retirada da chave receberá um e-mail informando se o quórum foi atingido ou negado.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

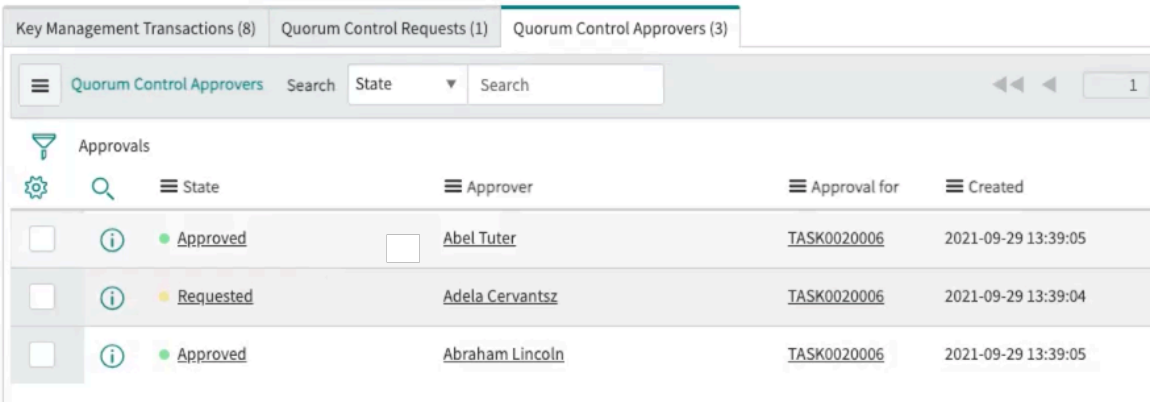
1. Execute as etapas para retirar uma chave gerenciada pelo cliente encontrada em Operações de gerenciamento de chaves.
2. Exiba as guias *Solicitações de controle de quórum* e *Aprovadores de controle de quórum* que foram ativadas.



3. Abra a guia **Solicitações de controle de quórum** para exibir a solicitação real criada.
   - Estado:
     - Aberto: a ação de retirada principal está aguardando o quórum ser atendido.
     - Encerrado concluído: o quórum foi atendido e não há nenhuma ação adicional nesta solicitação de quórum específica.
   - Aprovação:
     - Solicitado: os e-mails de aprovação foram enviados e o fluxo de trabalho foi acionado para atingir o quórum.
     - Aprovado: a chave será retirada e a instância será encerrada.
     - Negado: a solicitação de quórum foi cancelada e nenhuma ação adicional é realizada com esta solicitação. Uma nova solicitação de retirada será necessária para retirar a chave.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Abra a guia Aprovadores de controle de quórum para exibir a lista de aprovadores e o estado da solicitação de aprovação.



   Estado:

   - Solicitado: o aprovador ainda não executou uma ação na solicitação de aprovação.
   - Aprovado: a solicitação foi aprovada no e-mail ou na página de aprovações.

5. Selecione a guia **Transações de gerenciamento de chaves** para exibir o andamento da etapa de solicitação da retirada da chave.
   - Etapa 0 – Solicitação de quórum: a solicitação de quórum real. A solicitação de quórum deve ser concluída para acionar as etapas de retirada de chave.
   - Etapa 1 – Retirada de chave: a etapa de retirada de chave. Ela é composta pelas etapas dois a sete.
   - Etapa 2 – Request_preparation: cria uma solicitação para acionar o encapsulamento e a rotação.
   - Etapa 3 – request_integrity_check: valida se a solicitação é legítima e segura.
   - Etapa 4 – request_validation: valida que há uma solicitação em andamento. Somente uma solicitação de rotação pode ser processada por vez.
   - Etapa 5 – hsm_key_delete: faz a chamada para KeySecure para excluir a chave ativa.
   - Etapa 6 – key_metadata_withdraw: converte o estado do ciclo de vida de metadados da chave ativa em "destruído".
   - Etapa 7 – post_withdraw: faz uma chamada para encerrar a instância.

Aprovar ou negar uma solicitação de controle de quórum

Aprove ou negue uma solicitação de controle de quórum das Transações de gerenciamento de chaves.

Por Que e Quando Desempenhar Esta Tarefa

Quando uma solicitação de quórum é criada, o número mínimo de aprovações é exigido pelos membros. Depois que um fluxo de trabalho de operação de retirada for acionado, as ações de quórum poderão ser gerenciadas utilizando diversos métodos. Os usuários podem conceder aprovações da página Operações de gerenciamento de chaves, Minhas aprovações na instância, ou diretamente do e-mail de solicitação. A operação de retirada de chave é bloqueada até que o quórum seja atendido.

Este procedimento descreve como aprovar ou negar uma solicitação de quórum na página "Operações de gerenciamento de chaves".

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Funções necessárias: sn_kmf.admin ou sn_kmf.cryptographic_manager

Procedimento

1. Navegue até **Todos** > **Gerenciamento de chaves do Criptografia da nuvem** > **Transações de gerenciamento de chaves** > **Aprovadores de controle de quórum**.
2. Selecione seu nome de usuário na tabela.
3. Aprove ou negue a solicitação.

Aprovar ou negar uma solicitação de quórum

Quando uma solicitação de quórum é criada, o número mínimo de aprovações é exigido pelos membros. Depois que um fluxo de trabalho de operação de retirada for acionado, as ações de quórum poderão ser gerenciadas utilizando diversos métodos. Os usuários podem conceder aprovações da página Operações de gerenciamento de chaves, **Minhas aprovações** na instância, ou diretamente do e-mail de solicitação. A operação de retirada de chave é bloqueada até que o quórum seja atendido.

Antes de Iniciar
Funções necessárias: sn_kmf.admin ou sn_kmf.cryptographic_manager

Transações de gestão de chaves

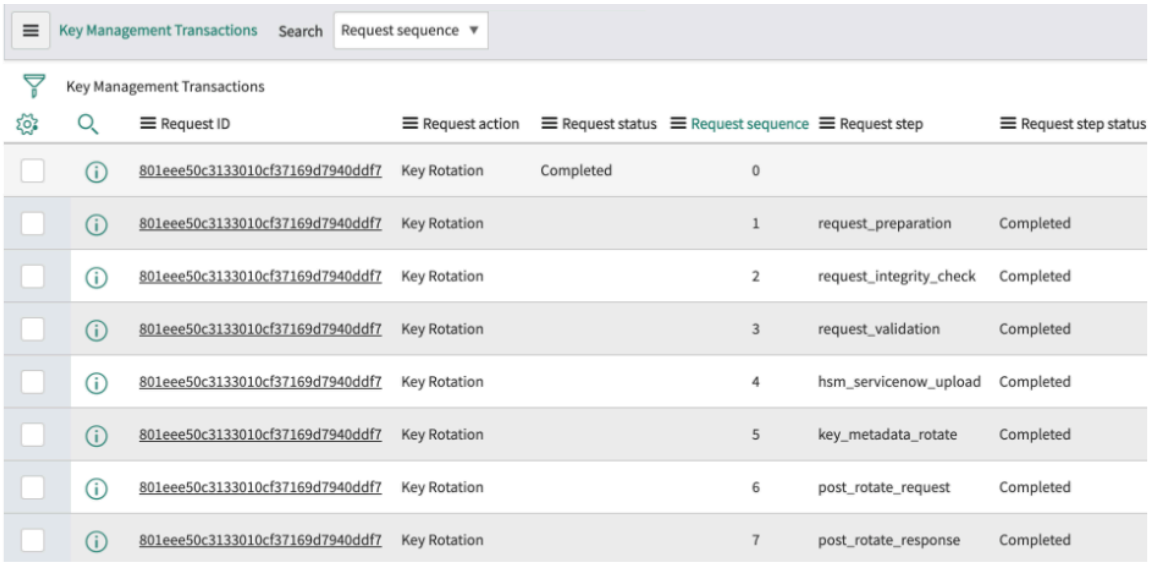
O submódulo de Transações de gerenciamento de chave exibe todas as transações que ocorreram nas chaves em sua instância ServiceNow.

- Uma transação de chave é definida pelo seguinte:
  - composta por várias etapas de solicitação.
  - Um único *ID de solicitação* é compartilhado em todas as etapas da solicitação.
  - A etapa inicial, sequência de solicitação 0, de uma transação fornece o estado atual da transação geral.

    Conforme mostrado na imagem abaixo, o *Status de solicitação* geral da etapa 0 é de Concluído.
- É possível identificar o seguinte para transação por meio da etapa de solicitação individual:
  - A ordem de cada etapa em uma transação pode ser identificada pelo número de sequência da etapa.
  - O status de cada transação é visível por meio do status da etapa da solicitação.
  - Se qualquer etapa além da etapa inicial falhar, a transação geral terá um status de Falha. Se todas as etapas tiverem sido concluídas, o status da transação também será Concluído.

A tela a seguir é um exemplo do tipo de informação exibida com uma rotação de chave do ServiceNow.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



A tabela a seguir exibe as informações de campo disponíveis na página Transações de gerenciamentos de chave.

Transações de gestão de chaves

Campo	Descrição
ID de solicitação	ID exclusivo gerado pelo sistema para a ação que está sendo executada Um ID de solicitação é compartilhado em todas as etapas da solicitação.
Ação de solicitação	Exibe a ação da operação de chave que está sendo executada.
Status da solicitação	• Processamento: uma solicitação foi inserida, mas ainda não foi concluída. • Concluído: a solicitação foi concluída com sucesso. • Falha: ocorreu um problema e o processo não foi concluído. **Nota:** Entre em contato com a Suporte e atendimento ao cliente e forneça o número da solicitação em que a ocorreu a falha.
Alias da chave	Entrada alfanumérica.
Estado de ciclo de vida da chave	Consulte Estados do ciclo de vida da chave do Key Management Framework para obter definições.
Origem	• Chave ServiceNow • Chave gerenciada pelo cliente
Versão da chave	Quando uma chave gira, o número da versão aumenta.
Sequência de solicitação	Exibe a ordem na qual uma solicitação está sendo processada no sistema.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Transações de gestão de chaves

Campo	Descrição
Etapa de solicitação	Exibe qual etapa está sendo processada no sistema durante a rotação da chave. A quantidade e o conteúdo das etapas variam de acordo com o tipo de operação de chave realizada. **1.** request_preparation: cria uma solicitação para acionar o encapsulamento e a rotação. **2.** request_integrity_check: valida se a solicitação é legítima e segura. **3.** request_validation: valida que há uma solicitação em andamento. Somente uma solicitação de rotação pode ser processada por vez. **4.** attachment_process: extrai o material da chave encapsulada do anexo. (Etapa adicional ao girar uma chave gerenciada pelo cliente). **5.** hsm_<key type> _upload: carrega o material da chave encapsulada para o KeySecure do HSM. **6.** key_metadata_rotate: gera os novos metadados de chave. **7.** post_rotate_request: envia uma solicitação para executar a rotação da chave. **8.** post_rotate_response: resposta para executar a rotação de chave com base na solicitação da instância do cliente. **Nota:** Forneça a etapa da solicitação ao Suporte e atendimento ao cliente para analisar a progressão do status caso uma etapa da solicitação não seja concluída.
Status da etapa de solicitação	• Concluído: a rotação foi bem-sucedida. • Falha: a rotação não foi bem-sucedida. **Nota:** Forneça a etapa da solicitação ao Suporte e atendimento ao cliente para analisar a progressão do status caso uma etapa da solicitação não seja concluída.

Registro em log da Criptografia da nuvem

Saiba mais sobre as opções de registro em log do Criptografia da nuvem.

Tabelas de registro em log da Criptografia da nuvem

Use essas tabelas para encontrar informações de registro em log relacionadas às transações da Criptografia da nuvem em sua instância.

Tabela	Descrição
Metadados da Criptografia da nuvem	Os Metadados da Criptografia da nuvem capturam os principais metadados do gerenciamento do ciclo de vida. Nesta tabela, encontre informações importantes sobre o ciclo de vida, o estado e a versão.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Descrição
	Ela é atualizada após cada operação de chave.
Transações de gerenciamento de chaves [dare_key_request]	As Transações de gerenciamento de chave capturam informações de transação de gerenciamento de chave. Nessa tabela, você pode encontrar o registro em log para cada etapa de uma transação. Ela registra todas as informações de erro de uma transação no campo de **mensagem de erro**.
Auditorias do sistema [sys_audit]	A tabela de Auditorias do sistema captura inserções e atualizações em todos os registros auditados em sua instância. Nela, você pode encontrar mudanças nos registros na sua instância, quando essas mudanças foram feitas e qual conta de usuário iniciou a mudança.

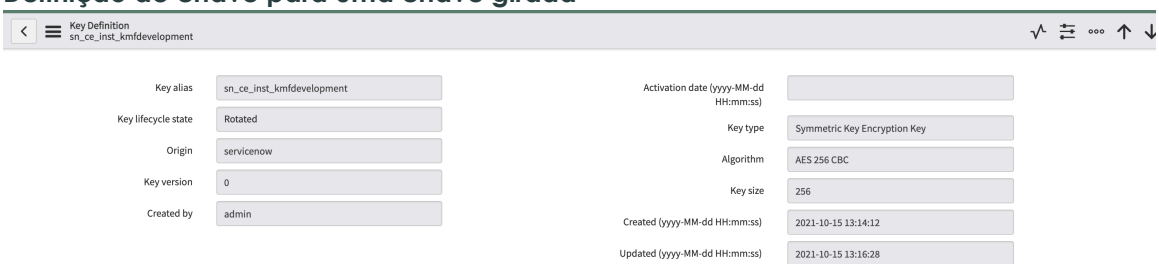
Monitoramento de operações de rotação de chave

Use a tabela Metadados de chave da Criptografia da nuvem [dare_key_metadata] para encontrar informações sobre o ciclo de vida da sua chave. Nela, pode encontrar informações como origem, data de ativação, estado e versão de suas chaves.

Use a tabela Transações de gerenciamento de chaves [dare_key_request] para monitorar transações de operações de chave. Nessa tabela, é possível encontrar todas as solicitações relacionadas às suas chaves, incluindo o estado, o status e a etapa do processo em que a solicitação se encontra. As solicitações concluídas são retidas nesta tabela com o status **Concluído**.

Este exemplo mostra uma operação de rotação de chave. Durante esta operação, o estado do ciclo de vida da chave antiga é atualizado de ativo para girado, e o estado da versão, de ativo para descontinuado.

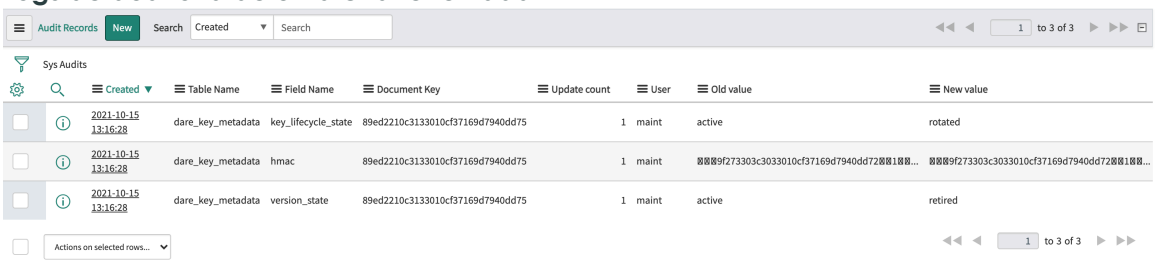
Definição de chave para uma chave girada



Observando a tabela Auditorias do sistema [sys_audit], os administradores podem ver as mudanças feitas nos registros na tabela Metadados da Criptografia da nuvem [dare_key_metadata]. Os administradores podem ver quais registros foram atualizados e quando. As entradas de log também registram o campo que foi alterado e os valores antigos e novos.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Logs de auditoria de uma chave retirada



Audit Records | New | Search | Created | Search | 1 to 3 of 3

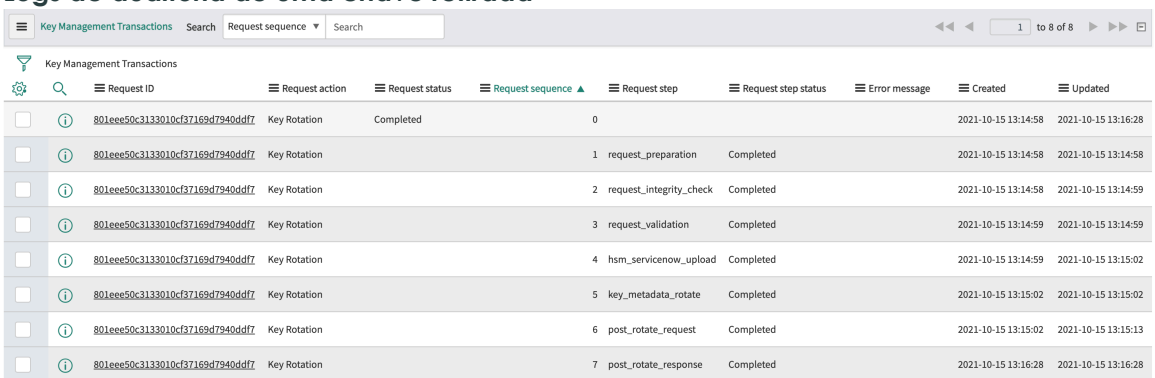
Sys Audits

Created	Table Name	Field Name	Document Key	Update count	User	Old value	New value
2021-10-15 13:16:28	dare_key_metadata	key_lifecycle_state	89ed2210c3133010cf37169d7940dd75	1	maint	active	rotated
2021-10-15 13:16:28	dare_key_metadata	hmac	89ed2210c3133010cf37169d7940dd75	1	maint	[redacted]	[redacted]
2021-10-15 13:16:28	dare_key_metadata	version_state	89ed2210c3133010cf37169d7940dd75	1	maint	active	retired

Actions on selected rows... | 1 to 3 of 3

Os administradores podem exibir os registros na tabela de Metadados da Criptografia da nuvem [dare_key_metadata]. Nos registros de auditoria abaixo, o status da solicitação foi alterado de processamento para concluído.

Logs de auditoria de uma chave retirada



Key Management Transactions | Search | Request sequence | Search | 1 to 8 of 8

Key Management Transactions

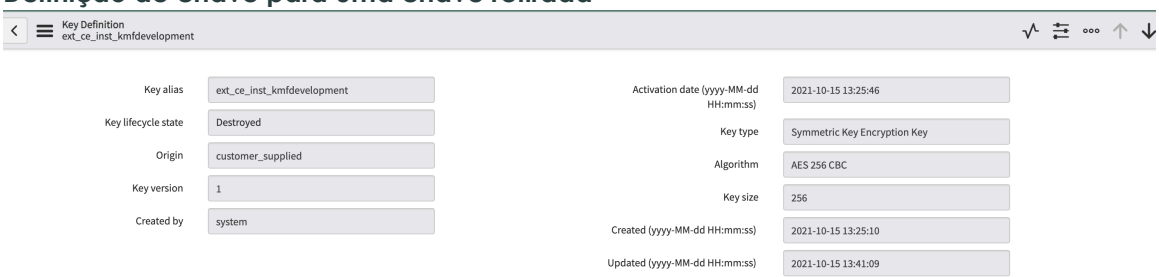
Request ID	Request action	Request status	Request sequence ▲	Request step	Request step status	Error message	Created	Updated
801eee50c3133010cf37169d7940ddf7	Key Rotation	Completed	0				2021-10-15 13:14:58	2021-10-15 13:16:28
801eee50c3133010cf37169d7940ddf7	Key Rotation		1	request_preparation	Completed		2021-10-15 13:14:58	2021-10-15 13:14:58
801eee50c3133010cf37169d7940ddf7	Key Rotation		2	request_integrity_check	Completed		2021-10-15 13:14:58	2021-10-15 13:14:59
801eee50c3133010cf37169d7940ddf7	Key Rotation		3	request_validation	Completed		2021-10-15 13:14:59	2021-10-15 13:14:59
801eee50c3133010cf37169d7940ddf7	Key Rotation		4	hsm_servicenow_upload	Completed		2021-10-15 13:14:59	2021-10-15 13:15:02
801eee50c3133010cf37169d7940ddf7	Key Rotation		5	key_metadata_rotate	Completed		2021-10-15 13:15:02	2021-10-15 13:15:02
801eee50c3133010cf37169d7940ddf7	Key Rotation		6	post_rotate_request	Completed		2021-10-15 13:15:02	2021-10-15 13:15:13
801eee50c3133010cf37169d7940ddf7	Key Rotation		7	post_rotate_response	Completed		2021-10-15 13:16:28	2021-10-15 13:16:28

Registro em log para operações de retirada de chave

As informações de registro em log sobre a retirada de chave são armazenadas na tabela Auditorias [sys_audit]. Essas informações de registro em log contêm informações sobre quem iniciou a retirada da chave e quando a retirada ocorreu.

Este exemplo mostra uma operação de retirada de chave. Durante essa operação, o estado do ciclo de vida da chave é atualizado de gerado para ativo e para destruído. A versão da chave é atualizada de desconhecida para ativa e para descontinuada.

Definição de chave para uma chave retirada



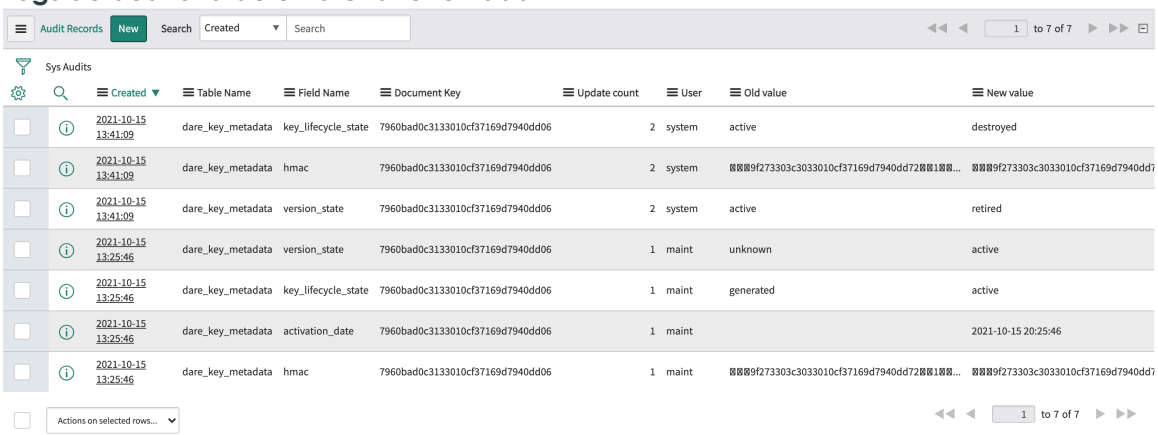
Key Definition
ext_ce_inst_kmfdevelopment

Key alias	ext_ce_inst_kmfdevelopment	Activation date (yyyy-MM-dd HH:mm:ss)	2021-10-15 13:25:46
Key lifecycle state	Destroyed	Key type	Symmetric Key Encryption Key
Origin	customer_supplied	Algorithm	AES 256 CBC
Key version	1	Key size	256
Created by	system	Created (yyyy-MM-dd HH:mm:ss)	2021-10-15 13:25:10
		Updated (yyyy-MM-dd HH:mm:ss)	2021-10-15 13:41:09

Observando a tabela Auditorias do sistema [sys_audit], os administradores podem ver as mudanças na tabela Metadados da Criptografia da nuvem [dare_key_metadata].

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Logs de auditoria de uma chave retirada



Detecção de adulteração

Use a detecção de adulteração para melhorar a segurança, detectando mudanças não autorizadas nas configurações de controle de quórum.

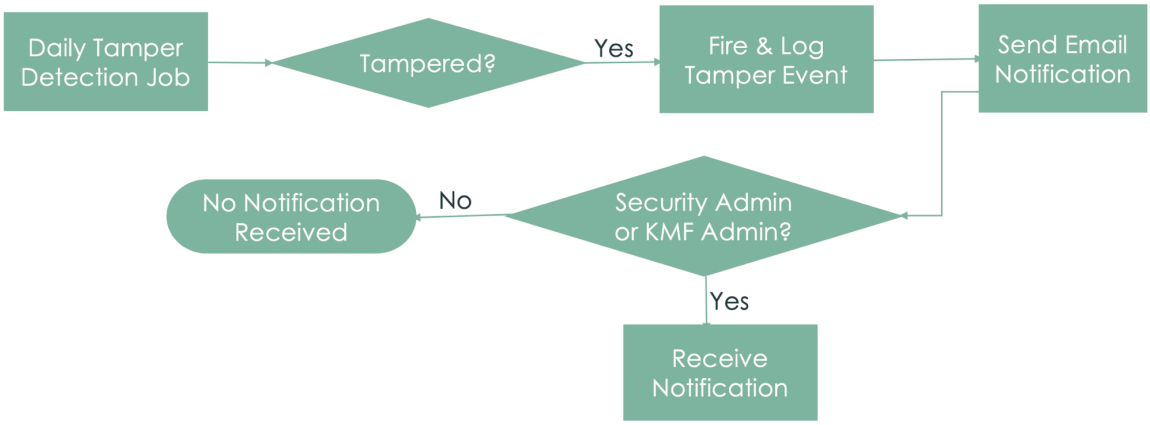
Processo de detecção de adulteração

Quando habilitada, a detecção de adulteração valida suas configurações de controle de quórum verificando se há modificações não autorizadas (adulteração). A detecção de adulteração usa o HMAC (hash-based message authentication code, código de autenticação de mensagem baseado em hash).

1. Quando uma configuração é alterada ou criada, sua instância cria um HMAC. O HMAC é baseado no valor do registro de configuração (dare_property).
2. Sempre que sua instância usa essas configurações, a detecção de adulteração as valida usando o HMAC.
3. Se a configuração for validada com sucesso, ela poderá ser usada pela plataforma, caso contrário, não poderá.

A detecção de adulteração é executada diariamente em sua instância

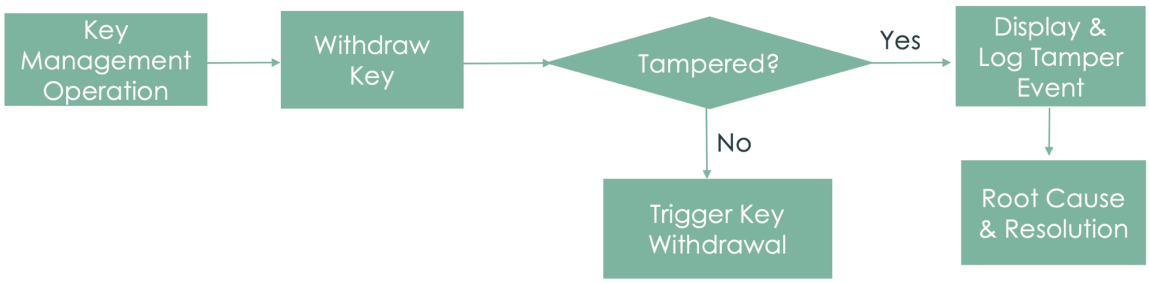
A detecção de adulteração verifica suas configurações para adulteração usando um trabalho agendado diariamente e relata falhas de validação em seu nó e logs de segurança. A detecção de adulteração envia uma notificação para os administradores de segurança e KMF sobre falhas de validação.



A detecção de adulteração é executada antes de executar uma retirada de chave

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A detecção de adulteração também valida suas propriedades quando você solicita uma retirada de chave. Se suas configurações não forem aprovadas na validação, a retirada da chave não será executada. Nesse caso, você deve resolver todos os problemas de validação antes que a retirada da chave possa concorrer.



Identificar adulteração

A detecção de adulteração atualiza seus logs quando a validação falha.

Se a detecção de adulteração não validar qualquer uma das configurações de controle de quórum, essas falhas serão exibidas em seus logs de nó e de segurança. A entrada de log inclui o sys_id do registro de configurações (dare_property) que falhou na validação.

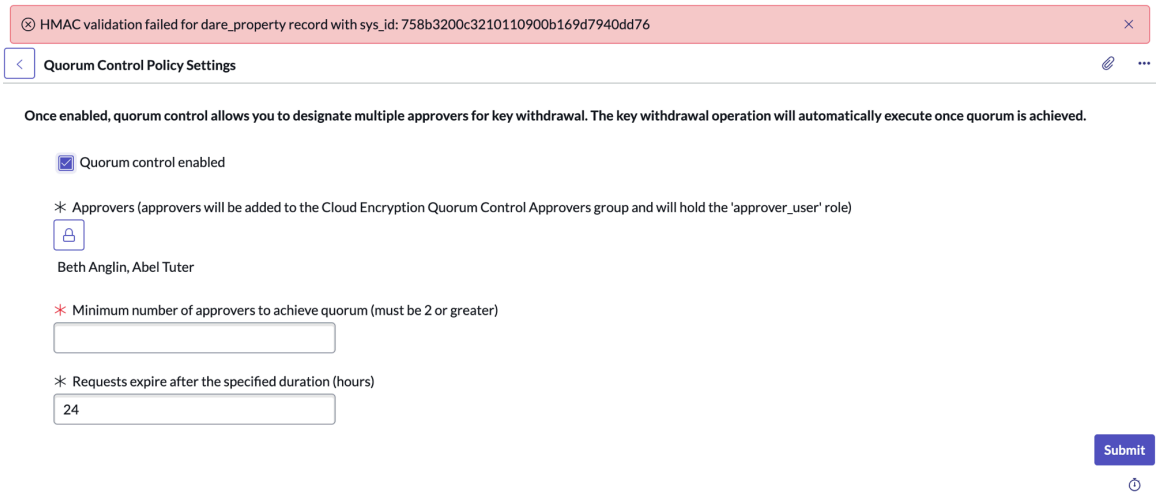
```
2022-06-28 13:45:46 (582) Default-thread-5
 B6FAC1F6C3D01110CF37169D7940DD6E txid=231c4d72c310 SEVERE
 HMAC_VALIDATION_FAILED:The dare_property record with sys_id:
 776e3200c3210110900b169d7940dd76 failed HMAC validation

2022-06-28 13:47:35 (264) Default-thread-8
 B6FAC1F6C3D01110CF37169D7940DD6E txid=8e8cc972c310 SEVERE
 HMAC_VALIDATION_FAILED:The dare_property record with sys_id:
 758b3200c3210110900b169d7940dd76 failed HMAC validation
```

O registro em log exibe informações semelhantes a esses exemplos quando a validação falha. Validações bem-sucedidas não aparecem nos logs.

A detecção de adulteração exibe uma mensagem de aviso na página de configurações de controle de quórum

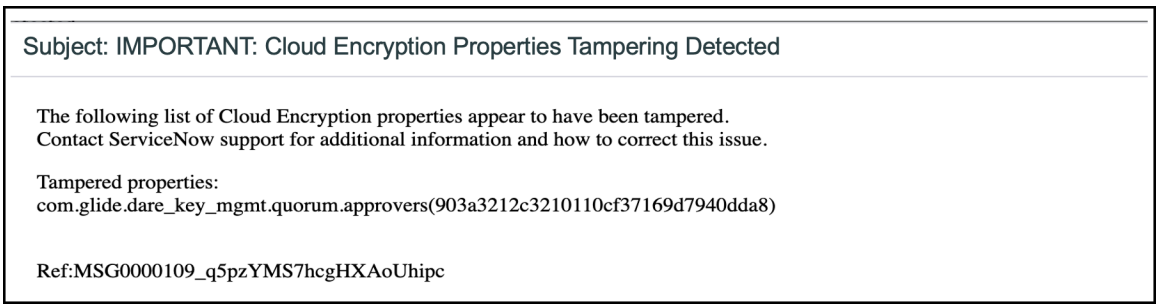
Se uma configuração de controle de quórum falhar na validação, você pode ver um aviso ao exibir a página de configurações da Política de controle de quórum em sua instância. O aviso inclui o sys_id do registro de configurações (dare_property) que falhou na validação.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



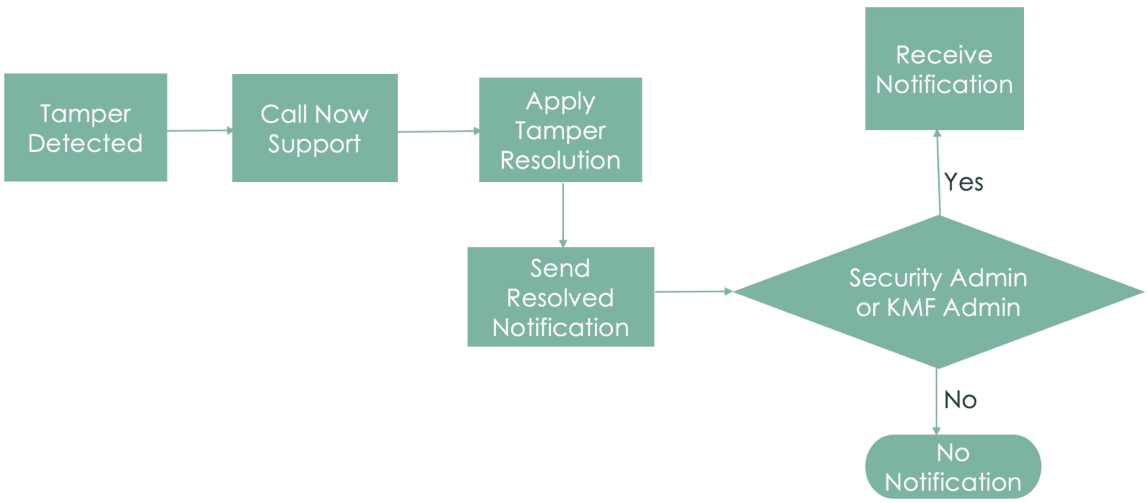
A detecção de adulteração envia notificações para usuários com as funções *Security Admin* e *KMF Admin*

Se a detecção de adulteração não validar qualquer uma das configurações de controle de quórum, os administradores de segurança e os administradores de KMF receberão uma notificação semelhante a este exemplo.



Resolver problemas de adulteração com o suporte da ServiceNow

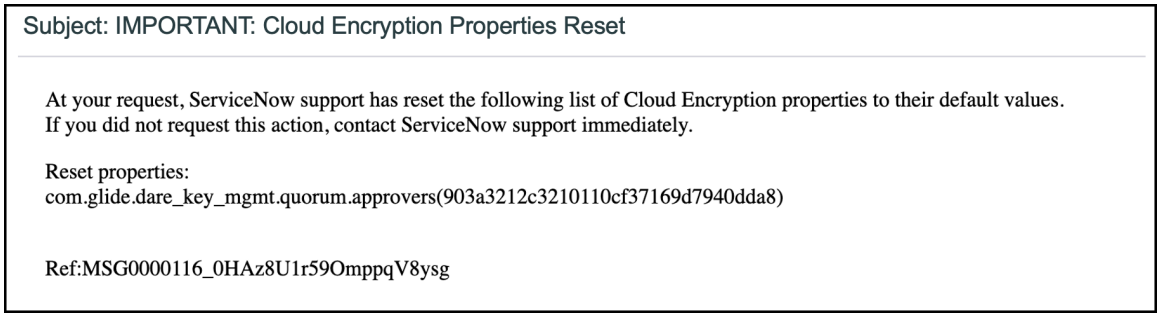
Importante: As falhas de validação de detecção de adulteração só podem ser resolvidas com a assistência do suporte da ServiceNow.



Se a detecção de adulteração não validar qualquer uma das configurações de controle de quórum, entre em contato com o suporte da ServiceNow para obter assistência na resolução do problema. Depois que um agente de suporte resolve a falha de validação, os

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

administradores de segurança e KMF recebem uma notificação indicando que o problema foi resolvido.


Subject: IMPORTANT: Cloud Encryption Properties Reset

At your request, ServiceNow support has reset the following list of Cloud Encryption properties to their default values.
If you did not request this action, contact ServiceNow support immediately.

Reset properties:
com.glide.dare_key_mgmt.quorum.approvers(903a3212c3210110cf37169d7940dda8)

Ref:MSG0000116_0HAz8U1r59OmppqV8ysg

Criptografia completa de disco

A criptografia completa de disco (FDE) aplica a criptografia a todo o sistema de armazenamento somente no servidor de banco de dados, porque este é o único componente de armazenamento de dados do cliente. A FDE protege somente contra perda física ou roubo de dispositivos de armazenamento. Quando os servidores de disco criptografados estão ligados e fornecendo dados, a criptografia não fornece proteção adicional.

Criptografia completa de disco

A criptografia completa de disco pode ser relevante para organizações altamente regulamentadas, mas pode adicionar um custo significativo à implantação de ServiceNow de um cliente . As medidas em vigor da ServiceNow para reduzir a perda ou o roubo de dispositivos de armazenamento também podem ser um fator na sua seleção.

Da perspectiva da Now Platform, todos os fluxos de dados são descriptografados.

Ambientes comerciais usam criptografia completa de disco (FDE) com hardware validado FIPS 140 ou dispositivos de armazenamento que estão no processo de validação junto com uma opção de hardware dedicado ServiceNow a um custo extra. A FDE se aplica ao próprio hardware e, portanto, fornece criptografia em repouso para todos os dados armazenados em cada instância atribuída a você.

Para obter mais detalhes sobre como selecionar FDE e opções de hardware dedicadas, entre em contato com seu representante ServiceNow.

Edge Encryption

O ServiceNow® Edge Encryption ™ criptografa dados confidenciais nas instalações da sua empresa antes de enviá-los pela Internet para sua instância da ServiceNow (criptografada em trânsito), onde permanecerão criptografados em repouso.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Conheça os recursos e o valor comercial do Edge Encryption.

Entenda como planejar o Edge Encryption.

de Instalação

Instale o Edge Encryption.

Atualizando o Edge Encryption

de upgrade

Saiba como fazer upgrade do Edge Encryption.

Configurar

Entenda como configurar o Edge Encryption.

Como explorar o Edge Encryption

O Edge Encryption é um sistema de criptografia de rede que reside em sua rede e que criptografa e descriptografa dados confidenciais conforme eles trafegam entre o datacenter e a nuvem do ServiceNow.

O que é Edge Encryption

Também conhecido como criptografia do "lado do cliente", o Edge requer que todo o tráfego bidirecional do usuário passe por proxies mantidos em sua infraestrutura. Você tem controle total sobre o gerenciamento de chaves porque elas são armazenadas no proxy na sua infraestrutura. A Now Platform não pode descriptografar seu texto cifrado para acessar suas chaves.

O recurso Edge Encryption é uma opção com custo adicional que fornece a capacidade de controlar a criptografia de ponta a ponta dos dados e o gerenciamento de chaves. O Edge Encryption usa uma aplicação proxy, fornecido pela ServiceNow e instalado por você em sua própria rede. Essa aplicação de proxy tokeniza padrões de dados especificados ou criptografa campos de cadeia de caracteres, campos de data, campos de data/hora e dados de anexo antes de serem enviados do seu ambiente para a sua instância. A aplicação de proxy também descriptografa os mesmos dados, novamente somente em sua própria rede, usando chaves armazenadas somente em sua própria rede.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

As chaves de criptografia relevantes e a configuração existem somente no proxy do Edge na sua rede e não estão visíveis para a ServiceNow. Os dados são criptografados a partir do momento em que saem do ambiente e só são descriptografados na recuperação. Em nenhum momento os dados são acessíveis em texto sem formatação por sistemas ou pessoal da ServiceNow.

Quem usa Edge Encryption

Somente um usuário conectado à instância por meio de um servidor proxy em sua rede pode exibir dados criptografados em texto simples. Da mesma forma, somente um usuário security_admin conectado a uma instância por meio de um servidor proxy em sua rede pode configurar e administrar o Edge Encryption.

Como o servidor proxy reside na sua rede, você possui e gerencia as chaves de criptografia e elas nunca são enviadas para a instância. Como resultado, a ServiceNow nunca mostra dados confidenciais em texto não criptografado.

Além da configuração de proxy do Edge e do gerenciamento de regras, você é responsável pelos requisitos usuais de operação de um servidor em seu ambiente (incluindo hospedagem, roteamento, backup, configuração de DNS e assim por diante) para habilitar e oferecer suporte a seus proxies do Edge.

Criptografia e tokenização

O Edge Encryption oferece suporte à criptografia (por meio de configurações de criptografia) e à tokenização (por meio de padrões de criptografia) como um meio de proteger suas informações confidenciais.

Configurações de criptografia

Você pode criptografar campos individuais usando configurações de criptografia. O Edge Encryption é compatível com chaves de criptografia AES de 128 bits e AES de 256 bits. O Edge Encryption oferece suporte a tipos de criptografia padrão, de preservação de igualdade e de preservação de ordem.

Além dos anexos, você pode criptografar os seguintes tipos de campo:

- Data
- E-mail
- Data/Hora
- HTML
- Endereço IP
- Diário
- Entrada de Diário
- Texto de várias linhas
- Texto de linha única
- Cadeia de caracteres
- URL

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

Se um campo de diário a ser criptografado for adicionado ao fluxo de atividades, todas as entradas do usuário no campo serão criptografadas no fluxo de atividades.

Caracteres de vários bytes nos tipos de campo compatíveis podem ser criptografados.

Também é possível criptografar os seguintes tipos de variáveis do catálogo de serviços:

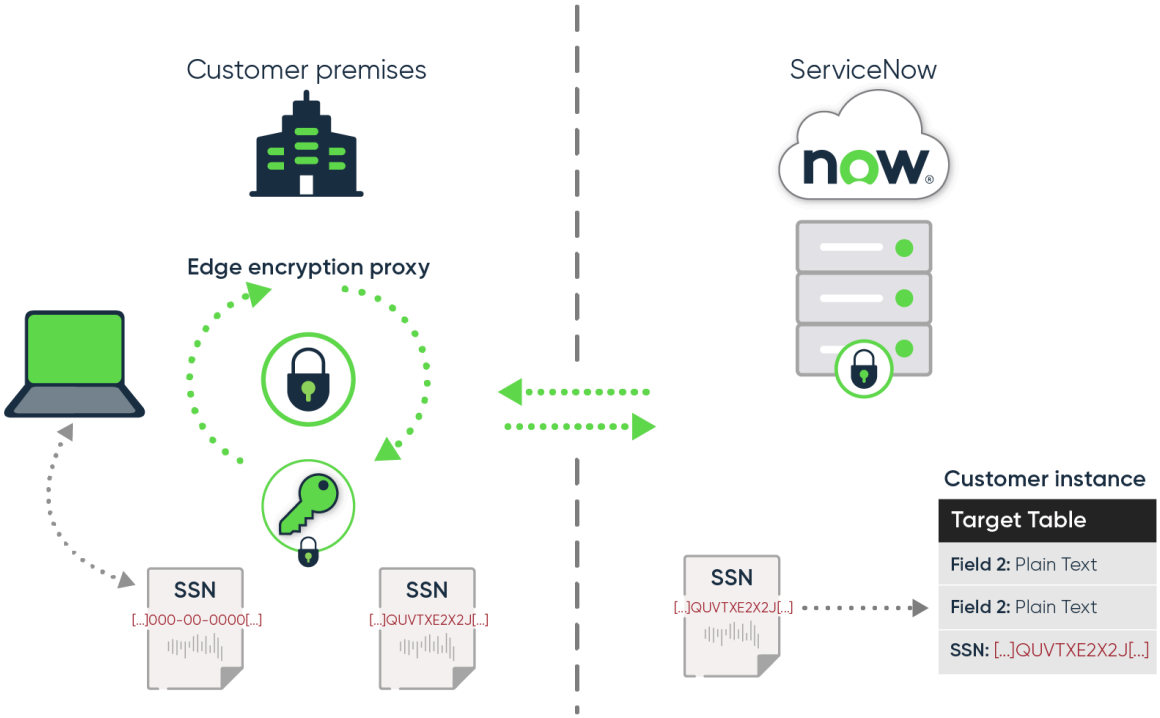
- Tipos de Cadeia de caracteres
- ◦ Texto de linha única
  ◦ Texto de várias linhas
  ◦ Texto de linha única larga
- Data
- Data/Hora
- URL
- E-mail
- HTML
- Endereço IP

Padrões de criptografia

É possível usar padrões de criptografia para tokenizar cadeias de caracteres que correspondem a padrões regulares, como CPF e números de cartão de crédito. Embora as configurações de criptografia devam ser o principal método de criptografia, use os padrões de criptografia como um suplemento para proteger informações confidenciais encontradas fora dos campos criptografados.

Nota: O servidor proxy do Edge Encryption requer um banco de dados MySQL em sua rede somente se estiver usando criptografia de preservação de ordem ou padrões de criptografia. Valores de texto não criptografado são armazenados no banco de dados do proxy em sua rede. Por esse motivo, é essencial que você proteja e faça backup regularmente do seu banco de dados de proxy. Para obter recomendações, consulte Componentes do Edge Encryption.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Edge Encryption na Now Platform

O Edge Encryption atua como um gateway entre seu navegador e sua instância da ServiceNow. O tráfego do seu navegador passa pelo gateway em seu caminho para a instância da ServiceNow. O gateway, por sua vez, é configurado para criptografar dados de saída que estão marcados para criptografia. O tráfego de entrada é descriptografado por meio do gateway e o usuário final vê o texto não criptografado no navegador. A vantagem desta implementação sob uma perspectiva de controle de segurança é que a criptografia e o gerenciamento de chaves são tratados externamente a partir da ServiceNow.

Prós e contras

Assim como acontece com o Criptografia em nível de coluna para empresas e o Criptografia em nível de coluna, o Edge Encryption impõe algumas limitações funcionais em uma instância como resultado da segurança adicional. O proxy local do Edge, no entanto, também fornece algumas funcionalidades adicionais relacionadas à classificação quando comparado ao Criptografia em nível de coluna.

Prós:

- O Edge Encryption fornece controle absoluto de quem vê suas informações e evita violações de dados.
- As informações permanecem no servidor proxy e nunca saem da rede sem criptografia.
- As informações são criptografadas em trânsito, antes mesmo de atingirem a instância da ServiceNow.
- Você mantém e gerencia todas as suas próprias chaves de criptografia. Mais ninguém, nem mesmo o pessoal da ServiceNow, pode acessar suas chaves.
- Você pode escolher a força do algoritmo de criptografia: AES-128 ou AES-256.
- O Edge Encryption inclui a capacidade de criptografar texto de cadeia de caracteres, campos de Data e Data/Hora, anexos, URLs e diários.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- O Edge Encryption fornece criptografia Padrão, de Preservação de igualdade e de Preservação de ordem de dados em repouso no banco de dados e na instância.
- As regras de criptografia permitem gravar scripts personalizados que informam ao servidor proxy especificamente o que criptografar e onde colocar essas informações criptografadas na instância. Esses scripts são úteis quando a estrutura de dados não corresponde exatamente à instância da ServiceNow.
- Os padrões de criptografia permitem tokenizar informações como senhas.

Contras:

- O Edge Encryption requer um salto de rede extra por meio do cluster de proxies do Edge e processamento extra, o que pode adicionar atraso ao tráfego. O atraso de processamento adicionado da aplicação Edge Encryption é insignificante em comparação com o salto de rede.
- Manter suas próprias chaves de criptografia pode ser complexo e demorado.
- Você pode manter no máximo duas chaves, sem flexibilidade para definir chaves diferentes para diferentes subconjuntos de colunas/dados ou para diferentes funções e assim por diante.
- O Edge Encryption tem o efeito colateral de impedir o servidor ou a plataforma de descriptografar os dados para executar qualquer manipulação dos dados descriptografados. Como consequência, a funcionalidade e o processamento de dados na Now Platform podem ser restritos ao criptografar colunas com o Edge Encryption.

O que saber antes de começar

Como a criptografia e a tokenização mudam a natureza dos dados, o Edge Encryption pode afetar outros processos de instância. Antes de usar o Edge Encryption, considere com cuidado o impacto em sua instância.

Como o servidor proxy é instalado e mantido em sua rede, o Edge Encryption requer administração e gerenciamento de rede. Revise os requisitos de rede para garantir uma implementação sem problemas.

Analise os tópicos a seguir para entender o impacto do Edge Encryption em sua instância:

- Planejamento do Edge Encryption
- Requisitos do sistema Edge Encryption
- Dimensionando seu ambiente do Edge Encryption
- Calcule o tamanho do banco de dados de preservação de ordem e tokenização
- Limitações do Edge Encryption
- Gerenciamento de chaves do Edge Encryption

Componentes do Edge Encryption

O Edge Encryption é composto pelo servidor proxy do Edge Encryption, que é executado em um servidor em sua rede, e pelo plug-in Edge Encryption que deve ser instalado em sua instância da ServiceNow. Se estiver usando tipos de criptografia que preservam a ordem ou padrões de criptografia, um banco de dados de proxy também deve ser instalado em sua rede.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Aplicação de proxy

Ao passar pelo servidor proxy do Edge Encryption, o plug-in do Edge Encryption permite que você especifique quais campos, padrões e anexos devem ser criptografados. Você também pode gerenciar regras de criptografia para criptografar solicitações específicas e programar trabalhos de criptografia em massa.

Servidor proxy

O servidor proxy do Edge Encryption usa regras de criptografia para identificar em uma solicitação HTTP o que precisa ser criptografado e criptografa antes de encaminhar a solicitação para a instância. Para descriptografia, o servidor proxy do Edge Encryption examina as respostas HTTP em busca de dados criptografados e os descriptografa antes de enviar a resposta de volta para o cliente. Para que essa descriptografia aconteça, todas as solicitações e respostas HTTP devem passar pelo servidor proxy do Edge Encryption. Essas solicitações HTTP incluem todas as solicitações originadas de um navegador, bem como solicitações SOAP ou REST.

Banco de dados do proxy

Se estiver usando criptografia de preservação de ordem ou padrões de criptografia, os servidores proxy devem contar com um banco de dados MySQL localizado em sua rede. Todos os servidores proxy em sua rede devem usar o mesmo banco de dados.

O banco de dados do proxy contém essas tabelas.

Tabelas de banco de dados do proxy

Nome	Descrição
db_id	ID exclusivo do banco de dados
edge_token_map	Dados de padrão de criptografia
token_map	Dados de criptografia de preservação de ordem

Como fazer o backup do seu banco de dados de proxy

Como os padrões de criptografia dependem de tokenização, os valores de texto não criptografado são armazenados no banco de dados do proxy. Se o banco de dados for perdido, os valores de texto não criptografado não poderão ser restaurados. É essencial que você mantenha backups regulares. Para evitar perda de dados, faça backup do banco de dados do proxy de acordo com as recomendações ServiceNow.

- Faça backup do seu banco de dados a cada 24 horas.
- Mantenha os arquivos de log binário do banco de dados MySQL por pelo menos dois dias. Depois de restaurar um backup, use o log binário para gerar novamente todos os dados perdidos desde o backup mais recente.

Clientes do Edge Encryption

O Edge Encryption usa três clientes para informar à instância que o proxy está em execução, para sincronizar as solicitações entre o proxy e a instância e para encaminhar todas as solicitações do usuário final para a instância após qualquer criptografia em potencial.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Cliente	Descrição
Cliente de pulsação/keepalive	Responsável por enviar uma solicitação para a instância da ServiceNow a cada 5 segundos para que a instância saiba que esse proxy está instalado e em execução. As solicitações orientam o campo last_response_on na tabela de proxy do Edge e, como consequência, orientam o estado do proxy. Se o seu sistema tiver problemas para enviar as solicitações, ou se a solicitação ou o processamento da solicitação estiverem atrasados, a instância poderá marcar o proxy como sem resposta, mesmo se os outros clientes (incluindo o para tráfego do usuário) estiverem ativos e em execução. Esse cliente também controla o status online do proxy na instância. A propriedade *edgeencryption.proxy.keepalive.interval* controla a taxa de pesquisa desse cliente. O padrão é 5 (segundos).
cliente de pesquisa/sincronização	Responsável por várias solicitações que o proxy envia à instância para sincronizar na configuração do Edge Encryption (por exemplo, qual tabela, coluna ou anexo a ser criptografado, chaves, trabalhos, regras e padrões de tokenização). A propriedade *edgeencryption.config.poll.interval* controla a taxa de pesquisa desse cliente. ⚠ **Aviso:** Não mude esta configuração. Mudar a configuração padrão do intervalo de pesquisa de proxy pode resultar em atrasos de sincronização ao atualizar as configurações do Edge Encryption.
cliente de tráfego padrão/de usuário	Para todo o restante, esse cliente lida com as todas as solicitações do usuário final e as encaminha para a instância da ServiceNow após qualquer criptografia em potencial. Esse cliente também lida com respostas da instância, encaminhando-as para o usuário final após qualquer descriptografia em potencial.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Gerenciamento de chaves do Edge Encryption

Você é responsável por fornecer e gerenciar as chaves de criptografia usadas pelo Edge Encryption.

Este tópico se refere a chaves para o produto Edge Encryption. Se estiver procurando informações sobre o Key Management Framework, que pode ser usado com o Criptografia em nível de coluna, consulteKey Management Framework.

Ao obter e criar chaves de criptografia compatíveis com os tipos de criptografia usados pelo Edge Encryption, considere o seguinte:

- Se deve ser usado o AES de 128 bits ou o AES de 256 bits. Você deve definir uma chave de criptografia AES de 128 bits padrão, mesmo que ela não seja usada.
- Se deve ser usado o sistema de arquivos, o Java KeyStore ou o Enterprise Key Management (EKM).
- Quando girar chaves de criptografia.
- Quando e se um trabalho de criptografia em massa deve ser usado para criptografar novamente os dados usando a nova chave.

Antes de remover uma chave dos arquivos de configuração de proxy e do repositório de chaves, é essencial descriptografar todos os dados na instância que usa a chave. É possível fazer isso adicionando uma nova chave de criptografia e programando um trabalho de rotação de chave em massa.

Repositórios de chaves

O Edge Encryption é compatível com os seguintes tipos de armazenamento de chave.

Repositório de arquivo

As chaves são armazenadas em um arquivo em um sistema de arquivos que pode ser acessado pelo proxy do Edge Encryption. As chaves de criptografia armazenadas em um arquivo não são criptografadas, portanto, é sua responsabilidade proteger esses arquivos.

Java KeyStore

As chaves são armazenadas no JCEKS KeyStore do Java. Um Java KeyStore é protegido por senha, portanto, é mais seguro do que armazenar chaves em um arquivo no repositório de arquivos. Um único Java KeyStore pode armazenar várias chaves e as elas são identificadas por um alias de chave, facilitando o gerenciamento de várias chaves.

Enterprise Key Management (EKM)

As chaves são armazenadas e recuperadas com os sistemas de gerenciamento de chaves SafeNet KeySecure ou Unbound Technology.

O proxy do Edge Encryption é fornecido com o arquivo do Java JCEKS KeyStore chamado `keystore.jceks` no diretório do `repositório de chaves`. Este arquivo do repositório de chaves contém a chave pública da ServiceNow usada para validar regras de criptografia assinadas pela ServiceNow.

Nota: Se estiver usando um repositório de chaves diferente do sistema de base Java JCEKS KeyStore, você deverá importar a chave pública da ServiceNow para o repositório de chaves. O alias da chave pública é *`servicenow`*.

Além das chaves de criptografia, o Java JCEKS KeyStore é usado para armazenar o par de chaves RSA para assinar digitalmente a configuração de criptografia e as regras de

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

criptografia armazenadas na instância, além do certificado digital que o proxy do Edge Encryption usa para estabelecer uma conexão segura com os navegadores e outros clientes.

Controle de versões de chave da SafeNet para Edge Encryption

Use o controle de versões de chave da SafeNet para simplificar a mudança de chaves. Em vez de criar um alias para cada nova chave, o controle de versões de chave da SafeNet mantém o mesmo alias e incrementa a versão.

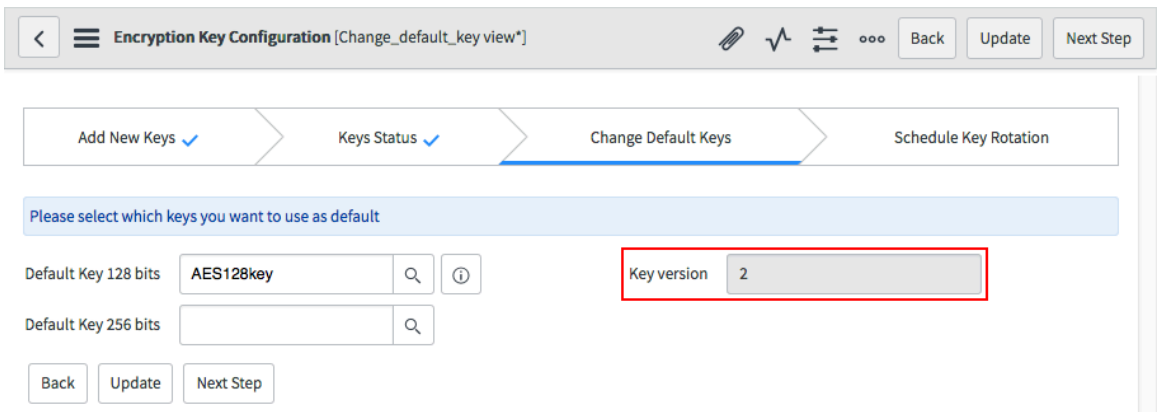
Você deve configurar o controle de versões de chave na SafeNet antes de configurar o controle de versões de chave da SafeNet no servidor proxy do Edge.

Nota: Os proxies do Edge instalados antes da versão London são compatíveis com chaves da SafeNet, mas não com o controle de versões de chaves da SafeNet. Se você usar por engano uma chave com controle de versão em um proxy do Kingston ou anterior, ao fazer upgrade para uma versão London ou posterior, o proxy do London ou posterior detectará o problema e, para evitar possível perda de dados, não iniciará.

Você deve primeiro programar um trabalho de rotação de chave em massa ou um trabalho de rotação de chave única para substituir a chave com controle de versão antiga da SafeNet por uma chave sem controle de versão e, em seguida, criar uma nova chave com controle de versão da SafeNet, se necessário. Essa nova chave com controle de versão é segura para uso com o proxy do London ou posterior e você pode reiniciar o proxy.

Configuração de chave de criptografia

Se estiver usando chaves com controle de versão da SafeNet, a seção Mudar chaves padrão do formulário Configuração de chave de criptografia incluirá novos campos para a **versão de chave** das chaves padrão de 128 bits e 256 bits. Os campos **Versão de chave** de chave estarão esmaecidos e não poderão ser editados.

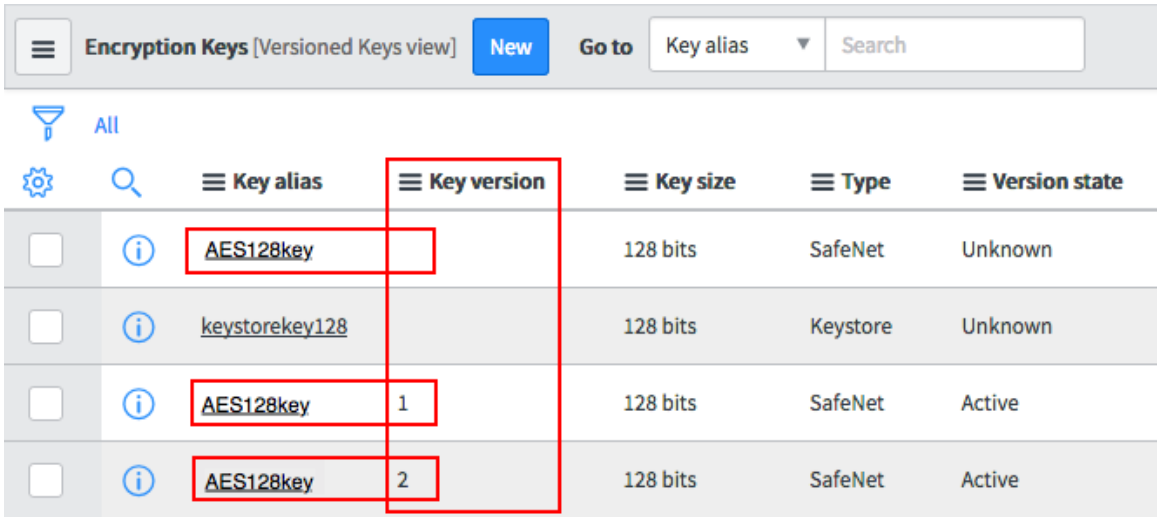


Para obter os procedimentos, consulte Configurar chaves de criptografia na instância.

Chaves com controle de versão

Se estiver usando chaves com controle de versão da SafeNet, quando navegar até a **Configuração do Edge Encryption** > **Configuração de chave de criptografia** > **Todas as chaves**, as chaves com controle de versão incluirão a **Versão da chave**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Um número de versão não aparece nas entradas iniciais feitas na seção Mudar chaves padrão do formulário de Configuração de chave de criptografia. Quando o servidor proxy solicita uma chave da SafeNet, o sistema adiciona uma nova linha para o alias e adiciona a **Versão da chave**.

No exemplo acima, **AES128key** está listada três vezes:

- A primeira listagem, sem indicação de **versão da chave**, é a entrada inicial.
- A segunda listagem, com **1** na coluna **Versão da chave**, é a primeira versão da chave retornada da SafeNet.
- A segunda listagem, com **2** na coluna **Versão da chave**, é a segunda versão da chave retornada da SafeNet.
- Conforme outras versões da chave são retornadas da SafeNet, novas linhas são adicionadas para registrar a **Versão da chave** em uso atual.

Configurações e padrões de criptografia

Com o Edge Encryption, você pode criptografar campos e tokenizar cadeias de caracteres.

Configurações de criptografia

Você pode criptografar campos individuais usando configurações de criptografia. O Edge Encryption oferece suporte a chaves de criptografia AES de 128 bits. Se os arquivos de Política de Jurisdição de Força Ilimitada do Java Cryptography Extension (JCE) estiverem instalados, o Edge Encryption será compatível a chaves de criptografia AES de 256 bits para cada tipo de criptografia. O Edge Encryption é compatível com os seguintes tipos de configurações de criptografia.

Criptografia padrão

O valor criptografado de um campo será diferente cada vez que o campo for criptografado, mesmo quando o valor do campo permanecer o mesmo. A criptografia padrão é a forma mais robusta de criptografia. Os campos que usam criptografia padrão não podem ser classificados, agrupados ou filtrados.

Criptografia de preservação da igualdade

O valor criptografado de um campo será o mesmo quando o valor do campo permanecer o mesmo. É compatível com a comparações de igualdade e agrupamento por operações em um campo.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Quando a criptografia de preservação de igualdade for selecionada para um campo que já contém dados, a execução de um grupo por ação no campo poderá não agrupar campos com o mesmo valor se um estiver criptografado e o outro não.

Criptografia de preservação de ordem

Usa tokens e criptografia para proteger dados em seu banco de dados de proxy. Oferece suporte a comparações de igualdade, operações de grupo por e a capacidade de classificar dados. O tipo de criptografia de preservação de ordem só será compatível se houver um banco de dados MySQL configurado para o servidor proxy do Edge Encryption.

Nota: Ao usar a criptografia de preservação de ordem e o banco de dados do proxy estiver desativado, as atualizações podem ser feitas nos campos usando a criptografia de preservação de ordem. No entanto, a ordem de classificação não será correta ao tentar classificar dados com base nesses campos. Os grupos também não funcionarão como esperado. Quando o banco de dados do proxy estiver operacional novamente, programe um trabalho de reparo de token de ordem para reparar tokens ausentes.

Tipos de criptografia

Os tipos de criptografia a seguir estão listados em qualidade de segurança decrescente.

Tipo de criptografia	Descrição
AES 256 padrão	Os campos não podem ser filtrados, classificados ou comparados.
AES 128 padrão	Os campos não podem ser filtrados, classificados ou comparados.
Preservação de igualdade AES 256	Os campos podem ser filtrados usando comparações de igualdade.
Preservação de igualdade AES 128	Os campos podem ser filtrados usando comparações de igualdade.
Preservação de ordem AES 256	Os campos podem ser classificados e a filtragem de comparação de igualdade pode ser usada. Requer o uso de um banco de dados MySQL em sua rede.
Preservação de ordem AES 128	Os campos podem ser classificados e a filtragem de comparação de igualdade pode ser usada. Requer o uso de um banco de dados MySQL em sua rede.

Padrões de criptografia

Você pode proteger dados confidenciais encontrados em cadeias de caracteres usando padrões de criptografia. Depois que um padrão de criptografia é armazenado e ativado, o servidor proxy do Edge Encryption identifica cadeias de caracteres que correspondem ao padrão nas solicitações. Uma vez localizada, a cadeia de caracteres de texto não criptografado é armazenada no banco de dados do proxy e substituída na instância por um token. Use padrões de criptografia para tokenizar cadeias de caracteres que correspondem a padrões regulares, como CPF e números de cartão de crédito. Embora recomendemos as configurações de criptografia como principal método de criptografia,

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

use os padrões de criptografia como um suplemento para proteger informações confidenciais encontradas fora dos campos criptografados.

Nota: O servidor proxy do Edge Encryption requer um banco de dados MySQL em sua rede somente se estiver usando criptografia de preservação de ordem ou padrões de criptografia. Valores de texto não criptografado são armazenados no banco de dados do proxy em sua rede. Por esse motivo, é essencial que você proteja e faça backup regularmente do seu banco de dados de proxy. Para obter recomendações, consulte Componentes do Edge Encryption.

Informações relacionadas

Como criptografar campos usando configurações de criptografia

Como tokenizar cadeias de caracteres usando padrões de criptografia

Instalação com Edge Encryption

O Edge Encryption instala tabelas para armazenar dados relacionados à criptografia, propriedades do sistema para configurar o comportamento padrão e a função edge_encryption para administrar o Edge Encryption.

Tabelas instaladas com o Edge Encryption

O Edge Encryption adiciona as seguintes tabelas.

Configuração do Edge Encryption [sys_encryption_configuration]

Contém campos e tabelas criptografados para os quais os anexos serão criptografados.

Regra do Edge Encryption [sys_encryption_rule]

Contém um registro para cada regra. Uma regra tem um nome, a condição quando ela é usada, um script e um campo de ordem.

Log de inserção inválida do Edge Encryption [sys_edge_encryption_invalid_insert_log]

Contém mensagens de log criadas para tentativas de salvar dados não criptografados em um campo criptografado.

Proxy do Edge Encryption [sys_encryption_proxy]

Contém informações sobre a aplicação de proxy de criptografia.

Tipo de criptografia de proxy do Edge [sys_proxy_encryption_type]

Usado para habilitar e desabilitar tipos de criptografia no formulário de criptografia.

Execução de trabalho de criptografia [sys_encryption_job_execution]

Oferece suporte a trabalhos de criptografia em massa.

Parte da execução do trabalho de criptografia [sys_encryption_job_execution_chunk]

Oferece suporte a trabalhos de criptografia em massa.

Trabalho de criptografia programado [sysauto_encryption_job]

Lista trabalhos agendados de criptografia, descriptografia, rotação de chave, reparo de token de ordem e recuperação de banco de dados.

Configuração de chave de criptografia [sys_encryption_key_configuration]

Lista as chaves de criptografia padrão

Chave de criptografia [sys_encryption_key]

Lista as chaves e os atributos de chave disponíveis.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Chave de criptografia de proxy [sys_encryption_proxy_key]

Lista as chaves de criptografia de proxy.

Propriedades instaladas com o Edge Encryption

O Edge Encryption adiciona as seguintes propriedades.

Nota: Para abrir a tabela Propriedades do sistema [sys_properties], digite `sys_properties.list` no filtro de navegação.

glide.edge.pattern.disallowed.chars

Uma lista de caracteres que não são permitidos nos padrões.

- **Tipo**: uma cadeia de caracteres de uma lista de valores separados por vírgulas
- **Local**: Tabela [sys_properties] Propriedades do sistema

glide.edge.pattern.min.size

O tamanho mínimo do padrão permitido. Permitir padrões menores significa encontrar mais correspondências, o que aumenta a sobrecarga.

- **Tipo**: número
- **Valor padrão**: 5
- **Local**: Tabela [sys_properties] Propriedades do sistema

sn_edge_encryption.logging.destination

Onde as mensagens são registradas.

- **Tipo**: cadeia de caracteres
- **Valor padrão**: arquivo
- **Local**: Tabela [sys_properties] Propriedades do sistema

sn_edge_encryption.logging.verbosity

O nível de registro em log a ser usado.

- **Tipo**: cadeia de caracteres
- **Valor padrão**: info
- **Local**: Tabela [sys_properties] Propriedades do sistema

sn_edge_encryption.encryption.proxy.buildtag

A versão do proxy registrada com sua instância.

- **Tipo**: cadeia de caracteres
- **Local**: Tabela [sys_properties] Propriedades do sistema

sn_edge_encryption.cleartext.allowed

Quando verdadeiro, permite que o texto não criptografado seja salvo em um campo criptografado. Isso acontece quando um usuário está acessando a instância sem passar pelo proxy do Edge Encryption. Quando falso, o sistema impede que o texto não criptografado seja salvo em um campo criptografado.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- **Tipo**: booleano
- **Valor padrão**: falso
- **Local**: Tabela [sys_properties] Propriedades do sistema

Planejamento do Edge Encryption

A implementação bem-sucedida do Edge Encryption requer planejamento e preparação.

Na fase de planejamento, responda as seguintes questões.

- Quais campos devem ser criptografados?
- Quais tipos de criptografia devem ser usados?
- Quantos proxies do Edge Encryption são necessários? Consulte Dimensionando seu ambiente do Edge Encryption para recomendações e considerações.
- Se foram usados um tipo de criptografia de preservação de ordem ou padrões de criptografia, onde está localizado o banco de dados MySQL?
- Qual sistema de gerenciamento de chaves será usado?

Os administradores do sistema, administradores de rede e membros da equipe de segurança têm diferentes tarefas a cumprir para implementar Edge Encryption.

- Os administradores do sistema precisam da função de administrador de segurança. O administrador do sistema deve:
  - Baixar a aplicação de proxy do Edge Encryption.
  - Configurar uma conta de usuário do Edge Encryption a serem usados pelos proxies para se conectarem à instância. A função edge_encryption deve ser atribuída ao usuário.
  - Configurar chaves de criptografia e definir as chaves padrão.
  - Configurar o Edge Encryption na instância.
  - Programar trabalhos de criptografia.
  - Monitorar o Edge Encryption.
  - Criar e editar regras de criptografia.
- O administrador da rede deve:
  - Instalar a aplicação de proxy do Edge Encryption.
  - Conhecer os endereços de rede dos servidores proxy e o banco de dados do proxy usado para preservar a ordem e os padrões de criptografia.
  - Instalar o banco de dados do proxy a ser usado para preservar a ordem e os padrões de criptografia.
  - Iniciar e parar as aplicações de proxy.
  - Executar gerenciamento de chave de criptografia.
  - Determinar como mapear usuários para aplicações de proxy de criptografia. Isso pode ser feito com configurações de DNS ou regras de roteamento e é específico para cada rede.
  - Gerenciar vários servidores proxy.
  - Configurar os pools e as definições do balanceador de carga.
- Seu administrador de segurança deve determinar os tipos de criptografia a serem atribuídos a cada campo.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Requisitos do sistema Edge Encryption

É possível executar a aplicação de proxy Edge Encryption em servidores ou máquinas virtuais que são executados em sistemas operacionais Microsoft Windows ou Linux. Para obter o desempenho ideal, verifique se sua configuração atende a esses requisitos.

Requisitos do Java

A máquina host que instala ou executa o servidor proxy Edge Encryption deve manter uma versão compatível do Java. As versões atualmente compatíveis são Java 11.0.6 ou posterior na série da versão 11.x

Nota: O Java 8 não será mais compatível a partir da versão Utah. Faça o upgrade do seu ambiente com o proxy Edge Encryption para Java 11 antes de tentar instalar a versão Utah do proxy Edge Encryption.

Nota: O Java não permite chaves de força ilimitada automaticamente. Você deverá habilitar especificamente o uso da criptografia AES de 256 bits.

Suporte para OpenJDK

O Now Platform é compatível com o OpenJDK versão 11.

Configuração mínima do servidor proxy

Um servidor proxy necessita da seguinte configuração mínima:

- 4 GB de RAM por servidor proxy (Recomendamos 6 GB é para a maioria das implantações).

  Nota: O host do servidor proxy requer pelo menos 1 GB de RAM a mais do que o servidor proxy. O host do servidor proxy precisa de 1 GB extra para serviços do sistema operacional. Por exemplo, se você configurar um servidor proxy para usar 4 GB de RAM, deverá instalar pelo menos 5 GB de RAM no host do servidor proxy.

  Como o servidor proxy requer pelo menos 4 GB de memória, os JREs de 32 bits e os sistemas operacionais de 32 bits já não compatíveis a partir da versão London.

- CPU de 3 GHz ou mais (De preferência, CPU de 4 núcleos para desempenho ideal).
- Vários servidores proxy por trás de um balanceador de carga. O número de servidores proxy necessários depende do número de nós de aplicação, do número de usuários simultâneos e do número de servidores necessários para o failover. Consulte Dimensionando seu ambiente do Edge Encryption para obter mais informações.
- Capacidade de execução simultaneamente com outros serviços, dependendo da utilização do servidor e da disponibilidade de recursos.

Sistemas compatíveis com servidor proxy

Os seguintes sistemas são compatíveis

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Sistema Compatível	Descrição
Windows Server 2012, 2012-R2, 2016 e edições 2019	• Máquinas virtuais ou hardware físico • Sistemas de 64 bits
Linux	• Máquinas virtuais ou hardware físico • Sistemas de 64 bits Em sistemas Linux de 64 bits, você deve instalar a biblioteca GNU C de 32 bits (glibc). O comando de instalação do CentOS é `yum install glibc.i686`.

Requisitos de versão do servidor proxy

Mantenha a sua versão do proxy do Edge Encryption em sincronia com a versão da instância ServiceNow (mesma versão principal, por exemplo Tokyo). Para eliminar o tempo de inatividade durante o processo de upgrade, o proxy do Edge Encryption é compatível com versões anteriores. No entanto, é importante realizar o upgrade o mais rápido possível para garantir que os usuários possam acessar novos recursos e correções de erros importantes.

Requisitos de conexão do servidor proxy

O servidor proxy que executa a aplicação Edge Encryption deve ser capaz de se comunicar com as máquinas em sua rede. Certifique-se de que o servidor proxy tenha estes privilégios de rede:

Privilégio de rede	Descrição
Acesso ao firewall	Configure quaisquer firewalls entre o servidor proxy e os dispositivos do cliente para permitir uma conexão. Se sua rede usa uma zona desmilitarizada (DMZ) para adicionar uma camada extra de segurança à sua rede local (LAN) e se os protocolos de segurança de rede limitam o acesso à porta de dentro da rede para o DMZ, talvez seja necessário implantar um servidor proxy em uma máquina dentro do DMZ.
Acesso de rede	Configure cada cliente para permitir que o servidor proxy se conecte a ele. Se a segurança da rede impedir que você configure novas máquinas que possam se conectar aos clientes, instale o servidor proxy em uma máquina existente com privilégios de conexão.
Acesso à instância	Certifique-se de que o servidor proxy tenha acesso à rede para a instância. Certifique-se de configurar a rede do servidor proxy para permitir o tráfego pela porta TCP 443.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Privilégio de rede	Descrição
Conta de rede	Instale o servidor proxy com um administrador local ou de domínio.

Requisitos do sistema de preservação de pedidos e de banco de dados de tokenização

A criptografia que preserva a ordem e os padrões de criptografia exigem a configuração de um banco de dados Oracle MySQL para o servidor proxy do Edge Encryption. A criptografia de preservação de ordem permite que qualquer operação de comparação seja aplicada diretamente nos dados criptografados, sem descriptografar os dados antes. Os padrões de criptografia permitem substituir padrões de cadeia de caracteres por tokens (a chamada tokenização) antes de serem enviados e armazenados no banco de dados. Devido ao tamanho do banco de dados do MySQL, use um servidor proxy dedicado para executar o banco de dados de preservação de ordem e de tokenização.

Os requisitos mínimos do sistema de banco de dados incluem:

Banco de dados MySQL	Requisito
Versão	Banco de Dados MySQL versões 5.7 e 8.0 **Nota:** As versões 5.5 e 5.6 do MySQL não são mais testadas e atingiram o fim do suporte.
SO	Sistemas de 64 bits
CPU	CPU de 2 GHz ou mais (De preferência, CPU de 4 núcleos para obter um desempenho ideal).
RAM	16 GB
Disco	Rede de Área de Armazenamento (SAN) ou armazenamento local (RAID 10 é recomendado)
Tamanho	Determinado pelo número de registros potenciais multiplicado pelo tamanho do registro. Consulte Calcule o tamanho do banco de dados de preservação de ordem e tokenização.
Configuração	Cluster de alta disponibilidade. Se você não tiver certeza de como configurar o servidor MySQL, entre em contato com o MySQL para obter informações de configuração.

Dimensionando seu ambiente do Edge Encryption

A escolha do número de servidores proxy para o seu ambiente é uma tarefa importante. Considere o número de usuários, as necessidades de redundância e a latência aceitável.

Redundância

Mantenha servidores proxy redundantes em caso de falha de hardware. Os servidores proxy devem estar localizados atrás de um balanceador de carga para fornecer um caminho

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

funcional para todos os usuários se um servidor proxy ficar inacessível. Certifique-se de que, no mínimo, dois servidores proxy estejam sempre disponíveis.

Tamanho

O tamanho se refere ao número de servidores proxy necessários para evitar a latência adicional produzida pela criptografia de dados. Dependendo do uso, é possível reduzir a quantidade de latência adicionando servidores proxy. Por exemplo, se forem executadas criptografias em massa regularmente, adicione servidores proxy adicionais para lidar com a carga ou execute as criptografias em massa quando a carga do usuário for leve. Além disso, o hardware em que o servidor proxy é executado influencia o desempenho e a latência. Servidores proxy em execução em hardware com CPUs mais rápidas, mais CPUs e mais RAM têm rendimento maior do que sistemas mais lentos e limitados.

As diretrizes a seguir presumem que o servidor proxy está sendo executado com pelo menos os requisitos mínimos de hardware. Para determinar o número de servidores proxy:

- Considere configurar um servidor proxy para cada dois nós de aplicação na instância.
- Para redundância, configure um mínimo de dois servidores proxy atrás de um balanceador de carga.
- Adicione um servidor proxy extra para cada 500 usuários simultâneos.
- Dependendo da redundância desejada, adicione servidores proxy adicionais para failover.

Por exemplo, para uma instância com 2.000 usuários, você deve ter pelo menos cinco servidores proxy atrás de um balanceador de carga. Este cálculo inclui um servidor proxy para cada 500 usuários, com um servidor proxy extra para failover. Determine com antecedência quando se aproximará o limite de 500 usuários e coloque outro servidor proxy no pool do balanceador de carga.

Balanceadores de carga

Para equilibrar as solicitações e melhorar o tempo de resposta do servidor, distribua os servidores proxy em um pool de balanceador de carga. Configure balanceadores de carga para usar o método "menos conexões". Esse método conecta as solicitações ao servidor proxy com o menor número de conexões ativas, evitando a sobrecarga de um único proxy.

Utilização da CPU

Como a criptografia e a tokenização de dados são operações com uso intensivo de CPU, os picos de CPU durante a criptografia de dados são normais e esperados. Quando a utilização da CPU é superior a 80% por vários minutos de uma vez, provavelmente o servidor proxy tem muito trabalho a fazer. Quando isso acontece, a latência aumenta no período em que a utilização da CPU está alta. Se a latência persistir, adicionar outro servidor proxy pode ajudar a diminui-la.

Memória

O servidor proxy deve ter um mínimo de 4 GB de RAM disponível (6 GB recomendado). Defina os limites inicial e superior de memória do servidor proxy com as configurações recomendadas.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Calcule o tamanho do banco de dados de preservação de ordem e tokenização

Se estiver usando criptografia de preservação de ordem ou padrões de criptografia, determine o tamanho do banco de dados MySQL multiplicando o número de registros potenciais pelo tamanho do registro.

Antes de Iniciar

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

Use uma máquina dedicada para executar o banco de dados de preservação de pedidos e de tokenização. Não execute o banco de dados no mesmo hardware que o servidor proxy.

Procedimento

1. Determine o número potencial de registros que podem incluir campos criptografados com criptografia de preservação de ordem.
   a. Multiplique o número de configurações de criptografia usando a criptografia de preservação de ordem pelo número de registros aos quais cada configuração é aplicada.
   b. Para permitir o crescimento, multiplique o resultado por três.
2. Multiplique o resultado da etapa 1 por 1.536.
   1.536 é o tamanho médio de um registro em bytes.
3. Se estiver usando padrões de criptografia, execute as etapas 1–2 para registros em token e adicione o resultado ao total.

Resultados

O valor calculado é o tamanho recomendado em bytes para seu banco de dados de preservação de pedido e tokenização.

Limitações do Edge Encryption

O Edge Encryption tem impacto nas funções do sistema. Avalie com cuidado o impacto da criptografia de um campo.

Restrições de tipos de campo

Só é possível criptografar os seguintes tipos de campo:

- Data
- E-mail
- Data/Hora
- HTML
- Endereço IP
- Diário
- Entrada de Diário
- Texto de várias linhas
- Texto de linha única

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Cadeia de caracteres
- URL

Não é possível criptografar os seguintes tipos de campo:

- Campos de opção
- Campos virtuais
- Campos em tabelas do sistema, exceto para determinados campos em sys_user
- Campos do sistema em tabelas
- Campos numéricos ou campos associados a um esquema de numeração automática
- Qualquer outro tipo de campo não listado acima

Restrições adicionais:

- Quando um campo de diário é criptografado, o botão **Publicar** é inativado, mesmo se houver vários campos de diário e somente um deles estiver criptografado.
- Os campos criptografados não estão disponíveis nas caixas **Ir para** e de filtro de cabeçalho.
- Ao criptografar campos usados como um índice, só é possível usar tipos de criptografia de preservação de pedido e preservação de igualdade. Campos indexados não podem ser criptografados usando o tipo de criptografia padrão.

Para obter mais informações, consulte Tipos de campo.

Restrições de filtragem e pesquisa

Criptografia padrão

Ao selecionar uma cadeia de caracteres, data, data/hora ou campo de URL com uma configuração de campo criptografado padrão como o operando esquerdo em um filtro, não haverá opções de filtragem disponíveis.

Criptografia de preservação da igualdade

Ao selecionar uma cadeia de caracteres, data, data/hora ou campo de URL com uma configuração de campo criptografado de preservação de igualdade como o operando esquerdo em um filtro, os seguintes operadores ficam disponíveis

- **é**
- **não é**
- **está vazio**
- **não está vazio**

Criptografia de preservação de ordem

Ao selecionar uma cadeia de caracteres com uma configuração de campo criptografado de preservação de pedido como o operando esquerdo em um filtro os seguintes operadores ficam disponíveis, além de **é**, **não é**, **está vazionão está vazio**:

- **maior que**
- **menor que**

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Ao selecionar um campo de data ou data/hora ou campo com uma configuração de campo criptografado de preservação de pedido como o operando esquerdo em um filtro, os seguintes operadores ficam disponíveis, além de **é**, **não é**, **está vazionão está vazio**:

- **depois**
- **antes**
- **após ou em**
- **antes ou em**

Seletores de data e data/hora

Em campos de Data, use o seletor de data para especificar a data:

Em campos de Data/Hora, use o seletor de data e hora para especificar a data e a hora:

Filtros de condição de lista

As opções **Mostrar correspondência** e **Filtrar** são compatíveis com listas. Somente correspondências exatas são retornadas ou filtradas.

Nota: A adição de campos criptografados em filtros de condição é compatível com scripts, como políticas de IU e regras de negócio.

Restrições de configuração

Restrições e comportamento das configurações de criptografia:

- Depois de adicionar um campo à tabela Configuração do Edge Encryption, não será possível excluir o registro de configuração. Se não desejar mais que um campo seja criptografado, desative o registro na tabela Configuração do Edge Encryption e programe um trabalho de criptografia para descriptografar os dados.
- Se um campo em uma tabela primária estiver marcado para ser criptografado, ele também será criptografado em todas as tabelas herdadas. Por exemplo, se o campo

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Descrição resumida na Tabela de tarefas estiver criptografado, o conteúdo do campo **Descrição resumida** na tabela Incidente será criptografado.

- Se um campo herdado de uma tabela primária estiver marcado para ser criptografado, o campo na tabela primária não poderá ser criptografado. Por exemplo, se o campo **Descrição resumida** na tabela Incidente for marcado para ser criptografado, o conteúdo do campo **Descrição resumida** na Tabela de tarefas não poderá ser criptografado. Nesse exemplo, é possível criptografar a **Descrição resumida** na tabela Problema.
- Quando um campo com uma configuração de criptografia definida for exportado para qualquer formato, a saída incluirá valores criptografados mesmo quando exportados por meio do servidor proxy.
- Não é possível importar dados para um campo com uma configuração de criptografia definida.
- Não é possível criptografar campos de Data e Data/Hora herdados. Os campos Data ou Data/Hora herdados de uma tabela primária não estão listados na lista suspensa do campo **Coluna** e não será possível criar configurações de criptografia de Data ou Data/Hora para esses campos.
- Só é possível criptografar um campo de Cadeia de caracteres ou URL de uma tabela primária ou de uma tabela secundária, mas não de ambas.

Restrições de instância

Impacto do uso do Edge Encryption na instância:

- A lógica de back-end não pode processar dados criptografados. Quando a instância tiver dados criptografados, qualquer regra de negócio, script de back-end ou recurso de back-end que depende da avaliação dos dados no campo criptografado não será executado corretamente.

  Nota: Os dados criptografados com criptografia de preservação de igualdade ou de pedido ainda são aprovados nas verificações de equivalência quando comparados com um valor criptografado idêntico.

- Como o processamento de e-mail vai dos sistemas de e-mail direto para a instância e não pode passar pelo proxy do Edge, os dados enviados ou recebidos por e-mail não podem ser criptografados ou descriptografados pelo proxy do Edge.
  - Dados e anexos em e-mails de entrada não são criptografados.
  - Dados e anexos em e-mails de saída permanecem criptografados e não podem ser descriptografados.
- Os scripts executados no servidor não podem mudar os dados criptografados.
- A pesquisa global não é compatível. Como a pesquisa global tenta pesquisar dados criptografados e de texto não criptografado, os resultados podem não ser os esperados.
- Os dados criptografados não podem ser copiados e colados em um registro em que o campo não esteja criptografado.
- Dependendo do tipo de criptografia selecionado, a funcionalidade da interface do usuário para os campos criptografados será reduzida. Por exemplo, a possibilidade de comparar, agrupar por, classificar e pesquisar pode ser afetada. Geralmente, quanto mais forte for a criptografia selecionada, mais a funcionalidade será reduzida.
- Nenhum hardware ou software de gerenciamento de criptografia chave de criptografia é compatível, exceto Java KeyStore, SafeNet e Unbound Technology.
- Embora vários servidores proxy conectados a uma única instância sejam compatíveis, o gerenciamento e o monitoramento do cluster de proxy de criptografia não estão disponíveis. Cada proxy deve ser gerenciado separadamente.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Configurações do sistema, como carga de trabalho e o número de campos criptografados, podem afetar o desempenho dos campos criptografados.
- O servidor proxy do Edge Encryption só pode se conectar a uma instância.
- Se a sua instância usar um banco de dados Oracle e o campo Cadeia de caracteres marcado para ser criptografado tiver mais de 2925 caracteres, esse campo não poderá ser classificado mesmo quando a criptografia de preservação de ordem estiver selecionada.
- Se sua instância usa um banco de dados Oracle, o único conjunto de caracteres compatível é o Unicode AL32UTF8.
- Dados criptografados não podem ser usados em relatórios.
- Edge Encryption não pode ser usado com o Arquivamento de dados.

Instalando o Edge Encryption

Você pode instalar um proxy do Edge Encryption manualmente ou usando o instalador interativo do Edge Encryption.

Requisitos do Java

A máquina host que instala ou executa o servidor proxy Edge Encryption deve manter uma versão compatível do Java. As versões atualmente compatíveis são Java 11.0.6 ou posterior na série da versão 11.x

Nota: O Java 8 não será mais compatível a partir da versão Utah. Faça o upgrade do seu ambiente com o proxy Edge Encryption para Java 11 antes de tentar instalar a versão Utah do proxy Edge Encryption.

Instalando o servidor proxy

A instalação do Edge Encryption inclui estas etapas.

- Instale a aplicação de proxy Edge Encryption em um servidor em sua rede usando o instalador interativo ou o instalador manual.
- Gere o par de chaves RSA para configurações de assinatura digital e regras de criptografia
- Instale a Java Cryptography Extension (JCE) se você planeja usar a criptografia AES 256.
- Se estiver usando uma conexão SSL segura, obtenha um certificado do servidor e importe-o para o Java KeyStore.
- Configure o repositório de chaves e a chave de criptografia.
- Se for necessário usar tipos de criptografia de preservação de ordem ou padrões de criptografia, configure um banco de dados MySQL em uma máquina em sua rede.
- Defina as propriedades desejadas. As propriedades estão localizadas no arquivo de configuração `edgeencryption.properties`.
- Especifique um servidor proxy como fonte confiável para que o Edge Encryption possa processar solicitações provenientes desse servidor proxy.

Acesso ao servidor proxy

Quando a instalação estiver concluída, aponte o navegador de cada usuário para um proxy do Edge Encryption usando o formato de URL:<host> `:`<port> .

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Os valores são determinados pelas propriedades de host e porta no arquivo `edgeencryption.properties`.

Como o exemplo com os seguintes valores:

Propriedade	Valor de exemplo
edgeencryption.proxy.host	hostname.mycompany.com
edgeencryption.proxy.http.port	8081

Um cliente acessará o servidor proxy usando o seguinte endereço: `http://hostname.mycompany.com:8081/`.

Nota: Configurações de DNS e regras de roteamento podem ser usadas. Os valores de host e porta são determinados pelo administrador da rede.

Solicitar o Edge Encryption

O plug-in do Edge Encryption (com.glide.edgeencryption) está disponível como uma assinatura separada.

Antes de Iniciar

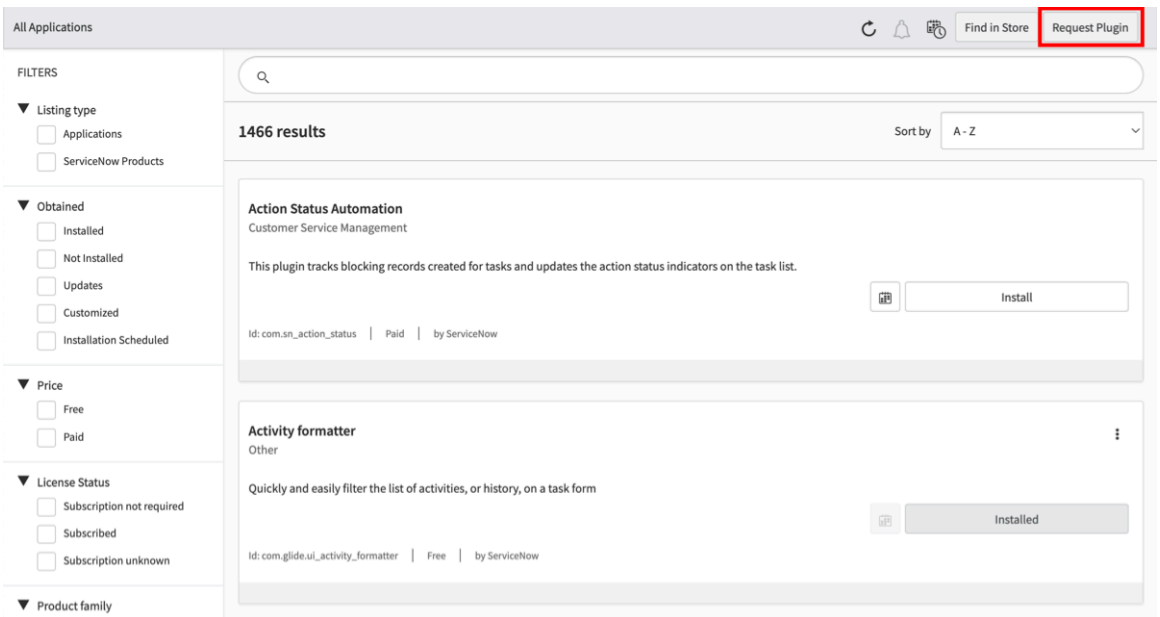
Para adquirir uma assinatura, entre em contato com o seu gerente de contas ServiceNow. O gerente de contas pode providenciar para que o plug-in seja ativado nas instâncias de produção e subprodução da sua organização, geralmente dentro de alguns dias.

Se você não tem um gerente de conta, se decidiu atrasar a ativação após a compra ou se quer avaliar o produto em uma instância de subprodução sem custos, siga estas etapas.

Função necessária: nenhuma

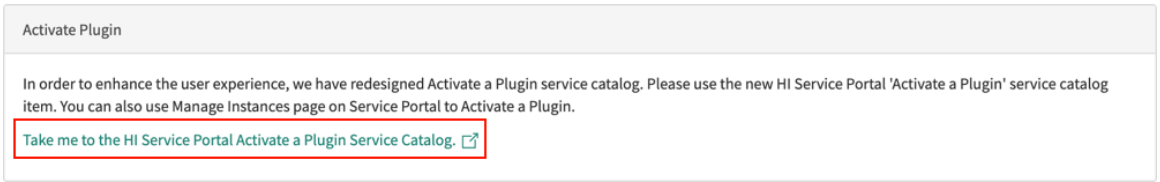
Procedimento

1. Navegue até **Todas** > **Aplicações do sistema** > **Todas os aplicações disponíveis** > **Todas**.
2. Na página Todas as Aplicações, selecione **Solicitar plug-in** para abrir o formulário **Ativar plug-in** em Now Support.



© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. No Now Support, selecione o link para acessar o Now Support Portal de serviços Catálogo de serviços.



4. Selecione sua instância.
5. Selecione **Ações > Ativar plug-in**.
6. No formulário **Ativar plug-in**, forneça as seguintes informações.

Formulário Ativar plug-in

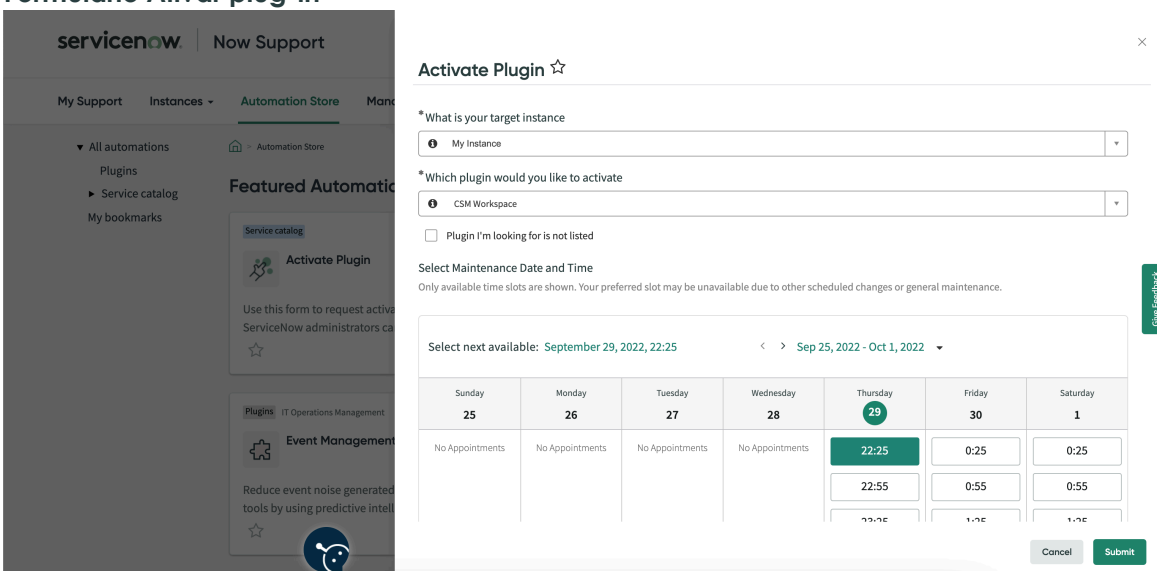
Campo	Descrição
Qual é a sua instância de destino	Instância na qual o plug-in será ativado.
Qual plug-in você deseja ativar	Nome do plug-in a ser ativado. **Nota:** Se o sistema não listar o plug-in desejado ou se você estiver ativando o plug-in em uma instância do OEM ou no local, marque a caixa de seleção O **plug-in que estou procurando não está listado** e insira o nome do plug-in.
Selecionar data e hora de manutenção	A data e a hora para ativar o plug-in. **Nota:** Os plug-ins são ativados em dois lotes, uma pela manhã e outra à noite, em todos os dias úteis no fuso horário do Pacífico dos EUA. Se o plug-in deve ser ativado em um momento específico, insira a solicitação no campo **Motivo/ Comentários**.

Example

Por exemplo, consulte o formulário a seguir para ativar o plug-in Espaço de trabalho CSM em uma instância chamada Minha instância.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formulário Ativar plug-in



7. Selecione **Enviar**.
   Para obter detalhes adicionais sobre como solicitar um plug-in, consulte Solicitar um plug-in no artigo do Catálogo de serviços [KB0751715] em Now Support Base de conhecimento.

Configurar uma conta de usuário do Edge Encryption

Os proxies do Edge Encryption se conectam à instância como um usuário para obter e atualizar informações de configuração de criptografia. Crie uma conta de usuário para essa finalidade e atribua a ele a função edge_encryption.

Antes de Iniciar

O plug-in do Edge Encryption deve ser instalado para que você possa atribuir a função.

Função necessária: administrador

Procedimento

1. Em sua instância do ServiceNow, crie uma conta de usuário a ser usada pelas aplicações de proxy do Edge Encryption.
2. Atribua a função edge_encryption ao usuário.

Baixar o servidor proxy do Edge Encryption

Baixe a aplicação do servidor proxy do Edge Encryption da sua instância e copie o arquivo para cada computador que executará o servidor proxy do Edge Encryption.

Antes de Iniciar

Antes de iniciar este procedimento, o plug-in do Edge Encryption deve ser instalado e ativado em sua instância.

Nota: O proxy do Edge Encryption só é oficialmente compatível com o Oracle JRE.

Função necessária: security_admin

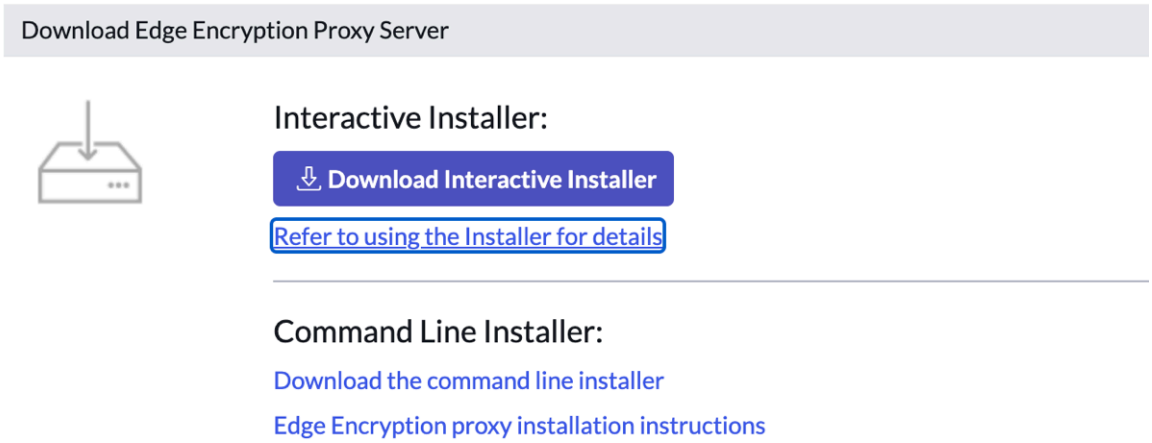
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

Procedimento

1. Navegue até **Todos** > **Configurações do Edge Encryption** > **Instalação e downloads** > **Downloads**.
2. Para usar o instalador interativo, clique em **Baixar instalador interativo**.

   Se estiver instalando o servidor proxy manualmente, selecione a versão do SO para seu servidor proxy.



   Nota: Como o servidor proxy requer pelo menos 4 GB de memória para ser executado, os JREs de 32 bits e os sistemas operacionais de 32 bits já não compatíveis a partir da versão Washington DC.

3. Copie o instalador em cada computador que executará o servidor proxy Edge Encryption.

   Nota: Se você estiver instalando o servidor proxy do Edge Encryption manualmente, copie o arquivo ZIP para cada computador que executará o servidor proxy do Edge Encryption.

O que Fazer Depois

Depois de baixar o instalador do Edge Encryption, Instalar o servidor proxy Edge Encryption usando o instalador interativo. Se estiver instalando manualmente, Instalar o servidor proxy do Edge Encryption usando o instalador de linha de comando.

Instalar o servidor proxy Edge Encryption usando o instalador interativo

Instale o servidor proxy do Edge Encryption em um computador Windows ou Linux usando o instalador interativo.

Antes de Iniciar

Nota: Os arquivos do repositório de chaves SafeNet KeySecure não são compatíveis com o instalador Edge Encryption. Para usar um repositório de chaves SafeNet KeySecure, Instalar o servidor proxy do Edge Encryption usando o instalador de linha de comando.

O plug-in do Edge Encryption deve ser instalado e ativado em sua instância antes de iniciar este procedimento. Certifique-se de o Java versão 11.0.6 ou mais recente esteja instalado na máquina que executa o instalador do Edge Encryption.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Função necessária:

- security_admin em sua instância do ServiceNow
- administrador local ou de domínio em um host do Windows
- usuário do serviço com acesso total ao sistema de arquivos em um host Linux

Por Que e Quando Desempenhar Esta Tarefa

Depois de instalar um novo servidor proxy, você pode executar o instalador novamente para realizar testes para detectar problemas com uma instalação ou modificar as configurações atuais. Suas opções incluem:

- **Instalar novo**: instale um novo servidor proxy.
- **Verificar instalação**: execute testes para detectar e corrigir problemas em uma instalação anterior.
- **Reinstalar existente**: execute testes para detectar e corrigir problemas em uma instalação anterior e exibir ou modificar as configurações existentes.

Nota: Se estiver instalando o servidor proxy em uma máquina Linux em uma porta privilegiada (porta 80 ou 443), você deverá executar o instalador como um usuário raiz com acesso total ao sistema de arquivos. Para restringir o acesso ao sistema de arquivos após a instalação do servidor proxy, use o recurso SetUID no instalador do proxy. Para habilitar este recurso, inicie o instalador como root ou sudo root. Quando solicitado pelo instalador, forneça o nome de usuário e o grupo de usuários de um usuário sem privilégios. O servidor proxy será instalado com os privilégios do sistema de arquivos do usuário fornecido. Você pode ignorar esta etapa para continuar a instalação padrão com privilégios raiz.

Procedimento

Use o instalador para instalar vários proxies para sua instância em várias máquinas, garantindo que os seguintes critérios se apliquem:

- Todos os proxies devem ter as mesmas chaves de criptografia e o mesmo par de chaves RSA usado para assinar digitalmente configurações e regras de criptografia.
- A chave de criptografia deve ser a chave padrão configurada na instância.
- Quando um banco de dados de proxy for configurado como parte da instalação, todos os proxies deverão usar o mesmo banco de dados de proxy.

  Talvez você precise de um banco de dados de proxy para criptografia de preservação de igualdade, criptografia de preservação de ordem ou tokenização. Se você não usar nenhum desses recursos, não será necessário um banco de dados de proxy.

O que Fazer Depois

Para usar o NVDA, um leitor de tela de Tecnologia de Assistência projetado para ler aplicações Java habilitadas para acessibilidade criadas para usuários de teclado, consulte Configurar um host Windows de 64 bits para usar NVDA de 32 bits com aplicações Java.

Depois de instalar o servidor proxy do Edge Encryption, defina o limite de memória inicial e o limite superior de memória do servidor proxy.

Instale o servidor proxy do Edge Encryption (instalador interativo)

Instale o proxy do Edge Encryption em um computador Windows ou Linux.

Antes de Iniciar

Função necessária: administrador

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

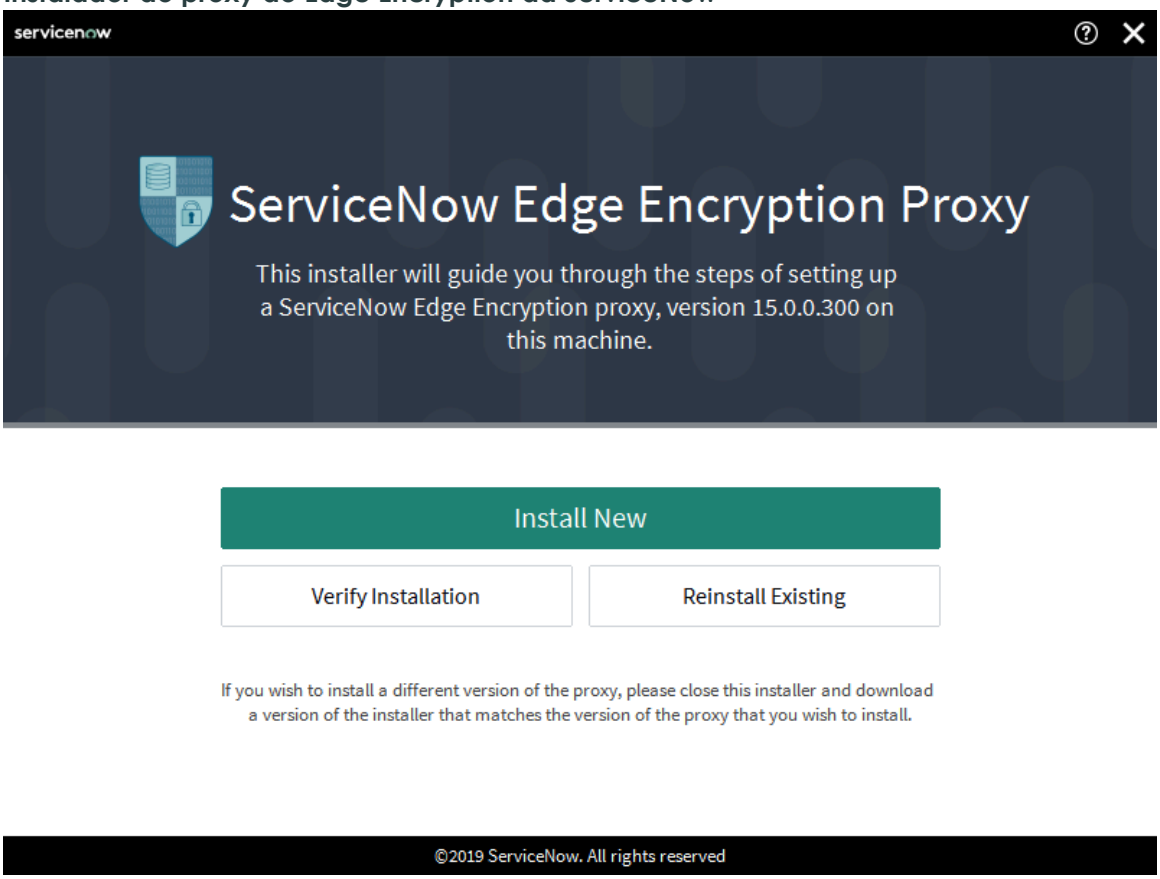
Procedimento

1. Baixe o instalador do servidor proxy do Edge Encryption.
2. Abra o instalador de proxy do Edge Encryption.

> **Nota:** Se a instalação for feita em uma máquina Windows, você deve executar o instalador como Administrador.

   a. Para executar o instalador como Administrador em uma máquina Windows, clique com o botão direito do mouse no Prompt de comando e selecione **Executar como administrador**.
   b. Na linha de comando, navegue até o diretório que contém o arquivo .jar baixado.
   c. Execute o seguinte comando: `java -jar<file name>.jar`.

Instalador do proxy do Edge Encryption da ServiceNow



3. Para instalar um novo servidor proxy, selecione**Instalar novo**.
   Se um proxy já estiver instalado, você poderá executar o instalador para:
   - **Verificar instalação**: execute testes para detectar e corrigir problemas em uma instalação anterior.
   - **Reinstalar existente**: execute testes para detectar e corrigir problemas em uma instalação anterior e exibir ou modificar as configurações existentes.
4. Configure o **Local de instalação** e a **instância de destino da ServiceNow**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Clique em **Procurar** para selecionar um local de instalação ou insira manualmente um caminho de instalação.

b. Insira o URL da instância de destino da ServiceNow.
Inclua o protocolo e o número da porta.

Example
`https://example.servicenow.com:443`

c. Insira o nome de usuário e a senha de um usuário com a função edge_encryption na instância de destino da ServiceNow.

5. Clique em **Avançar**.

6. Defina as **Configurações de conexão** e as **configurações de proxy**.

Configuração	Descrição
Host de Proxy	Nome de domínio totalmente qualificado da máquina na qual o servidor proxy está sendo instalado. **Nota:** Clique em **Detectar FQDN** para pesquisar o nome de domínio totalmente qualificado da máquina e preenchimento prévio do campo **Host do proxy**. Junto com a porta, essa propriedade define o URL usado pelo cliente para acessar o servidor proxy.
Porta HTTP	Porta no proxy para comunicação HTTP.
Porta HTTPS	Porta no proxy para comunicação HTTPS.
Nome do proxy	Nome do proxy e do serviço. O nome do proxy deve ser exclusivo.
Intervalo de pesquisa de proxy	Intervalo de pesquisa em segundos Com a configuração padrão, demora 5 segundos para o proxy aprender sobre as mudanças na configuração de criptografia. Valores maiores fazem com que a instância demore mais para detectar proxies que ficaram online. **Nota:** Alterar a configuração padrão do Intervalo de pesquisa de proxy pode resultar em atrasos na detecção de quando um proxy fica online.
Intervalo de manutenção de atividade do proxy	Tempo em segundos entre os pings emitidos pelo proxy para a instância. Os pings são emitidos periodicamente para

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configuração	Descrição
	verificar a conectividade entre o proxy e a instância. O valor padrão é 10. O valor mínimo é 5.

7. Clique em **Instalar**.
   O servidor proxy do Edge Encryption é instalado. A instalação pode demorar alguns minutos.

Configurar a proteção das propriedades do CyberArk

De forma opcional, configure a proteção das propriedades do CyberArk para armazenar com segurança senhas do Edge Encryption em um cofre digital centralizado e seguro.

Antes de Iniciar

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

Você deve comprar e configurar o CyberArk AIM (Application Identity Management) antes de configurar os parâmetros de conexão do CyberArk e as credenciais protegidas para um servidor proxy. Como parte da instalação do cliente AIM, o arquivo `JavaPasswordSDK.jar` é instalado no diretório de instalação do cliente AIM. O cofre da CyberArk é instalado em um servidor protegido independente e os clientes do AIM permitem acesso seguro a esse servidor.

Nota: Você deve instalar o cliente CyberArk AIM em cada computador host em que um proxy de borda está instalado.

No instalador do Edge, você deve especificar o local do arquivo `JavaPasswordSDK.jar` para configurar a conexão do CyberArk com o proxy do Edge. Você também deve inserir outros valores definidos durante a instalação do cliente do AIM.

A configuração do armazenamento de senha do CyberArk é opcional. Se não quiser configurar o armazenamento de senha do CyberArk, clique em **Ignorar** nas telas do CyberArk.

Procedimento

1. Na página Conexão do CyberArk do instalador Edge Encryption, insira os parâmetros de conexão do CyberArk.

Parâmetros de conexão do CyberArk

Configuração	Descrição
Caminho para PasswordSDK.jar	O caminho para o arquivo `JavaPasswordSDK.jar` instalado na máquina host do Windows durante a configuração do CyberArk.
ID de Aplicativo	O **ID do app** inserido durante a configuração do CyberArk.
Nome do cofre	O **Nome do cofre** do aplicativo inserido durante a configuração do CyberArk.

2. Clique em **Avançar**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Na página Credenciais protegidas do CyberArk do instalador, insira as credenciais a serem protegidas pelo CyberArk.
   - Para usar um único nome de credencial para todas as senhas protegidas, marque a caixa de seleção **Aplicar um nome de credencial a todas as credenciais**, insira o nome da credencial e clique em **Aplicar**.
   - Insira o nome da credencial para um ou mais campos a seguir. Nomes de credenciais são os nomes de usuário inseridos para as chaves SSH durante a configuração do CyberArk.

Credenciais protegidas do CyberArk

Configuração	Descrição
Usuário do Edge Encryption	O nome da credencial do CyberArk para um usuário do Edge Encryption.
Armazenamento de chaves da assinatura	O nome da credencial do CyberArk para o armazenamento de chaves da assinatura.
Armazenamento de chaves de certificado HTTPS	O nome da credencial do CyberArk para o armazenamento de chaves da certificação HTTPS.
Armazenamento das chaves da criptografia	O nome da credencial do CyberArk para o armazenamento de chaves da criptografia.
Banco de dados	O nome da credencial do CyberArk para o armazenamento de chaves do banco de dados.
Armazenamento de chaves do certificado HTTPS da SafeNet	O nome da credencial do CyberArk para o armazenamento de chaves da certificação HTTPS da SafeNet.
Servidor SafeNet	O nome da credencial do CyberArk para o servidor SafeNet.
Encaminhar proxy	O nome da credencial do CyberArk para encaminhamento de proxy.

4. Clique em **Avançar**.

Configurar a chave de assinatura

Configure a chave de assinatura depois de instalar o servidor proxy por meio do instalador de proxy do Edge Encryption.

Antes de Iniciar
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa
A chave de assinatura sinaliza mudanças para configurações e propriedades feitas pelo servidor proxy. A chave de assinatura deve ser um par de chaves RSA assimétrico em um JCEKS KeyStore.

Nota: Se estiver instalando vários proxies, cada proxy deve usar a mesma chave de assinatura.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Na página Chave de assinatura do instalador do Edge Encryption, selecione o repositório de chaves na máquina host para armazenar a chave de assinatura.
   - **Criar novo Java KeyStore**: insira o local do diretório, o nome e a senha do novo repositório de chaves.
   - **Usar repositório de chaves existente**: insira o local do arquivo de repositório de chaves e a senha.
2. Clique em **Avançar**.
3. Selecione ou crie uma chave de assinatura.
   - **Nova chave**: crie uma chave de assinatura para este proxy.
   - **Usar chave existente**: use um par de chaves RSA do repositório de chaves selecionado.
   - **Importar chave existente**: importe um par de chaves RSA de um repositório de chaves diferente. Navegue até o arquivo de repositório de chaves, insira a senha do repositório de chaves e selecione o alias da chave. Forneça um novo alias para a chave.
4. Clique em **Avançar**.

Configurar o certificado HTTPS

Para permitir que os clientes se conectem ao servidor proxy do Edge Encryption usando uma conexão SSL segura, importe o certificado HTTPS para o servidor proxy.

Antes de Iniciar
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa
O proxy do Edge Encryption fornece o certificado HTTPS para clientes que tentam se conectar.

Procedimento

1. Na página Certificado HTTPS do instalador do Edge Encryption , selecione o repositório de chaves para armazenar o certificado.
   - **Criar novo Java KeyStore**: insira o local do diretório, o nome e a senha do novo repositório de chaves.
   - **Usar repositório de chaves existente**: insira o local do arquivo de repositório de chaves e a senha.
2. Clique em **Avançar**.
3. Selecione ou importe um certificado.
   O alias da chave é o alias fornecido para o certificado.
   - **Usar certificado existente**: use um certificado existente no repositório de chaves selecionado.
   - **Importar de arquivo ou do KeyStore**: importe um certificado de um repositório de chaves diferente ou de um arquivo .cer. Navegue até o arquivo de repositório de chaves ou até o arquivo .cer, insira a senha e selecione o alias. Você deve fornecer um novo alias para o certificado.
4. Clique em **Avançar**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configure a chave de criptografia AES de 128 bits

Depois de configurar o certificado HTTPS por meio do instalador de proxy do Edge Encryption, configure a chave de criptografia AES de 128 bits para criptografar seus dados.

Antes de Iniciar

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

A chave de criptografia é um arquivo de texto sem formatação dentro do diretório `/chaves` ou uma chave secreta dentro de um repositório de chaves. Se estiver utilizando um repositório de chaves para suas chaves de criptografia AES de 128 bits e AES de 256 bits, elas deverão usar o mesmo repositório de chaves.

Se estiver atualizando um certificado SSL em um servidor proxy do Edge, consulte Atualizar certificado SSL.

Procedimento

1. Selecione o local da chave de criptografia.

Opção	Descrição
Repositório de arquivo	Use um arquivo para armazenar uma única chave de criptografia. Você pode usar um arquivo existente no diretório `/chaves` ou pode gerar um novo arquivo. Para gerar um novo arquivo, insira um alias e clique em **Gerar**. Será criado um arquivo que contém uma chave de criptografia. **Nota:** Essa opção designa o local de armazenamento e a chave de criptografia. Se selecionar **Repositório de arquivo**, clique em **Avançar** e vá para a etapa 5.
Criar novo Java KeyStore	Crie um repositório de chaves para armazenar a chave de criptografia.
Arquivo Java KeyStore	Armazene a chave de criptografia em um arquivo Java KeyStore.

2. Clique em **Avançar**.

3. Selecione ou crie a chave de criptografia.

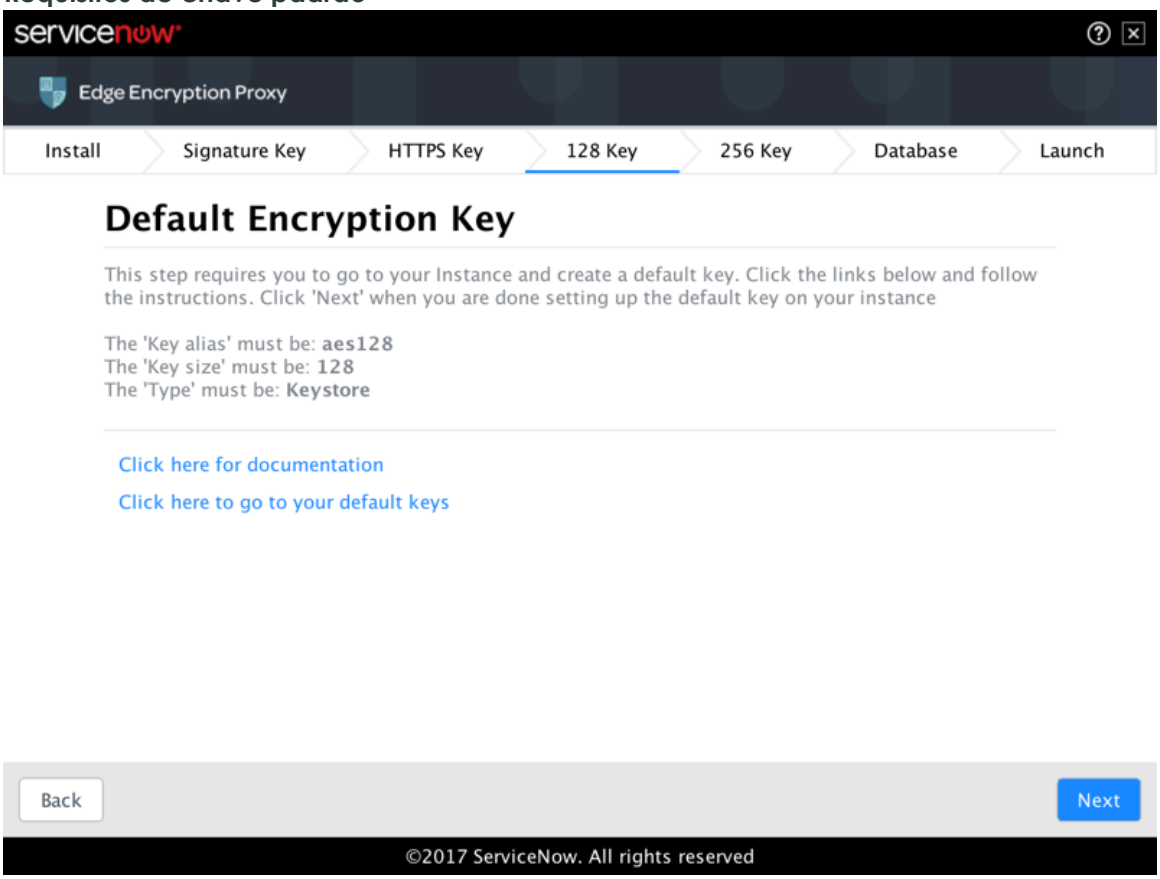
Opção	Descrição
Nova chave	Crie uma chave de criptografia e um alias. **Nota:** O nome do alias (nome da chave, alias de chave) deve conter letras minúsculas e números de acordo com os requisitos do Java KeyStore. Para saber mais sobre o utilitário keytool, consulte a documentação do Java

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
Usar chave existente	Use uma chave de criptografia existente no repositório de chaves selecionado.
Importar chave existente	Importe uma chave de criptografia de um repositório de chaves diferente.

4. Clique em **Avançar**.
5. Configure a chave na instância de acordo com os requisitos definidos no seu instalador. Para configurar a chave na instância, navegue até a instância e defina uma chave padrão. Consulte Configurar chaves de criptografia na instância. Certifique-se de que o alias, o tamanho e o tipo da chave correspondam aos requisitos definidos no instalador.

Requisitos de chave padrão



6. Depois que a chave estiver configurada na instância, retorne ao instalador e clique em **Avançar**.

Configurar a chave de criptografia AES de 256 bits

Depois de configurar a chave AES de 128 bits por meio do instalador de proxy do Edge, é possível configurar opcionalmente a chave de criptografia AES de 256 bits para criptografar seus dados.

Antes de Iniciar

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

A chave de criptografia é um arquivo de texto sem formatação dentro do diretório `/chaves` ou uma chave secreta dentro de um repositório de chaves. Caso use um repositório de

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

chaves para suas chaves de criptografia AES de 128 bits e AES de 256 bits, ambas as chaves deverão usar o mesmo repositório de chaves. Se não desejar configurar uma chave de criptografia AES de 256 bits, selecione **Ignorar** para continuar instalando o servidor proxy.

Se estiver atualizando um certificado SSL em um servidor proxy do Edge, consulte Atualizar certificado SSL.

Procedimento

1. Selecione o local da chave de criptografia.

Opção	Descrição
Repositório de arquivo	Use um arquivo para armazenar uma única chave de criptografia. Você pode usar um arquivo existente no diretório `/chaves` ou pode gerar um novo arquivo. Para gerar um novo arquivo, insira um alias e selecione **Gerar**. Será criado um arquivo que contém uma chave de criptografia. **Nota:** Essa opção designa o local de armazenamento e a chave de criptografia. Se selecionar **Repositório de arquivo**, selecione **Avançar** e vá para a etapa 5.
Criar novo Java KeyStore	Crie um repositório de chaves para armazenar a chave de criptografia.
Arquivo Java KeyStore	Armazene a chave de criptografia em um arquivo Java KeyStore.

2. Selecione **Avançar**.

3. Selecione ou crie a chave de criptografia.

Opção	Descrição
Nova chave	Crie uma chave de criptografia e um alias. **Nota:** O nome do alias (nome da chave, alias de chave) deve conter letras minúsculas e números de acordo com os requisitos do Java KeyStore. Para saber mais sobre o utilitário keytool, consulte a documentação do Java
Usar chave existente	Use uma chave de criptografia existente no repositório de chaves selecionado.
Importar chave existente	Importe uma chave de criptografia de um repositório de chaves diferente.

4. Selecione **Avançar**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Opcional: Se quiser usar a criptografia AES de 256 bits, consulte Configurar a chave de criptografia AES de 256 bits.
6. Para usar a criptografia AES de 256 bits, você também deve configurar a chave de criptografia padrão do AES de 256 bits na instância.

   Para fazer isso, navegue até a instância e defina uma chave padrão. Consulte Configurar chaves de criptografia na instância. Certifique-se de que o alias, o tamanho e o tipo da chave correspondam aos requisitos definidos no instalador.
7. Após a configuração da chave na instância, retorne ao instalador e selecione **Avançar**.

Atualizar certificado SSL

Ao atualizar um certificado SSL em um servidor proxy do Edge, você deve excluir o antigo.

Antes de Iniciar
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa
Ao atualizar um certificado SSL em um servidor proxy do Edge, você deve também excluir o certificado antigo. Caso contrário, o certificado antigo (na forma de um alias no arquivo do KeyStore) continuará a ser usado mesmo que o servidor proxy do Edge esteja configurado para usar o novo certificado.

Procedimento

1. No servidor proxy do Edge, liste as entradas no Java KeyStore:

```
keytool -list -keystore keystore.jceks -storetype jceks -storepass
 MY_SUPER_PASSWORD
```

2. Remova o certificado SSL antigo:

```
keytool -delete -alias MY_OLD_ALIAS -keystore keystore.jceks -storetype
 jceks -storepass MY_SUPER_PASSWORD
```

3. Adicione o novo certificado SSL ao Java KeyStore.

Configurar o banco de dados do proxy do Edge Encryption

Se estiver usando tipos de criptografia que preservam a ordem ou padrões de criptografia, você pode configurar opcionalmente as propriedades do banco de dados do proxy do EdgeEdge Encryption.

Antes de Iniciar
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa
Para usar tipos de criptografia que preservam a ordem ou padrões de criptografia é obrigatório ter um banco de dados MySQL em execução na rede Essa tarefa conecta o proxy ao banco de dados, mas não instala ou configura o banco de dados.

Nota: Se estiver usando vários servidores proxy, todos os servidores proxy devem usar o mesmo banco de dados de proxy. Os valores inseridos no instalador devem ser os mesmos para todos os servidores proxy.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Confirme ou mude o URL do banco de dados, que é o local do banco de dados do proxy.
2. No campo **Nome**, insira o nome do banco de dados do proxy.
   O valor padrão é *edgeencryption*.
3. Insira o nome de usuário e a senha para acessar o banco de dados do proxy.
4. Clique em **Avançar**.

Inicializar o servidor proxy do Edge Encryption

Depois da instalação e configuração do proxy do Edge Encryption você pode iniciar o proxy a partir do instalador.

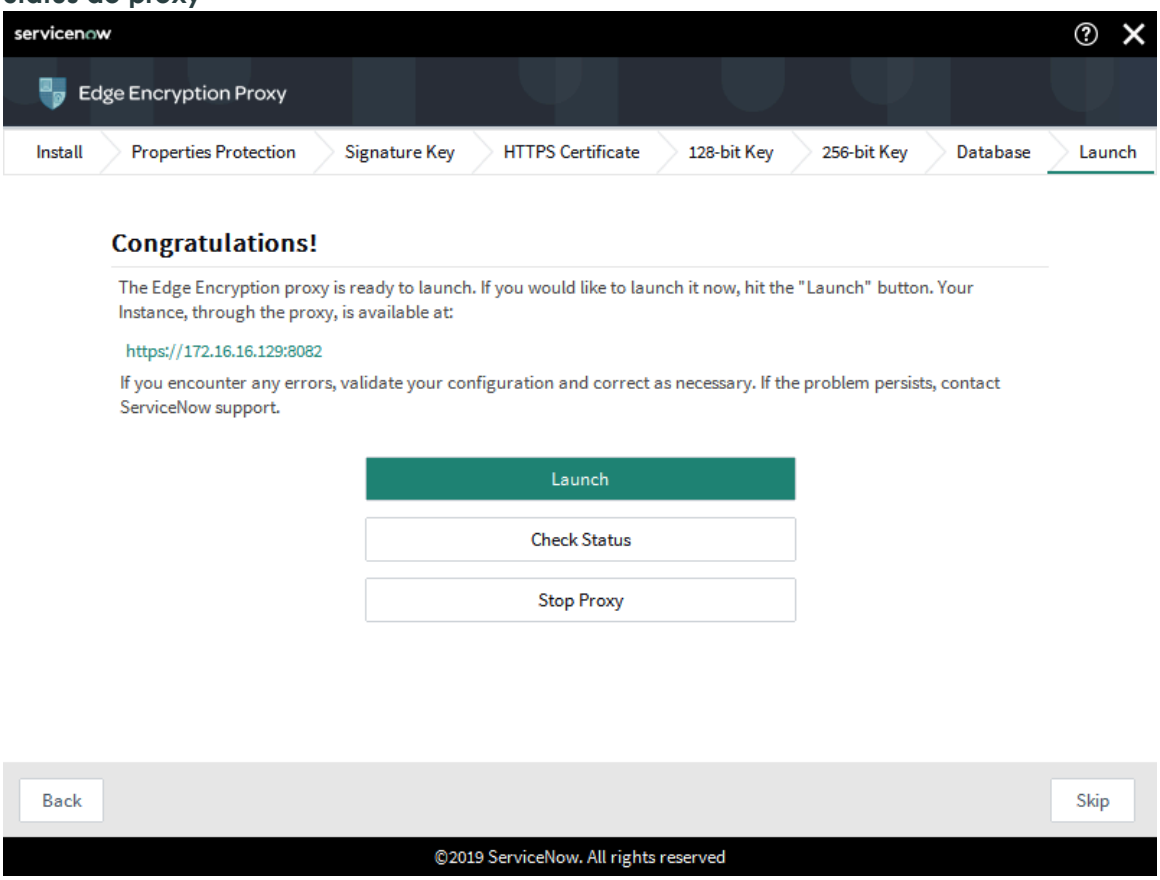
Antes de Iniciar

Função necessária: administrador

Procedimento

1. Depois de configurar as chaves na instância e o banco de dados do proxy, retorne ao instalador do proxy do Edge Encryption e clique em **Iniciar**.
2. Se um problema for detectado, ou para verificar o status do seu servidor proxy, clique em **Verificar status** para verificar se o proxy está sendo executado.
   Uma mensagem exibirá o status do proxy.

Status do proxy



O que Fazer Depois

Depois de instalar com sucesso o servidor proxy do Edge Encryption, Definir o limite de memória inicial e o limite superior de memória do servidor proxy.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Verificar e solucionar problemas de instalação do servidor proxy do Edge Encryption

Depois da instalação do o proxy Edge Encryption, você poderá verificá-la para localizar problemas ou iniciar e parar o proxy.

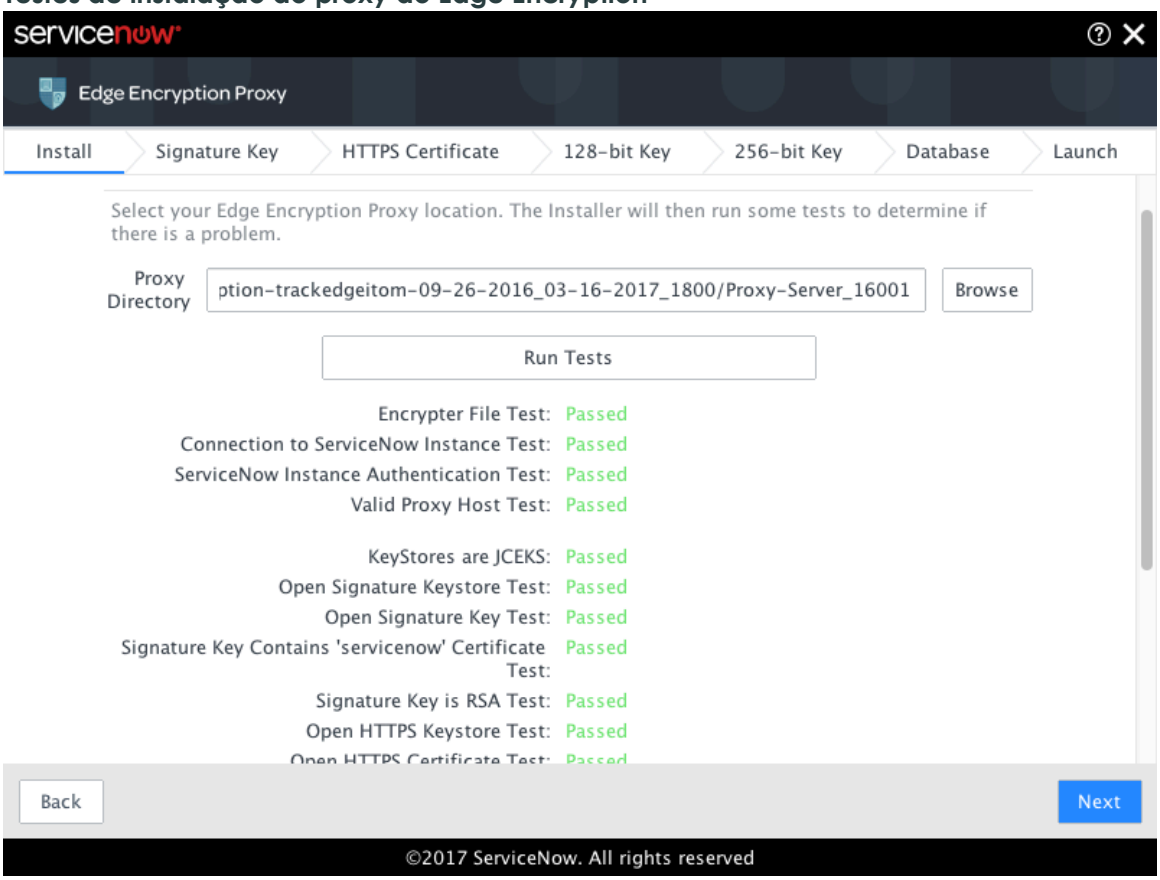
Antes de Iniciar

Função necessária: administrador

Procedimento

1. Abra o instalador de proxy do Edge Encryption.
2. Selecione **Verificar instalação**.
3. Clique em **Diretório de proxy** e selecione o diretório do proxy.
4. Clique em **Executar testes**.
   Os resultados do teste serão exibidos.

Testes de instalação do proxy do Edge Encryption



5. Clique em **Avançar**.
   Se for encontrado um problema, você poderá percorrer o instalador para corrigir a configuração. Se nenhum problema for encontrado, o instalador irá para a página **Inicializar**. Você pode verificar o status do proxy, interromper o proxy ou iniciar o proxy na página **Inicializar**.

Instalar o servidor proxy do Edge Encryption usando o instalador de linha de comando

Instale manualmente vários servidores proxy do Edge Encryption em sua rede.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Funções necessárias: security_admin em sua instância da ServiceNow e administrador local na máquina host.

Se foram usados tipos de criptografia de preservação ou padrões de criptografia, configure um banco de dados MySQL em uma máquina na sua rede, caso ainda não exista.

Nota: Se estiver usando chaves de criptografia da Unbound Technology com Edge Encryption, instale o servidor proxy usando o instalador de linha de comando na máquina cliente Unbound. O servidor proxy Edge Encryption deve ser executado na mesma máquina que o cliente da Unbound Technology.

Por Que e Quando Desempenhar Esta Tarefa
Primeiro, configure um único servidor proxy do Edge Encryption. Depois que o primeiro servidor proxy for executado com sucesso, adicione servidores proxy adicionais para uma instância para garantir um ambiente ideal. Consulte Dimensionando seu ambiente do Edge Encryption para determinar o número de servidores proxy adicionais necessários.

Instalar o servidor proxy do Edge Encryption (instalador de linha de comando)

Instale o proxy do Edge Encryption em um computador Windows ou Linux de 64 bits.

Antes de Iniciar
Função necessária: admin

O Java versão 11.0.6 ou posterior na série de versões 11.x é necessário para executar o instalador.

Por Que e Quando Desempenhar Esta Tarefa
Instale o servidor proxy do Edge Encryption em uma máquina na sua rede usando o comando apropriado da sua máquina de destino. Se estiver instalando o servidor proxy do Edge Encryption em uma máquina Windows, deverá instalar adicionalmente o servidor proxy como um serviço do Windows.

Quando você atualiza o servidor proxy do Edge Encryption, o sistema faz backup do proxy antigo no diretório `backup.dist-upgrade-<timestamp>` sob o diretório de instalação atual. O diretório de backup é gerado durante o processo de upgrade e armazena as informações do proxy antigo.

Quando você executa uma atualização por meio da linha de comando, um dist-upgrade.log pode ser gerado no diretório em que o comando é executado. O dist-upgrade.log contém logs do processo de atualização.

Em caso de falha na atualização, o sistema cria um diretório `fail-backup.dist-upgrade-<timestamp>` . Além disso, `logs/wrapper.log` no diretório de proxy original também pode conter informações de falha.

Procedimento

1. Crie o diretório de instalação
2. Baixe o arquivo do proxy do Edge Encryption para o diretório de instalação.
3. Abra o terminal e mude para o diretório de instalação.

Nota: Se a instalação ocorrer em uma máquina Windows, você deve iniciar o Prompt de comando do Windows com privilégios de administrador.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Execute este comando na máquina de destino e mude as variáveis de acordo com sua configuração: `java-jar edgeencryption-<version> -all.jar -m install -n<ProxyName> --instancehost<host> -p<InstancePort> --protocol https`

Opção	Variável	Descrição
nenhum	versão	Número da versão do proxy do Edge Encryption que está sendo usado para executar a operação atual.
-m	Modo	A operação ou o modo a ser executado (install ou dist-upgrade).
-n	ProxyName	O nome da instância do proxy de criptografia. Use um `ProxyName` exclusivo para poder identificar instâncias de proxy específicas.
--instancehost	Host	O nome do host da sua instância da ServiceNow (por exemplo, `mycompany.service-now.com`).
-p	InstancePort	A porta da sua instância. Quando o protocolo é https, a porta normalmente é 443.
--protocol	protocolo	O protocolo usado para acessar sua instância da ServiceNow (normalmente https).

Nota: Não copie e cole comandos do navegador. Ocasionalmente, as operações de copiar/colar fazem com que caracteres inesperados sejam colados na máquina de destino e resultem na execução incorreta do comando. É melhor digitar o comando manualmente usando a documentação como referência.

Para ver a tela de ajuda, execute este comando sem argumentos: `java -jar edgeencryption-<version> -all.jar`

5. Se a instalação for feita em uma máquina Windows, instale o proxy do Edge Encryption como um serviço do Windows.

   a. Opcional: Mude o nome do serviço abrindo o arquivo `conf/wrapper.conf` no novo proxy e definindo as propriedades na tabela a seguir.

Propriedade	Descrição
wrapper.ntservice.name	Nome exclusivo do serviço de proxy do Edge Encryption.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Propriedade	Descrição
wrapper.ntservice.displayname	Edge Encryption: o nome de exibição do serviço de proxy.
wrapper.ntservice.description (opcional)	Descrição do servidor proxy.

Se esta etapa não for executada, o serviço de proxy do Edge Encryption será instalado com o nome de **Edge Encryption**.

b. Salve e feche o arquivo.

c. Abra o Prompt de comando do Windows e faça `cd` para `ServerName_port /bin`.

d. Execute o`edgeencryption.bat install`.

Resultados
O diretório `ProxyName_port` será criado no diretório atual. O arquivo `edgeencryption.properties` será atualizado com os valores de host, porta e protocolo da linha de comando.

Criar e configurar o par de chaves RSA para a assinatura digital

Crie um par de chaves RSA que o servidor proxy pode usar para criar a assinatura digital para assinar mudanças nas propriedades de criptografia e na configuração.

Antes de Iniciar
Função necessária: administrador

Para gerar e validar a assinatura digital, um par de chaves RSA deve ser gerado e armazenado no JCEKS Java KeyStore e cada proxy deve ser configurado para usar este par de chaves. Gere um par de chaves de criptografia usando o comando keytool.

Para usar o utilitário keytool com um proxy instalado no SElinux (CentOS), você deve habilitar o carregamento de bibliotecas compartilhadas do diretório de instalação do proxy java. Para fazer isso, execute o seguinte comando como raiz.

```
chcon -R -t texrel_shlib_t proxy_install_dir/java/jre /lib
```

Você deve usar a versão Java 1.8 do utilitário keytool. Uma cópia do utilitário pode ser encontrada em `<proxy install dir>java/jre/bin/keytool`.

Procedimento

1. Mude para o diretório do KeyStore no diretório de download do proxy.

2. Mude a senha padrão.

A senha padrão é *changeme*.

```
keytool -keystore keystore.jceks -storetype jceks -storepasswd -new
 <newpassword>
```

3. Crie um par de chaves de criptografia.

Nota: Não insira uma senha para a chave quando o utilitário keytool solicitar uma.

Insira este comando em uma única linha.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

```
keytool -genkeypair -alias <key alias> -keyalg rsa -keystore
 keystore.jceks
-storetype jceks -storepass <keystore password> -keysize 2048
```

4. Atualize o arquivo de propriedade do proxy de criptografia (`edgeencryption.properties`).

   a. Mude para o diretório `<installation directory>/conf/`.

   b. Abra o arquivo `edgeencryption.properties`.

   c. Insira as propriedades da assinatura digital.

      Essas propriedades devem ser as mesmas para todos os proxies.

5. Salve e feche o arquivo `edgeencryption.properties`.

Importar e configurar o certificado de conexão SSL segura

Para usar uma conexão SSL segura, importe um certificado do servidor e adicione-o ao Java KeyStore.

Antes de Iniciar

Função necessária: administrador

Você deve obter o certificado do servidor e a chave privada correspondente antes de adicioná-lo ao Java KeyStore.

Procedimento

1. Gere uma solicitação de assinatura de certificado (CSR) usando o comando `openssl`.

```
openssl req -newkey rsa:2048 -keyout PRIVATEKEY.key -out MYCSR.csr
```

2. Envie seu CSR (MYCSR.csr no exemplo acima) para sua autoridade de certificação para que ele seja assinado.
3. Crie um repositório de chaves P12 para importação usando o comando `openssl`.

```
openssl pkcs12 -export -in MYSIGNEDCERT.pem -inkey PRIVATEKEY.key -name
 shared > MY_SERVER.p12
```

4. Armazene seu certificado e chave privada em um arquivo jceks.

```
keytool -importkeystore -destkeystore keystore.jceks -deststoretype
 jceks -srckeystore MY_SERVER.p12 -srcstoretype pkcs12 -alias MYALIAS
```

   O alias, mostrado no exemplo como `MYALIAS`, pode ser qualquer valor. Você usará este alias na propriedade `edgeencryption.proxy.https.cert.alias` no arquivo `edgeencryption.properties` localizado na pasta `<installation directory>/conf/`.

5. Pare e reinicie o proxy do Edge.

   Nota: Durante uma reinicialização, o servidor proxy fica off-line por um curto período de tempo. A duração é determinada pelo seu ambiente e quanto tempo leva para parar e reiniciar o serviço de proxy.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configure o repositório de chaves e as chaves de criptografia.

Configure o repositório de chaves e as chaves de criptografia usadas pelo servidor proxy do Edge Encryption.

Antes de Iniciar

Função necessária: security_admin

Procedimento

1. Determine com cuidado o tipo apropriado de repositório de chaves a ser usado com base nas necessidades da sua organização.

Repositório de chave compatível	Descrição
Repositório de arquivo	As chaves são armazenadas em um arquivo em um sistema de arquivos acessado pelo servidor proxy do Edge Encryption. Como as chaves de criptografia armazenadas em um arquivo não são criptografadas, é sua responsabilidade proteger esses arquivos.
Java KeyStore	Um Java KeyStore: ◦ Armazena chaves em um Java JCEKS KeyStore. ◦ É protegido por senha e mais seguro do que armazenar chaves em um arquivo no sistema de arquivos. ◦ Pode armazenar várias chaves. Um alias de chave representa cada chave, facilitando o gerenciamento de várias chaves. O proxy do Edge Encryption é fornecido com o arquivo do Java JCEKS KeyStore chamado `keystore.jceks` no diretório do `repositório de chaves`. Este arquivo do repositório de chaves contém a chave pública da ServiceNow usada para validar regras de criptografia assinadas pela ServiceNow.
Enterprise Key Management (EKM)	**SafeNet KeySecure** As chaves são armazenadas e recuperadas com os sistemas de gerenciamento de chaves SafeNet KeySecure. Você deve garantir uma licença com a Gemalto, baixar as bibliotecas e instalar o SafeNet KeySecure em uma máquina host em sua rede antes de configurar o repositório de chaves no servidor proxy do Edge Encryption. **Tecnologia não associada** A chave de criptografia encapsulada codificada em base64 é armazenada como arquivo de texto no servidor proxy Edge Encryption. A implementação da Unbound Technology (antiga Dyadic Security) mantém o controle da chave encapsulada. O servidor proxy do Edge Encryption deve ser executado na mesma máquina que o cliente da tecnologia não associada.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Se estiver usando um repositório de chaves diferente do sistema de base Java JCEKS KeyStore, você deverá importar a chave pública da ServiceNow para o repositório de chaves. O alias da chave pública é *servicenow*.

2. Configure o repositório de chaves e as chave de criptografia na sua rede local.

Configurar um repositório de chaves no Java KeyStore

Você pode usar um Java KeyStore para armazenar chaves de criptografia.

Antes de Iniciar
Função necessária: administrador

Você deve usar a versão Java 1.8 do utilitário keytool. Uma cópia do utilitário pode ser encontrada em `<proxy install dir>/java/jre/bin/keytool`.

Por Que e Quando Desempenhar Esta Tarefa
O proxy do Edge Encryption é fornecido com o arquivo do Java JCEKS KeyStore chamado `keystore.jceks` no diretório do `repositório de chaves`. Este arquivo do repositório de chaves contém a chave pública da ServiceNow usada para validar regras de criptografia assinadas pela ServiceNow.

Procedimento

1. Configure as propriedades do repositório de chaves.
   a. Mude para o diretório `<installation directory>/conf/`.
   b. Abra o arquivo `edgeencryption.properties`.
   c. Insira as propriedades do Java KeyStore.
2. Salve e feche o arquivo `edgeencryption.properties`.

O que Fazer Depois
Depois de configurar o Java KeyStore, Criar chaves de criptografia usando a ferramenta Java KeyStore.

Criar chaves de criptografia usando a ferramenta Java KeyStore

Você pode usar a ferramenta de chave fornecida com a distribuição do proxy de criptografia para criar chaves de criptografia AES de 128 bits e AES de 256 bits.

Antes de Iniciar
Função necessária: administrador

Você deve usar a versão Java 1.8 do utilitário keytool. Uma cópia do utilitário pode ser encontrada em `<proxy install dir>/java/jre/bin/keytool`.

Para saber mais sobre o utilitário keytool, consulte a documentação do Java SE.

Por Que e Quando Desempenhar Esta Tarefa
Nota: A Java KeyStore requer que nome do alias (nome da chave, alias de chave) contenha letras minúsculas e números.

Procedimento

1. Mude para o diretório `<installation directory>/keystore/`.
2. Para criar a chave de criptografia, execute um dos comandos a seguir.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Se optar por executar esses comandos a partir um diretório diferente do diretório de repositório de chaves (ou seja, a etapa anterior foi ignorada), deve alterar a opção *-keystore* para incluir o caminho do diretório atual para o diretório de repositório de chaves. Por exemplo, se você estava no `<installation directory>\bin`, a opção seria `-keystore ../keystore/keystore.jceks`.

Opção	Descrição
AES 128	`keytool -genseckey -alias 128bitkey -keyalg aes -keysize 128 -keystore keystore.jceks -storetype jceks`
AES 256	`keytool -genseckey -alias 256bitkey -keyalg aes -keysize 256 -keystore keystore.jceks -storetype jceks`

Adicione o alias à instância ao atribuir chaves padrão.

Nota: A senha da chave deve ser igual à senha do repositório de chaves.

Configurar um repositório de chaves SafeNet KeySecure

Se estiver usando um repositório de chaves SafeNet, copie um conjunto de bibliotecas para o diretório de distribuição do proxy.

Antes de Iniciar

Função necessária: administrador

Você deve instalar e configurar o repositório de chaves da SafeNet antes de executar esta etapa. Garanta uma licença com a Thales para baixar as bibliotecas.

Nota: Para o IngrianNAE versão 8.12, você também deve baixar o arquivo `commons-collections.jar`

Por Que e Quando Desempenhar Esta Tarefa

Nota: No Linux, os caminhos de arquivo usam uma barra (/).

Procedimento

1. Mude para o diretório `<installation directory>/conf/` e abra o arquivo `edgeencryption.properties`.
2. Insira as propriedades do repositório de chaves da SafeNet.

Nota: Você pode configurar o repositório de chaves da SafeNet usando autenticação de nome de usuário/senha ou autenticação de certificado de cliente, mas não uma combinação dos dois.

Example

Exemplo de repositório de chaves da SafeNet usando autenticação de nome de usuário e senha.

```
edgeencryption.nae.retries = 3
edgeencryption.nae.enabled = true
edgeencryption.nae.server = url
edgeencryption.nae.port = 9000
edgeencryption.nae.protocol = ssl
```

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

```
edgeencryption.nae.keystore.path = keystore/safenet_truststore
edgeencryption.nae.keystore.password = password
edgeencryption.nae.user = safenet_user
edgeencryption.nae.password = safenet_password
```

Example

Exemplo de repositório de chaves da SafeNet usando autenticação de cerificado do cliente Esse método de autenticação elimina a necessidade de armazenar o nome de usuário e a senha do servidor SafeNet no arquivo de propriedades.

```
edgeencryption.nae.retries = 3
edgeencryption.nae.enabled = true
edgeencryption.nae.server = url
edgeencryption.nae.port = 9000
edgeencryption.nae.protocol = ssl
edgeencryption.nae.keystore.path = keystore/safenet_clientcert
edgeencryption.nae.keystore.password = password
edgeencryption.nae.client.certificate = cert_name
```

3. Adicione ou crie uma chave no repositório de chaves da SafeNet.
   Adicione o nome da chave (alias) à instância ao atribuir chaves padrão.
4. Salve e feche o arquivo `edgeencryption.properties`.

Upgrade de Kingston ou inferior para London ou superior

Se você usar um servidor SafeNet NAE para armazenamento de chaves com o Edge, antes de atualizar o proxy do Kingston ou inferior para o London ou superior, será necessário copiar os arquivos de cliente ProtectApp JAR do SafeNet da Gemalto e adicionar novas propriedades.

Antes de Iniciar

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

Nota: No Linux, os caminhos de arquivo usam uma barra (/).

Procedimento

1. Copie os seguintes arquivos de `<installation directory>/lib` para `<installation directory>/nae directory`:

   - `commons-collections<version>.jar`
   - `ingrianlog4j-api-<version>.jar`
   - `ingrianlog4j-core-<version>.jar`
   - `ingrianNAE-<version>.jar`

2. Na versão atual (sem upgrade) do proxy, atualize o arquivo `<installation directory>/conf/edgeencryption.properties` adicionando as duas propriedades a seguir:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- *edgeencryption.ekm.provider.classname* = com.snc.edgeencryption.encryption.CloudEdgeNaeKeyProvider
- *edgeencryption.thirdparty.vendor.library.path* = <directory path to the directory where you copied the jar files in step 1>

Nota: *edgeencryption.thirdparty.vendor.library.path* para Java 11.

3. Salve as mudanças.
4. Prossiga com o upgrade para o London ou superior.

Configurar chaves de tecnologia não associada

Use as chaves de Tecnologia não associada (anteriormente Segurança Diádica) com o Edge Encryption, armazenando a chave de criptografia encapsulada codificada em base64 como arquivo de texto no servidor proxy do Edge Encryption e fornecendo o alias da chave de encapsulamento. A implementação da tecnologia não associada mantém o controle da chave de encapsulamento.

Antes de Iniciar

Função necessária: security_admin

Em sua implementação de tecnologia não associada, identifique a chave de encapsulamento e a chave encapsulada. Use o algoritmo RSA/ECB/OAEPWITHSHA-256ANDMGF1PADDING para encapsulamento e preenchimento. Exporte a chave encapsulada no formato de texto codificado em base64. Salve o arquivo usando o alias da chave como o nome sem extensão de arquivo.

Nota: Se estiver usando chaves de criptografia da Unbound Technology com Edge Encryption, instale o servidor proxy usando o instalador de linha de comando na máquina cliente Unbound. O servidor proxy Edge Encryption deve ser executado na mesma máquina que o cliente da Unbound Technology.

Procedimento

1. Adicione a chave de criptografia encapsulada no formato de texto codificado em base64 ao diretório `<proxy-installation-directory>/keys`.
   O nome do arquivo deve ser o alias da chave sem nenhuma extensão de arquivo.
2. Atualize o arquivo `edgeencryption.properties`.
   a. Mude para o diretório `<proxy-installation-directory>/conf`.
   b. Abra o arquivo `edgeencryption.properties`.
   c. Insira as propriedades do repositório de arquivos e defina o valor de *edgeencryption.keyfile.directory* como `chaves`.

      Essa propriedade instrui o servidor proxy a procurar a chave de criptografia no diretório do `<Java-home-directory>/keys`.

      Para obter mais informações sobre propriedades do Edge Encryption, consulte Propriedades do servidor proxy do Edge Encryption.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

d. Remova o comentário das propriedades da configuração do provedor Diádica e defina o valor de *edgeencryption.ekm.provider.rsa.wrapping.key.alias* como o alias da chave de encapsulamento em sua implementação não associada.

e. Salve e feche o arquivo.

O que Fazer Depois

Adicione o alias da chave de criptografia à instância. O alias da chave de criptografia é o nome do arquivo da chave de criptografia encapsulada adicionada ao diretório `<proxy-installation-directory>/keys`. Por exemplo, se o nome do arquivo no diretório for `myunboundkey`, adicione este nome ao campo **Alias da chave**. Consulte Configurar chaves de criptografia na instância.

Criar uma chave de criptografia armazenada em um arquivo

Você pode usar um arquivo de texto simples como um repositório de chaves. Cada arquivo contém uma única chave de criptografia.

Antes de Iniciar

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

Essa etapa cria o armazenamento de chave e a chave de criptografia.

Nota: O nome do arquivo de chave deve corresponder ao alias de chave especificado na tabela de chaves de criptografia na instância. Consulte Configurar chaves de criptografia na instância.

Procedimento

1. Crie um arquivo na pasta `/keys` do diretório de instalação do servidor proxy.
2. Adicione aa chave de criptografia à instância.

Opção	Descrição
AES 128	Insira a chave de criptografia, de exatamente 16 bytes, no arquivo.
AES 256	Insira a chave de criptografia, de exatamente 32 bytes, no arquivo.

3. Atualize o arquivo `edgeencryption.properties`.
   a. Mude para o diretório `<installation directory>/conf/`.
   b. Abra o arquivo `edgeencryption.properties`.
   c. Insira as propriedades do repositório de arquivo.
   d. Salve e feche o arquivo.

Configurar chaves de criptografia na instância

O Edge Encryption fornece as ferramentas para gerenciar chaves de criptografia sem colocar o proxy offline.

Antes de Iniciar

Função necessária: security_admin

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de configurar novas chaves de criptografia na instância:

1. Crie a chave de criptografia.
2. Disponibilize a nova chave para todos os proxies de criptografia. Copie o arquivo ou o arquivo do Java KeyStore para cada proxy ou certifique-se de que cada proxy tenha acesso ao dispositivo Java KeyStore ou Enterprise Key Management (EKM).

Por Que e Quando Desempenhar Esta Tarefa

Os aliases de chave devem ser exclusivos. Cada alias de chave deve ter o mesmo tamanho e tipo de chave em cada proxy, ou a chave não poderá ser atribuída como padrão.

Procedimento

1. Navegue até **Todos** > **Configuração do Edge Encryption** > **Configuração de chave de criptografia** > **Configurar chaves**.
2. Na seção Adicionar novas chaves do formulário, conclua as etapas a seguir para adicionar uma nova chave.

   Importante: Se estiver usando chaves com controle de versão da SafeNet, uma coluna adicional da **versão da chave** será exibida. A **versão da chave** não pode ser editada. Clique no link **Recuperar versões de chave mais recentes** nos Links relacionados para recuperar a versão mais recente de cada chave do proxy do Edge.

   Linhas na lista com um **X** na coluna esquerda podem ser excluídas. Chaves que foram usadas como padrão ou que tenham um **Status** de **Disponível** não podem ser excluídas.

   a. Clique duas vezes em **Inserir uma nova linha**.

   b. Na caixa de edição, insira um nome para a chave e clique na marca de seleção.

      Os aliases de chave são letras minúsculas e números. As letras maiúsculas serão alteradas para letras minúsculas quando você clicar em **Atualizar**. Os aliases de chave devem ser exclusivos.

      Nota: Se estiver usando chaves de tecnologia não associadas, adicione o alias da chave de criptografia. O alias da chave de criptografia é o nome do arquivo da chave de criptografia encapsulada adicionada ao diretório `<proxy-installation-directory>/keys`. Por exemplo, se o nome do arquivo no diretório for `myunboundkey`, adicione este nome ao campo **Alias da chave**.

   c. Na mesma linha, clique duas vezes na coluna **Tamanho da chave**.

   d. Na caixa de seleção, escolha um tamanho de chave, **128 bits** ou **256 bits**, e clique na marca de seleção.

   e. Na mesma linha, clique duas vezes na coluna **Tipo**.

   f. Na caixa de seleção, selecione um tipo de chave, **Arquivo**, **Keystore**, **SafeNet**ou **Não associado**e clique na marca de seleção.

   g. Quando terminar de adicionar chaves, clique em **Próxima etapa**.
      Você deve especificar um alias, tamanho de chave e tipo de chave para cada chave antes de prosseguir.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Na seção Status das chaves do formulário, verifique o **Estado** da chave e certifique-se de que ela esteja **Disponível**.
4. Quando a chave estiver **Disponível**, clique em **Próxima etapa**.
   Isso pode levar alguns minutos.

   Nota: Se estiver usando chaves com controle de versão da SafeNet, uma coluna adicional da **versão da chave** será exibida. A **versão da chave** não pode ser editada.

   A instância rastreia o status de cada chave de criptografia disponível para qualquer proxy. Quando uma chave estiver disponível em todos os proxies, seu estado se tornará o de **Disponível**. Se o estado não mudar após alguns minutos, verifique se a chave está disponível em todos os proxies. Se o estado permanecer **Indisponível**, um ou mais proxies não terão a chave.

   Estados de chaves de criptografia

Status	Descrição
Disponível	Todos os proxies online têm a chave.
Indisponível	Essa é uma nova chave e os proxies ainda não carregaram, ou houve uma falha em pelo menos um proxy ao carregar a chave.

5. Na seção Alterar chaves padrão do formulário, siga um destes procedimentos:
   - Digite o alias da chave.
   - Clique no ícone de lupa e selecione um alias.

   Nota: Se estiver usando chaves com controle de versão da SafeNet, será exibido um campo adicional para a **versão da chave**. A **Versão de chave** ficará esmaecida e não poderá ser editada. Escolha somente a versão de chave mais recente. Se escolher uma versão anterior, a mensagem a seguir será exibida ao clicar em **Atualizar** ou em **Próxima etapa**.

   ```
   One of the default keys chosen is not the latest version available
    for the key. Please use the latest version.
   ```

   Se as chaves padrão não forem as versões mais recentes das chaves da SafeNet, o link **Atualizar chaves padrão para a versão mais recente** aparecerá nos Links relacionados. Clique no link para atualizar as chaves padrão para usar a versão mais recente.

6. Na seção Programar rotação de chave do formulário, agende um trabalho de rotação de chave em massa ou um trabalho de rotação de chave única para criptografar os dados existentes usando a nova chave de criptografia.

   Se não executar um trabalho de rotação de chave em massa ou um trabalho de rotação de chave única, os dados existentes permanecerão criptografados com a chave antiga até que sejam acessados novamente.

Configurar propriedades adicionais no arquivo de propriedades do Edge Encryption.

Depois de instalar o servidor proxy do Edge Encryption na rede e configurar o repositório de chaves e as chaves, configure as propriedades adicionais do Edge Encryption.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: administrador

Procedimento

1. Abra o arquivo `<installation directory>/conf/edgeencryption.properties` e configure as seguintes propriedades do servidor proxy do Edge Encryption:
   - Propriedades do destino (instância)
   - Propriedades da conta de usuário
   - Propriedades do proxy
   - Se estiver usando tipos de criptografia de preservação de ordem ou padrões de criptografia, configure as Propriedades do banco de dados
   - Propriedades de texto não criptografado e de VI estático
2. Salve e feche o arquivo.

Configurar um proxy da web

Se a sua rede usa um proxy da web, você pode configurar o proxy do Edge Encryption para usar o proxy da web.

Antes de Iniciar
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa
Se sua rede não usa um proxy da Web, deixe as propriedades do proxy da Web comentadas no arquivo de configuração.

O servidor proxy do Edge Encryption oferece suporte à conexão HTTP e à autenticação básica com o proxy da web.

Procedimento

1. Mude para o diretório `<installation directory>/conf/`.
2. Abra o arquivo `edgeencryption.properties`.
3. Configure as propriedades do proxy web
4. Salve e feche o arquivo `edgeencryption.properties`.
5. Se o proxy da web estiver usando um certificado de servidor específico do cliente, adicione este certificado ao JVM usado pelo servidor proxy do Edge Encryption para estabelecer confiança entre o proxy da web e o servidor proxy do Edge Encryption.
   a. Use o comando `cd` para navegar até `<Java home directory>/jre/lib/security/cacerts`
   b. Execute o comando: `keytool -keystore cacerts -importcert -alias<chooseAlias> -file<certificateFile>`

Definir o limite de memória inicial e o limite superior de memória do servidor proxy

Defina o limite de memória inicial e o limite superior de memória do servidor proxy para especificar quanta memória ele pode consumir. Defina esses limites para evitar problemas de desempenho em sua implementação do Edge Encryption.

Antes de Iniciar
Função necessária: administrador

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

Como diretriz, defina o limite de memória inicial e o limite de superior de memória com o mesmo valor. Em qualquer máquina, aloque 2 GB da memória física para o sistema operacional (SO). Em seguida, aloque o restante da memória física para o heap usando as propriedades de limite inicial e limite superior de memória. Por exemplo, em uma máquina com 8 GB de memória, aloque 2 GB para o sistema operacional e aloque os 6 GB (6144 m) restantes para os limites inicial e superior de memória.

Importante: Se o servidor proxy do Edge Encryption estiver em execução, será necessário interrompê-lo e reiniciá-lo após atualizar essas propriedades.

Procedimento

1. No diretório do servidor proxy, abra `<install dir>/conf/wrapper.conf`.
2. Para definir o limite de memória inicial, adicione a seguinte linha no final do arquivo:

   ```
   wrapper.java.additional.<number>=-Xms<min_memory_in_MB>m
   ```

   Configure `<number>` como o próximo `<number>` disponível na sequência das propriedades `wrapper.java.additional<number>` definidas no arquivo `wrapper.conf`.

   Example

   Por exemplo, você tem a seguinte lista de propriedades `wrapper.java.additional.<number>`:

   ```
   wrapper.java.additional.1=
   wrapper.java.additional.2=
   ```

   O `<number>` máximo na lista acima é **2**. Ao adicionar a linha `wrapper.java.additional.<number>=-Xms<min_memory_in_MB>m`, defina o `<number>` como **3**, que é o próximo número disponível.

   Importante: Não deixe lacunas na sequência de numeração.

   Defina `<min_memory_in_MB>` com o número de megabytes de memória restantes após a alocação de 2 GB de memória para o sistema operacional.

3. Defina o limite superior de memória

   Como um limite superior de memória não está definido no sistema base, o servidor proxy pode usar toda a memória disponível. Se outros serviços estiverem sendo executados no servidor, defina o limite superior de memória.

   Adicione a seguinte linha no final do arquivo:

   ```
   wrapper.java.additional.<number>=-Xmx<max_memory_in_MB>m
   ```

   Configure `<number>` como o próximo `<number>` disponível na sequência das propriedades `wrapper.java.additional<number>` definidas no arquivo `wrapper.conf`.

   Example

   Por exemplo, você tem a seguinte lista de propriedades `wrapper.java.additional.<number>`:

   ```
   wrapper.java.additional.1=
   wrapper.java.additional.2=
   ```

   O `<number>` máximo na lista acima é **2**. Ao adicionar a linha `wrapper.java.additional.<number>=-Xmx<max_memory_in_MB>m`, configure `<number>` como **3**, que é o próximo número disponível.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Não deixe lacunas na sequência de numeração.

Defina `<max_memory_in_MB>` com o número de megabytes de memória restantes após a alocação de 2 GB de memória para o sistema operacional.

4. Salve e feche o arquivo.

Example: Exemplo: configuração dos limites de memória inicial e de limite superior do servidor proxy

```
wrapper.java.additional.1 = -Djava.io.tmpdir=../tmp
wrapper.java.additional.2 = -Dcloudedge.home.dist=..
# must ensure UTF8 encoding when running on Windows
wrapper.java.additional.3 = -Dfile.encoding=UTF8
# additional properties for heap settings
wrapper.java.additional.4 = -Xms6144m
wrapper.java.additional.5 = -Xmx6144m
```

O que Fazer Depois

Iniciar o proxy do Edge Encryption.

Iniciar o proxy do Edge Encryption

Depois da instalação e configuração do proxy do Edge Encryption você pode iniciar o proxy a partir da linha de comando.

Antes de Iniciar

Função necessária: administrador

Antes de iniciar o proxy de criptografia, verifique o seguinte:

- O plug-in do Edge Encryption foi ativado na instância.
- O arquivo `edgeencryption.properties` nesta máquina foi configurado.
- O banco de dados de proxy está em execução, caso esteja usando tipos de criptografia de preservação de ordem ou padrões de criptografia

Nota: Pode ser que na primeira vez que você configura o arquivo `edgeencryption.properties` ou muda as propriedades, não deseje definir a propriedade de criptografia de senha. Depois de verificar se tudo está funcionando, você poderá definir a propriedade de criptografia de senha, encerrar o proxy e reiniciá-lo.

Procedimento

1. Execute o servidor proxy.

Opção	Descrição
Em uma máquina Linux	**a.** `cd` para `ServerName_port` **b.** Execute `./startup.sh`
Em uma máquina do Windows	Execute as seguintes etapas na linha de comando como administrador:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	a. `cd` para `ServerName_port/bin` **b.** Execute `edgeencryption.bat start`

2. Verifique o log no servidor proxy para verificar se o proxy está em execução.

Ofuscar senhas no arquivo de propriedades

Ofusque senhas no arquivo `edgeencryption.properties` para compartilhar o arquivo de propriedades sem revelar senhas em texto não criptografado.

Antes de Iniciar
Função necessária: administrador

Certifique-se de que o servidor proxy do Edge Encryption esteja configurado e em execução com êxito antes de definir esta propriedade. Antes de definir esta propriedade, Interromper o proxy do Edge Encryption.

Por Que e Quando Desempenhar Esta Tarefa
A definição desta propriedade pode dificultar a depuração de problemas de conexão e acesso durante a inicialização. Somente defina esta propriedade em ambientes de produção depois que o proxy tiver sido configurado e testado com sucesso.

Procedimento

1. Mude para o diretório `<installation directory>/conf/`.
2. No diretório `conf`, crie um arquivo de texto contendo uma cadeia de caracteres ou frase complexa que possa ser usada como senha usada pelo proxy para ofuscar as senhas no arquivo `edgeencryption.properties`.
   Essa senha deve ser aleatória e complexa, não relacionada às senhas em si.
3. Abra o arquivo `edgeencryption.properties`.
4. Defina a propriedade de criptografia de senha.
5. Salve e feche o arquivo `edgeencryption.properties`.

O que Fazer Depois
Depois de definir esta propriedade, você pode Iniciar o proxy do Edge Encryption.

Adicionar manualmente um proxy adicional

Depois que o primeiro proxy doEdge Encryption for configurado e testado corretamente, você poderá configurar proxies adicionais em uma máquina Linux ou Windows. Não é recomendável instalar vários proxies na mesma máquina.

Antes de Iniciar
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa
Adicione servidores proxy adicionais em máquinas adicionais para garantir um ambiente ideal. Consulte Dimensionando seu ambiente do Edge Encryption para determinar o número de proxies adicionais necessários.

Nota: Assegure-se de que todos os proxies tenham as mesmas chaves de criptografia e o mesmo par de chaves RSA usado para assinar digitalmente configuração e regras de criptografia. Se foi configurado um banco de dados de proxy como parte da instalação, todos os proxies deverão usar esse mesmo banco de dados de proxy.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Instale o proxy usando o comando apropriado.
   Para obter mais informações, consulte Instale o servidor proxy do Edge Encryption (instalador interativo).
2. Copie todas as chaves de criptografia e o arquivo `edgeencryption.properties` do primeiro proxy para o novo proxy.
   As chaves de criptografia podem estar localizadas no repositório de chaves do proxy, no diretório `/ keys` ou em um repositório de chaves SafeNet KeySecure.
3. Abra o arquivo `edgeencryption.properties` no novo proxy.
4. Altere as seguintes propriedades:

Propriedade	Descrição
edgeencryption.proxy.name	Nome exclusivo do serviço de proxy.
edgeencryption.proxy.host	O nome do servidor, o endereço IP ou o nome de domínio totalmente qualificado do computador que executa o proxy.
edgeencryption.proxy.http.port	Porta no proxy para comunicação HTTP. Deve ser exclusiva em todos os processos da máquina.
edgeencryption.proxy.https.port	Porta no proxy para comunicação HTTPS. Deve ser exclusivo entre os processos na máquina.

5. Se estiver instalando o servidor proxy em um computador Windows, mude o nome do serviço abrindo o arquivo `conf/wrapper.conf` no novo proxy e incluindo as propriedades listadas na tabela a seguir.

   Nota: Essa etapa deve ser executada antes da inicialização do servidor proxy.

Propriedade	Descrição
wrapper.ntservice.name	Nome exclusivo do serviço de proxy do Edge Encryption.
wrapper.ntservice.displayname	Edge Encryption: o nome de exibição do serviço de proxy.
wrapper.ntservice.description (opcional)	Descrição do servidor proxy.

6. Salve e feche o arquivo.
7. Inicialize o proxy usando o comando apropriado.
   Para obter mais informações, consulte Iniciar o proxy do Edge Encryption.

Autenticar um servidor proxy do Edge Encryption

Especifique um servidor proxy como fonte confiável para que o Edge Encryption possa processar solicitações provenientes desse servidor proxy.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Se um servidor proxy não for autenticado, o log do console incluirá a seguinte mensagem:

```
WARN This Edge Encryption proxy has not yet been authenticated by the
 instance.
Please navigate to the matching Proxy record on your ServiceNow instance
 and authenticate it.
```

Se você tentar acessar o proxy, receberá a mensagem: `Este site não pode ser acessado`.

Para manter o proxy em um estado operacional durante o processo de upgrade, a autenticação não é necessária até que a atualização do proxy seja bem-sucedida.

Função necessária: administrador

Procedimento

1. Navegue até **Todos** > **Configuração do Edge Encryption** > **Proxies**.
2. Selecione o proxy e clique em **Autenticar**.

Resultados

O proxy passa de **Não autenticado** para **Pendente** e para **Autenticado**. O status muda de **Não autenticado** para **Pendente** quando você inicia a autenticação. Quando a autenticação é concluída, o status muda de **Pendente** para **Autenticado** e você pode acessar o proxy e o Edge Encryption pode aceitar solicitações do proxy.

Nota: Se você parar e reiniciar o proxy, ele permanecerá **Autenticado** e será reiniciado com êxito.

Interromper o proxy do Edge Encryption

Você interromper um proxy do Edge Encryption na linha de comando.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Interrompa o servidor proxy.

Opção	Descrição
Em uma máquina Linux	Execute `./shutdown.sh`
Em uma máquina do Windows	Execute `edgeencryption.bat stop` Para remover o serviço do Windows, execute `edgeencryption.bat remove`

2. Verifique o log no servidor proxy para verificar se o proxy foi interrompido.

Desinstalar o proxy do Edge Encryption no Linux

Você pode desinstalar o proxy do Edge Encryption. Se estiver atualizando o proxy, não será necessário encerrar e desinstalar a versão atual.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: administrador

Você deve ter acesso ao computador que executa o proxy do Edge Encryption.

Por Que e Quando Desempenhar Esta Tarefa
Antes de encerrar o proxy do Edge Encryption, certifique-se de que nenhum usuário esteja conectado à instância usando o proxy.

O proxy de criptografia em execução no Linux opera como um processo único. Você pode encerrar esse processo para acomodar tarefas como reimplantar o proxy de criptografia em outra máquina host, atualizar a versão do proxy, atualizar a versão Java ou alterar o nome exclusivo do proxy de criptografia ao implantar o proxy de criptografia em vários servidores proxy.

Procedimento
1. Você pode salvar o arquivo `edgeencryption.properties` antes de excluir o diretório de distribuição.
2. Execute o script de shell `shutdown.sh`.
3. Verifique o log no servidor proxy para verificar se o servidor proxy foi encerrado.
4. Exclua os arquivos na pasta de distribuição.

Desinstalar o proxy do Edge Encryption no Windows

Você pode desinstalar o proxy do Edge Encryption. Se estiver atualizando o proxy, não será necessário encerrar e desinstalar a versão atual.

Antes de Iniciar
Função necessária: administrador

Você deve ter acesso ao computador que executa o proxy do Edge Encryption.

Antes de encerrar o proxy do Edge Encryption, certifique-se de que nenhum usuário esteja conectado à instância usando o proxy.

Procedimento
1. Você pode salvar o arquivo `edgeencryption.properties` antes de excluir o diretório de distribuição.
2. Execute `edgeencryption.bat stop`
3. Execute `edgeencryption.bat remove`
4. Verifique o log no servidor proxy para verificar se o servidor proxy foi encerrado.
5. Exclua os arquivos na pasta de distribuição.

Configurar SSO de provedores múltiplos com o Edge Encryption

Configure o SSO de provedores múltiplos para habilitar o login por meio do URL do servidor proxy do Edge Encryption ou do URL da instância. Se estiver implementando o Single Sign-on (SSO) de vários provedores com o Edge Encryption habilitado, alguns usuários talvez precisem fazer login na sua instância por meio do servidor proxy do Edge Encryption, enquanto outros usuários não.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

- Habilite o plug-in Integration - Multiple Provider Single Sign-On Installer (com.snc.integration.sso.multi.installer).
- Habilite o plug-in Edge Encryption (com.glide.edgeencryption) e certifique-se de que um ou mais servidores proxy estejam configurados em sua rede.
- Determine o URL do servidor proxy do Edge Encryption no qual os usuários farão login usando o SSO de provedores múltiplos. Para determinar o URL de um servidor proxy do Edge Encryption, consulte Instalando o Edge Encryption.

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

O usuário que faz login precisará usar o URL apropriado para fazer login, usando o Edge Proxy ou não.

- Se estiver roteando todos os usuários por meio do servidor proxy do Edge Encryption, configure o registro de identificação do provedor e defina o URL do servidor proxy nos campos **Página inicial da ServiceNow**, **ID da entidade/do emissor**e **URI do público**.
- Para rotear alguns usuários por meio do servidor proxy e alguns usuários para a instância, crie dois registros de provedor de identificação. Ambos os registros devem usar o mesmo valor no campo **URL do provedor de identidade**. No entanto, um dos registros será roteado por meio do servidor proxy, enquanto o outro será roteado para a instância.
  - Login pelo nome da instância: `https://<instance name>.service-now.com/login_with_sso.do?glide_sso_id=<sys_id` do registro de IdP para proxy não Edge
  - Faça login via proxy do Edge: `https://<edge hostname> :<port> /login_with_sso.do?glide_sso_id= <sys_id` do registro IdP para o proxy do Edge

Procedimento

1. Habilite a duplicação de URLs do provedor de identidade nos registros de provedor de identidade.
   Uma restrição exclusiva evita a duplicação do URL do provedor de identidade em dois registros de provedor de identidade diferentes. Você pode habilitar a duplicação do URL do provedor de identidade em vários registros de IdP, definindo um campo como falso.
   a. Navegue até **Definição do sistema** > **Dicionário**.
   b. Abra o registro de definição do campo **idp** na tabela Provedores de identidade [saml2_update1_properties].
   c. Configure o formulário para adicionar o campo **Exclusivo**.
   d. Certifique-se de que o valor do campo **Exclusivo** esteja definido como **falso**.
2. Navegue até **SSO de vários provedores** > **Provedores de identidade**.
3. Crie dois registros de provedor de identidade para o mesmo provedor de identidade: um usando o URL da instância e um usando o URL do servidor proxy Edge Encryption.
   Para criar um registro de provedor de identidade, consulte Criar um provedor de identidade externo.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Para o URL do servidor proxy do Edge Encryption, preencha o formulário usando estes valores.

Campo	Valor
URL do provedor de identidade	Importado dos metadados do IdP
Página inicial do ServiceNow	O URL da página inicial do servidor proxy. Por exemplo: `https://<proxy hostname> :<port>/navpage.do`
ID da entidade/do emissor	`https://<proxy hostname>:<port>`
URI do público	`https://<proxy hostname>:<port>`

b. Clique em **Enviar**.

c. Para o URL da instância, preencha o formulário usando esses valores.

Campo	Valor
URL do provedor de identidade	Importado dos metadados do IdP
Página inicial do ServiceNow	`https://<instance>.service-now.com/navpage.do`
ID da entidade/do emissor	`https://<instance>.service-now.com/navpage.do`
URI do público	`https://<instance>.service-now.com/navpage.do`

d. Clique em **Enviar**.

4. Opcional: Se estiver usando mais de um provedor de identidade, modifique a saída de instalação do MultiSSO.

a. Navegue até **Definição do Sistema** > **Saídas de instalação**.
O sistema exibe a lista atual de saídas de instalação.

b. Abra a saída de instalação do **MultiSSO**.

c. Localize a declaração a seguir no campo **Script**.

```
var samlResponseTxt = request.getParameter("SAMLResponse");
if (!GlideSession.get().isLoggedIn() &&
 GlideStringUtil.notNil(samlResponseTxt)) {
    var idpRecord = this.getIdPRecord(request);
    if (idpRecord) {
        SSO_Helper.debug("IdP found based on SAML response: " +
 idpRecord.getUniqueValue());
        return new SSO_Helper(idpRecord.getUniqueValue(), false, null,
 true);
```

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

```
    }
}
```

d. Substitua a declaração pelo código a seguir.

```
var samlResponseTxt = request.getParameter("SAMLResponse");
if (!GlideSession.get().isLoggedIn() &&
 GlideStringUtil.notNil(samlResponseTxt)) {
   /* // You have two profiles that use the same IdP entity id it
 cannot use
   // the IdP issuer / entity id from the response otherwise it may
 result in the
   // wrong IdP profile. IdP initiated login will not work
   var idpRecord = this.getIdPRecord(request);
   if (idpRecord) {
      SSO_Helper.debug("IdP found based on SAML response: " +
 idpRecord.getUniqueValue());
      return new SSO_Helper(idpRecord.getUniqueValue(), false, null,
 true);
      }*/
   return new SSO_Helper(null, true);
   }
```

Nota: O login iniciado pelo IdP não funcionará nesta configuração.

e. Clique em **Atualizar**.

5. Opcional: Se estiver usando mais de uma empresa, configure os usuários para SSO de vários provedores e atualize o sys_id do registro do provedor de identidade, dependendo do usuário.

(Optional) Para obter mais informações, consulte Configuração de usuários para SSO de vários provedores.

- Para configurar um usuário para fazer login por meio do servidor proxy do Edge Encryption, use o sys_id do registro do provedor de identidade que usa o URL do servidor proxy do Edge Encryption.
- Para configurar um usuário para efetuar login na instância, use o sys_id do registro do provedor de identidade que usa o URL da instância.

URLs de login

URL	Destino do login
`https://<proxy hostname>:<port>/login_with_sso.do?glide_sso_id=<sys_id do registro IdP do URL do servidor proxy>`	Faz login por meio do servidor proxy.
`https://<instance name>.service-now.com/login_with_sso.do?glide_sso_id=<sys_id do registro IdP do URL da instância>`	Faz login por meio da instância.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Propriedades do servidor proxy do Edge Encryption

O arquivo de configuração `edgeencryption.properties` localizado na pasta `<installation directory>/conf/` contém propriedades usadas para configurar seu ambiente.

Você deve reiniciar o servidor proxy depois de fazer mudanças em qualquer propriedade do servidor proxy.

Propriedades de texto não criptografado e de VI estático

edgeencryption.customer.assigned.known.cleartext	Use o texto não criptografado ara permitir que a instância verifique se todos os proxies estão usando as mesmas chaves. Na inicialização, o proxy criptografa o texto não criptografado e o envia para a instância. A instância não conhece o texto não criptografado, nem são enviadas chaves para a instância. Essa propriedade deve ser a mesma para todos os proxies.
edgeencryption.encrypter.static.iv	VI estático (vetor de inicialização) usado na criptografia de preservação de igualdade e preservação de ordem. Esta propriedade deve ser a mesma para todos os proxies e deve ter exatamente 16 bytes (16 caracteres ASCII).

Propriedades da assinatura digital

edgeencryption.proxy.signature.keystore.path	Caminho e nome do arquivo do Java KeyStore.
edgeencryption.proxy.signature.keystore.password	Senha. A senha padrão é <changeme>. Altere a senha após instalar o Java KeyStore.
edgeencryption.proxy.signature.keystore.keyalias	O alias de chave fornecido como o argumento -alias quando o par de chaves RSA é gerado.

Propriedade de repositório de arquivos

edgeencryption.keyfile.directory	O diretório especifica onde os arquivos de chave são armazenados. Se estiver usando o Java KeyStore ou um repositório de chaves SafeNet KeySecure, deixe esta propriedade comentada. Exemplo: `edgeencryption.keyfile.directory=keys` Se estiver usando chaves de tecnologia não associadas, remova o comentário desta

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

	propriedade e defina o valor do diretório de chaves.

Propriedades gerais de configuração

edgeencryption.config.poll.interval	Intervalo de pesquisa em segundos Com a configuração padrão demora 5 segundos para o proxy aprender sobre as mudanças na configuração de criptografia. Valores maiores fazem com que a instância demore mais para detectar proxies que ficaram offline. ⚠ **Aviso:** Não mude esta propriedade. Alterar a configuração padrão do Intervalo de pesquisa de proxy pode resultar em atrasos na detecção de quando um proxy fica online.
edgeencryption.rules.dir	Pasta onde as regras de criptografia são armazenadas no proxy.
edgeencryption.encryption.order_preserving.cache.enable	A configuração determina se o cache é usado para oferecer suporte a tipos de criptografia de preservação de ordem.
edgeencryption.encryption.order_preserving.cache.size	Tamanho máximo de cache, em bytes
edgeencryption.jobs.concurrency	Número máximo de trabalhos de criptografia em massa que podem ser executados simultaneamente neste proxy.
edgeencryption.jobs.requests_per_second	Número de solicitações de trabalho http por segundo que podem ser enviadas para a instância por este proxy.
edgeencryption.attachments.request.timeout.seconds	Tempo limite da solicitação de carregamento de anexo em segundos.
edgeencryption.request.buffer.size	Tamanho de uma solicitação de criptografia. Se uma solicitação de criptografia for maior do que esse tamanho, o excesso será salvo no disco. ⚠ **Aviso:** Não mude esta propriedade.
edgeencryption.httpclient.request.buffer.size	Tamanho da solicitação do cliente. Se uma solicitação do cliente for maior do que esse tamanho, o excesso será salvo no disco. ⚠ **Aviso:** Não mude esta propriedade.
edgeencryption.httpclient.header.size	Tamanho do cabeçalho de solicitação/ resposta. • Valor mínimo: 8K • Valor máximo: 32K

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

	⚠ **Aviso:** Não mude esta propriedade.
edgeencryption.proxy.idle.timeout	Tempo em segundos após o qual uma transação expira. Valor padrão: 300 (segundos)
edgeencryption.proxy.keepalive.interval	Tempo em segundos entre os pings emitidos pelo proxy para a instância. Os pings são emitidos periodicamente para verificar a conectividade entre o proxy e a instância. • Valor padrão: 10 (segundos) • Valor mínimo: 5 (segundos)
edgeencryption.register.retry.count	Número máximo de vezes que o proxy executa ping na instância para tentar registrar. Valor padrão: 0 (sem limite)
edgeencryption.tokenization.exclusion.list	Os padrões de criptografia não podem tokenizar cadeias de caracteres encontradas nesses campos.

Propriedades do Java KeyStore

edgeencryption.keystore.path	Caminho para o Java KeyStore. Se estiver usando um repositório de arquivo ou um repositório de chaves SafeNet KeySecure, deixe esta propriedade comentada. Exemplo: `edgeencryption.keystore.path = keystore/keystore.jceks`
edgeencryption.keystore.password	Senha usada pelo proxy para se conectar ao Java KeyStore. Se estiver usando um repositório de arquivo ou um repositório de chaves SafeNet KeySecure, deixe esta propriedade comentada.

Propriedades de registro em log

As propriedades de registro em log são encontradas no arquivo lo4gj2.properties encontrado no diretório `<installation directory>/conf/`. Essas propriedades são alteradas somente para solução de problemas ou quando orientadas pelo suporte ServiceNow. Para obter detalhes, consulte Como aumentar o registro em log de depuração do proxy do Edge Encryption.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Propriedades de repositório de chaves do dispositivo NAE

edgeencryption.nae.retries	Número de novas tentativas a serem realizadas.
edgeencryption.nae.enabled	A configuração indica se um dispositivo NAE está disponível.
edgeencryption.nae.server	Nome do servidor NAE.
edgeencryption.nae.port	Porta usada pelo servidor NAE.
edgeencryption.nae.protocol	Protocolo usado pelo servidor NAE.
edgeencryption.nae.keystore.path	Caminho para o repositório de chaves no servidor NAE.
edgeencryption.nae.keystore.password	Senha do repositório de chave NAE
edgeencryption.nae.username	Nome de usuário a ser usado para autenticação com o dispositivo NAE.
edgeencryption.nae.password	Senha a ser usada para autenticação com o dispositivo NAE.
edgeencryption.nae.client.certificate	Certificado localizado no repositório de chaves no servidor NAE. Defina esta propriedade para autenticar usando um certificado em vez de um nome de usuário e senha.

Propriedade de senha

edgeencryption.encrypter.properties.password	Nome do arquivo na pasta `conf` que contém uma cadeia de caracteres usada em um processo seguro para ofuscar senhas no arquivo `edgeencryption.properties`. **Nota:** Nome do arquivo na pasta `conf` que contém uma cadeia de caracteres usada em um processo seguro para ofuscar senhas no arquivo `edgeencryption.properties`.

Propriedades do proxy

edgeencryption.proxy.host	O nome do servidor, o endereço IP ou o nome de domínio totalmente qualificado do computador que executa o proxy. Junto com a porta, essa propriedade define o URL usado pelo cliente para acessar o servidor proxy.
edgeencryption.proxy.name	Nome do proxy. Deve ser exclusivo para cada proxy.
edgeencryption.proxy.http.port	Porta no proxy para comunicação HTTP.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

edgeencryption.proxy.https.port	Porta no proxy para comunicação HTTPS.

Propriedade bloqueada da configuração de proxy

edgeencryption.proxy.locked	Quando verdadeiro, o proxy não aceita mudanças de configuração de criptografia ou mudanças de regra de criptografia pela instância. Defina essa propriedade na instância de produção depois que todas as configurações e regras de criptografia sejam as finais.

Propriedades do banco de dados do proxy

edgeencryption.db.url	Local do banco de dados do proxy. Deve ser o mesmo para todos os proxies de criptografia que se conectem à mesma instância.
edgeencryption.db.user	Nome de usuário para acessar o banco de dados do proxy. Deve ser o mesmo para todos os proxies de criptografia que se conectem à mesma instância.
edgeencryption.db.password	Senha para acessar o banco de dados do proxy. Deve ser o mesmo para todos os proxies de criptografia que se conectem à mesma instância.
edgeencryption.db.name	Nome do banco de dados do proxy Deve ser o mesmo para todos os proxies de criptografia que se conectem à mesma instância. O padrão desta propriedade é `edgeencryption`.
edgeencryption.db.bootstrap.file	Arquivo de inicialização do banco de dados do proxy. O arquivo é relativo ao diretório `sql/`. Deve ser o mesmo para todos os proxies de criptografia que se conectem à mesma instância. ⚠ **Aviso:** Em circunstâncias normais, não altere este parâmetro.

Propriedades de desempenho do servidor proxy

As propriedades de desempenho do servidor proxy não estão presentes no arquivo de configuração por padrão. Para mudar os valores padrão, você deve adicionar as propriedades e reiniciar o servidor proxy. Para obter mais informações, consulte Diagnóstico e desempenho do Edge Encryption.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

edgeencryption.stat.collection.enabled	Habilita a coleta de estatísticas usadas pelo painel de desempenho do servidor proxy do Edge Encryption. Valor padrão: verdadeiro Adicione essa propriedade e configure o valor como falso para desabilitar a coleta de estatísticas usada pelo painel de desempenho do servidor proxy do Edge Encryption.
edgeencryption.stat.collection.interval	Duração do intervalo em segundos durante o qual o servidor proxy doEdge Encryption coleta estatísticas. O valor não pode ser inferior a 30 segundos. Valor padrão: 30 (segundos)

Propriedades da certificação SSL

Reinicie o proxy se você alterar o valor de qualquer propriedade de certificação SSL. O sistema usa o par de chaves HTTPS na inicialização para estabelecer a conexão do servidor proxy e determinar como o proxy responde às solicitações do cliente.

edgeencryption.proxy.https.cert.alias	Alias do certificado fornecido pelo servidor proxy para conexão de clientes.
edgeencryption.proxy.https.keystore.path	Caminho para o repositório de chaves que contém o certificado HTTPS.
edgeencryption.proxy.https.keystore.password	Senha para o repositório de chaves que contém o certificado HTTPS.

Propriedades do destino (instância)

edgeencryption.target.host	Nome do host da instância. Deve ser o mesmo para todos os proxies de criptografia que se conectem à mesma instância. Essa propriedade é definida quando o proxy é instalado. Por exemplo, `instancename.servicenow.com`
edgeencryption.target.port	Porta de instância. Deve ser o mesmo para todos os proxies de criptografia que se conectem à mesma instância. Essa propriedade é definida quando o proxy é instalado.
edgeencryption.target.protocol	Protocolo de instância. Deve ser o mesmo para todos os proxies de criptografia que se conectem à mesma instância. Essa propriedade é definida quando o proxy é instalado. As opções incluem:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

	• http • https

Propriedades do provedor de tecnologia não associado

edgeencryption.ekm.provider.classname	Nome da classe interna para a implementação. ⚠ **Aviso:** Não mude esta propriedade.
edgeencryption.thirdparty.vendor.library.path	Caminho para o arquivo JAR da API não associada na máquina do cliente não associada.
edgeencryption.ekm.provider.rsa.wrapping.key.alias	Encapsulamento de alias de chave na implementação de tecnologia não associada. Deve ser a mesma para todos os proxies.

Propriedades da conta de usuário

edgeencryption.target.username	Nome de usuário usado pelo proxy para fazer login na instância. O usuário deve ter a função edge_encryption. Consulte Configurar uma conta de usuário do Edge Encryption.
edgeencryption.target.password	Senha usada pelo proxy para fazer login na instância.

Propriedades do proxy da web

edgeencryption.webproxy.host	Nome ou endereço IP do proxy da web.
edgeencryption.webproxy.port	Porta no proxy da web.
edgeencryption.webproxy.user	Nome de usuário usado para se conectar ao proxy da web. Se o proxy da web não usar autenticação, deixe esta propriedade comentada.
edgeencryption.webproxy.password	Senha a ser usada para se conectar ao proxy da web. Se o proxy da web não usar autenticação, deixe esta propriedade comentada.

Propriedades de criptografia de proxy descontinuadas

edgeencryption.encrypter.default.key128

Especifica o nome da chave AES 128 atual. Uma chave AES 128 deve estar disponível mesmo se não for usada. Deve ser a mesma para todos os proxies.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Execute a manutenção dessas chaves na instância.

edgeencryption.encrypter.default.key256

Especifica o nome da chave AES 256 atual. Deve ser a mesma para todos os proxies.

Execute a manutenção dessas chaves na instância.

edgeencryption.encrypter.key

Especifica o nome de cada chave e é usado para especificar as chaves padrão. Este é o alias de chave integrado com os metadados incluídos com cada item criptografado e, portanto, é armazenado na instância. O nome da chave deve ter letras minúsculas.

edgeencryption.encrypter.type

Especifica o tipo de sistema de armazenamento de chaves de criptografia.

edgeencryption.encrypter.file

Especifica o caminho e o nome do arquivo de texto associado à chave.

edgeencryption.encrypter.password

Especifica a senha para acessar o armazenamento de chaves.

Integração do CyberArk com o servidor proxy Edge

Use o CyberArk para armazenar senhas em um cofre digital centralizado e seguro para proteger senhas que foram armazenadas anteriormente em texto não criptografado e protegidas por acesso a arquivo, ou que foram criptografadas por meio de um segundo arquivo.

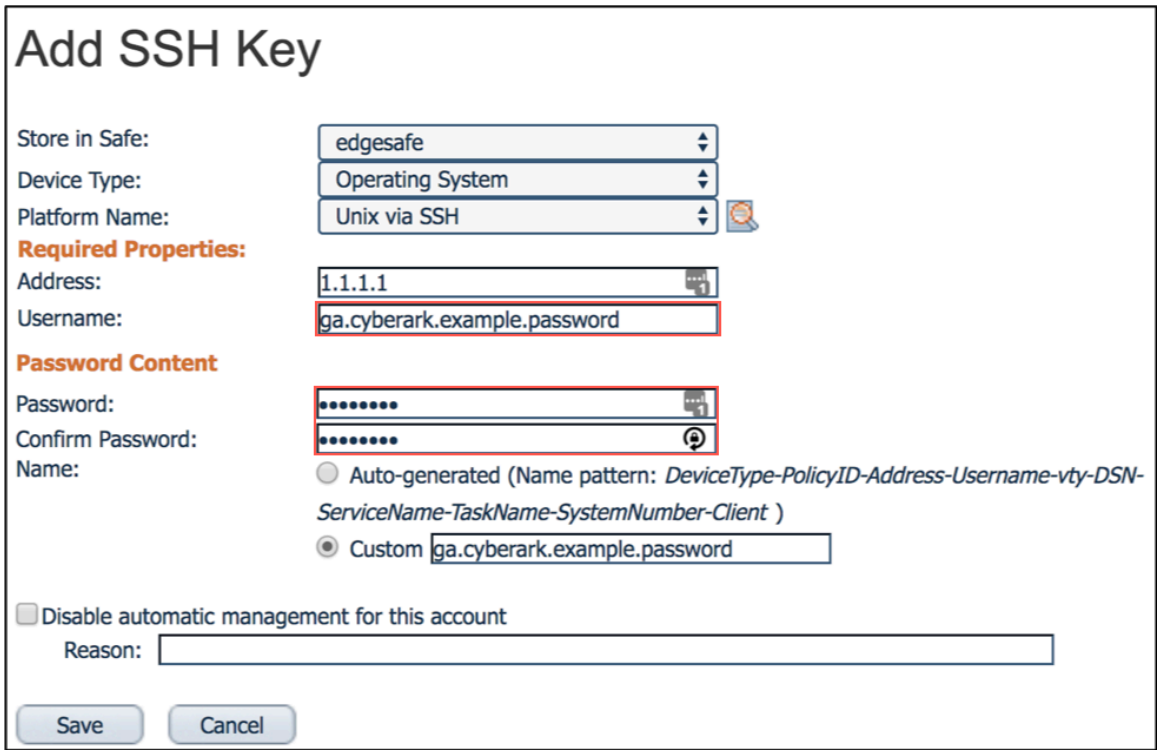
O CyberArk AIM (Application Identity Management) evita o acesso não autorizado, eliminando senhas codificadas e visíveis. O AIM armazena senhas em um cofre digital em um servidor protegido independente, onde elas são representadas como credenciais digitais. Os clientes do AIM (os servidores proxy do Edge) usam credenciais digitais da CyberArk e acessam o servidor independente para recuperar as senhas protegidas. Nenhuma senha é armazenada nos servidores proxy do Edge ou na instância.

Credenciais do cofre digital da CyberArk

É necessário comprar e configurar o CyberArk antes de configurar a integração do CyberArk com o servidor proxy do Edge.

Para adicionar uma credencial ao CyberArk (que é lida pelo proxy do Edge), defina o **Nome da plataforma** da credencial como **Unix via SSH** e certifique-se de criar um **Nome** de credencial **Personalizado** ou anotar o **Nome** de credencial **gerado automaticamente**. Quando você configura o proxy do Edge para usar essa credencial, o servidor proxy faz a correspondência entre o **Nome** dessa credencial com a configuração no proxy.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



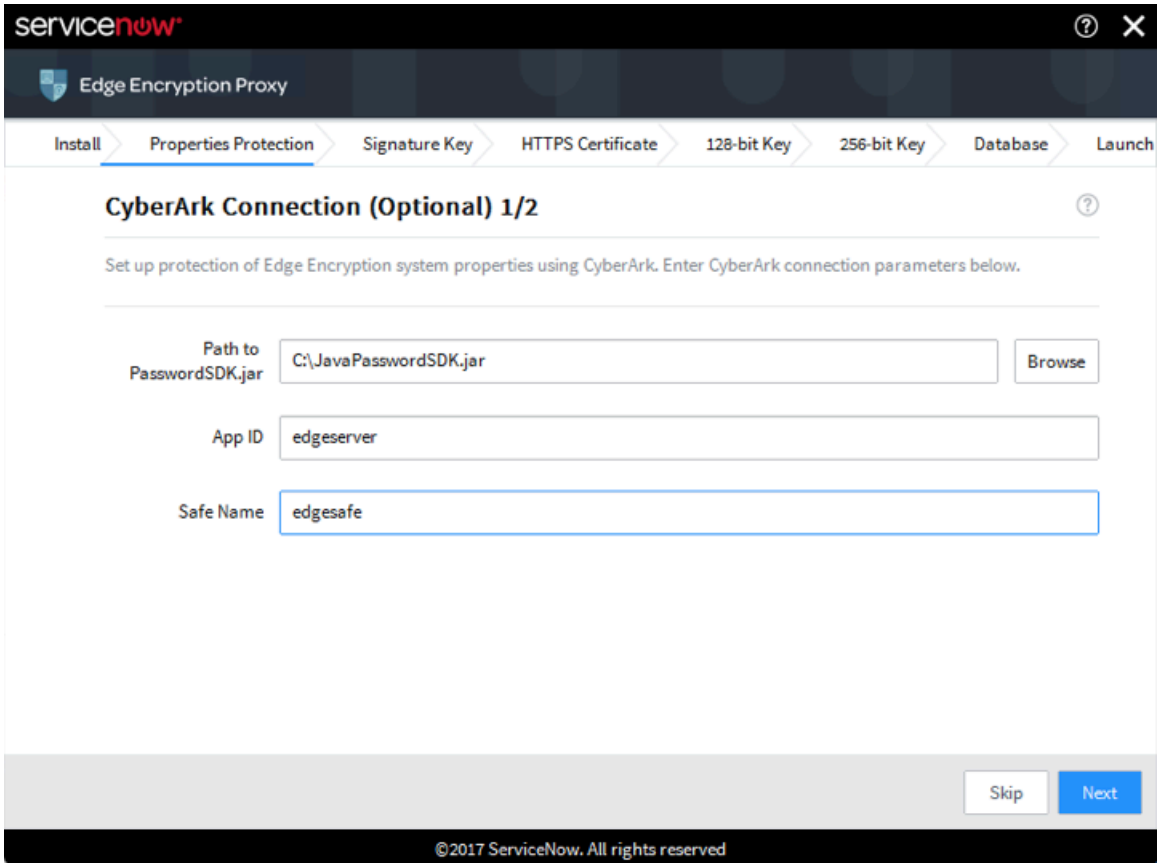
Cada entrada de credencial contém uma **Senha** que está sendo protegida, bem como um **Nome** de credencial usado por uma aplicação para acessar essa senha.

Nota: As credenciais do CyberArk não são chaves de criptografia.

Como adicionar o CyberArk durante uma instalação de proxy do Edge

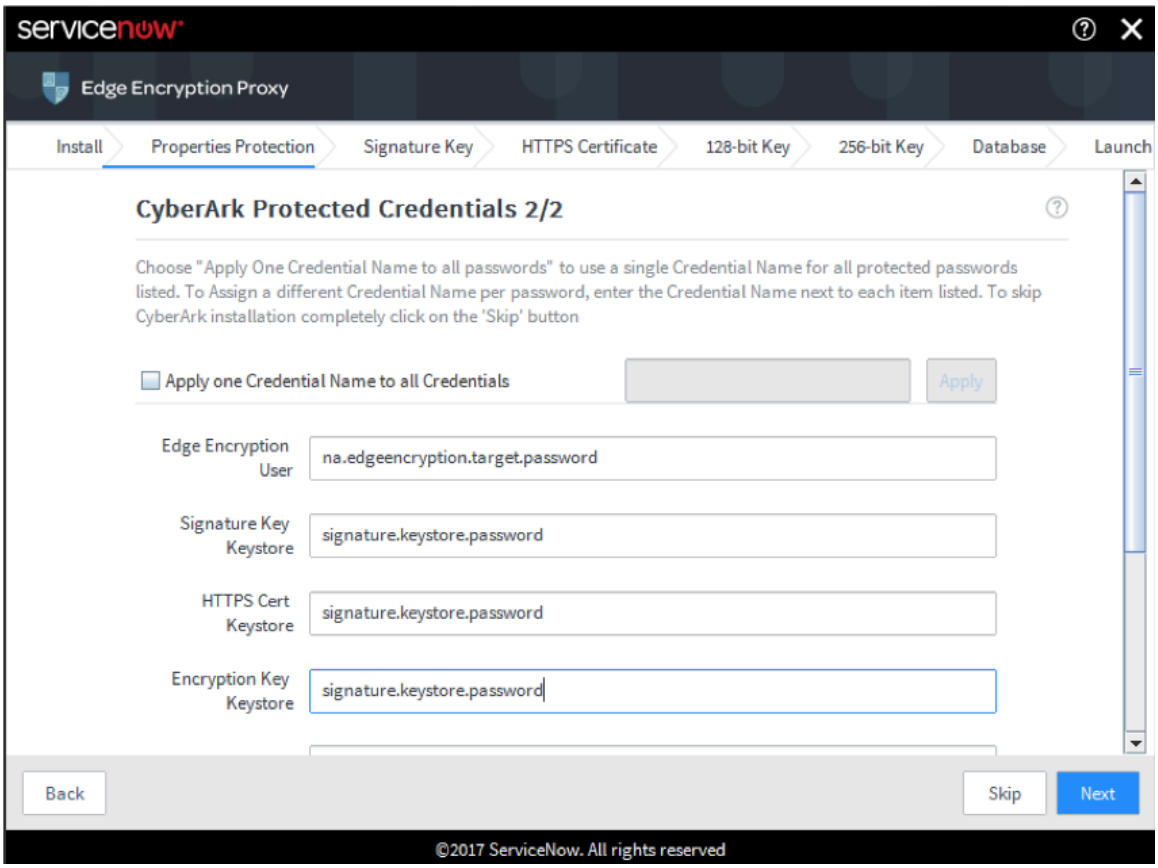
O instalador de proxy inclui uma nova página de configuração para a realização da integração do CyberArk. Ela é opcional caso não deseje incluir o CyberArk ao instalar seu proxy com o instalador de proxy. Você também pode definir manualmente a integração do CyberArk no arquivo de configuração.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



O instalador de proxy também inclui uma nova página de credenciais protegidas do CyberArk. Essa página permite configurações de diferentes propriedades usando um nome único ou vários nomes de credencial. Ela é opcional caso não deseje incluir o CyberArk ao instalar seu proxy com o instalador de proxy.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Proteção de senha do CyberArk

Qualquer campo de senha no instalador de proxy do Edge com uma credencial do CyberArk configurada no cofre do CyberArk e especificado na página Credenciais protegidas do CyberArk do instalador estará esmaecido e conterá a mensagem `Protegido pelo CyberArk`.

Usando um balanceador de carga com servidor proxy do Edge

Você pode usar um balanceador de carga para balancear a carga entre os servidores proxy na configuração do proxy Edge Encryption. Se o balanceador de carga e os servidores proxy estiverem usando portas diferentes, especifique o nome do host e a porta HTTPS do balanceador de carga para permitir que os usuários exibam respostas em seus navegadores.

Importante: Todos os ambientes de produção devem incluir pelo menos dois servidores proxy do Edge Encryption para redundância.

Processamento de solicitação do Edge sem um balanceador de carga

Se não estiver usando um balanceador de carga, uma solicitação será processada conforme descrito abaixo.

1. O usuário emite uma solicitação de um navegador.
2. O navegador envia a solicitação para o servidor proxy do Edge.
3. O servidor proxy envia a solicitação para a instância da ServiceNow.
4. A instância da ServiceNow retorna a resposta ao servidor proxy.
5. O servidor proxy adiciona seu próprio número de porta no cabeçalho da resposta antes de retornar a resposta ao navegador do usuário.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A solicitação foi concluída com sucesso porque o usuário pode visualizar a resposta do servidor proxy no número de porta especificado no cabeçalho da resposta.

Processamento de solicitação do Edge com um balanceador de carga

No entanto, se você estiver utilizando um balanceador de carga, o navegador do usuário se comunicará diretamente com o balanceador de carga, não com o servidor proxy. Uma solicitação será processada conforme descrito abaixo.

Nota: O exemplo a seguir usa `1025` como o número da porta do servidor proxy.

1. O usuário emite uma solicitação de um navegador.
2. O navegador envia a solicitação para um IP Virtual (VIP) do balanceador de carga, também conhecido como Servidor virtual.
3. O VIP está configurado para apontar para o servidor proxy (por exemplo, `10.2.200.148:1025`), portanto, o balanceador de carga encaminha a solicitação para o servidor proxy.
4. O servidor proxy envia a solicitação para a instância da ServiceNow.
5. A instância da ServiceNow retorna a resposta ao servidor proxy.
6. O servidor proxy reescreve o cabeçalho do local na resposta com valores configurados nas propriedades de `risk-servicenow.dev.echonet: 1025`.
   - **Host**: `edgencryption.proxy.host`
   - **Porta HTTP**: `edgeencryption.proxy.http.port`
   - **Porta HTTPS**: `edgeencryption.proxy.https.port`
7. O servidor proxy encaminha a resposta para o balanceador de carga com o cabeçalho do local apontando para a porta do servidor proxy.

O resultado depende de o balanceador de carga e os servidores proxy estarem usando a mesma porta.

- Se o balanceador de carga e os servidores proxy estiverem usando a mesma porta, a solicitação será bem-sucedida porque o usuário receberá a resposta da mesma porta identificada no cabeçalho de resposta.
- Se o balanceador de carga e os servidores proxy estiverem usando portas diferentes, a solicitação falhará porque o navegador do usuário se comunicará somente com o balanceador de carga, mas a resposta estará no servidor proxy.

Solução

O problema poderia ser resolvido simplesmente usando o balanceador de carga e todos os servidores proxy do Edge na mesma porta, mas essa não é a solução ideal. Uma solução melhor seria habilitar o sistema para identificar qual porta o balanceador de carga usa.

As propriedades a seguir permitem que o servidor proxy do Edge redirecione as mensagens de resposta para o balanceador de carga se o servidor proxy e o balanceador de carga estiverem usando portas diferentes.

- *`edgeencryption.proxy.rewrite.location.host`* especifica o nome do host usado para acessar a ServiceNow por meio do balanceador de carga.
- *`edgeencryption.proxy.rewrite.location.https.port`* especifica a porta HTTPS usada para acessar a ServiceNow por meio do balanceador de carga.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configurar o balanceador de carga

Se o balanceador de carga e os servidores proxy estiverem usando portas diferentes, especifique o nome do host e a porta HTTPS do balanceador de carga para permitir que os usuários exibam respostas em seus navegadores.

Antes de Iniciar

Funções necessárias:

- administrador local ou de domínio em um host do Windows
- usuário do serviço com acesso total ao sistema de arquivos em um host Linux

Procedimento

1. Faça login no host do servidor proxy como administrador, administrador de domínio ou usuário do serviço.
2. Navegue até o diretório de instalação do proxy do Edge e selecione `conf/edgeencryption.properties`.
3. Configure as seguintes propriedades:

Propriedade	Descrição
edgeencryption.proxy.rewrite.location.host	Se sua configuração do Edge incluir um balanceador de carga para balancear a carga entre os servidores proxy, as respostas serão reescritas no balanceador de carga para que as solicitações possam ser concluídas. ◦ Se houver um balanceador de carga na configuração do proxy, especifique o nome do host usado para acessar a ServiceNow por meio do balanceador de carga. ◦ Opcional: se não houver nenhum balanceador de carga na configuração do proxy, você poderá definir este valor como o nome do host usado pelo servidor proxy.
edgeencryption.proxy.rewrite.location.https.port	Se sua configuração do Edge incluir um balanceador de carga para balancear a carga entre os servidores proxy, especifica a porta HTTPS usada para acessar a ServiceNow por meio do balanceador de carga. ◦ Se houver um balanceador de carga na configuração, especifique a porta HTTPS usada para acessar a ServiceNow por meio do balanceador de carga. ◦ Opcional: se não houver nenhum balanceador de carga na configuração

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Propriedade	Descrição
	do proxy, você poderá configurar este valor como a porta HTTPS usada pelo servidor proxy.

4. Salve o arquivo.

Resultados
As solicitações podem ser concluídas porque os usuários agora podem exibir as respostas em seus navegadores.

Atualizando o Edge Encryption

Os upgrades de instância e de servidor proxy exigem consideração especial em um ambiente Edge Encryption.

Upgrades de instância

Upgrades de instância em um ambiente Edge Encryption exigem cuidado para garantir que os controles de borda funcionem corretamente após o upgrade da instância.

Durante um upgrade de instância, não adicione, edite ou exclua:

- Configurações do Edge Encryption
- Regras do Edge Encryption
- Padrões de tokenização do Edge Encryption
- Trabalhos agendados do Edge Encryption
- Configurações-chave do Edge Encryption
- Upgrades programados do Edge Encryption
- Configurações de IP da lista de proibições do Edge Encryption

Qualquer trabalho agendado em execução durante o upgrade da instância não será concluído. Para concluir o trabalho interrompido, execute-o novamente depois que a instância for atualizada. Ao reprogramar o trabalho, o processamento que ocorreu antes do upgrade da instância não é perdido e o trabalho continua a processar somente os dados que ainda não foram processados.

Upgrades do servidor proxy

Programe um upgrade de proxy para permitir que a instância atualize o servidor proxy Edge Encryption ou atualize manualmente o servidor proxy a qualquer momento.

⚠ **Aviso:** Para um upgrade no Windows, você pode encontrar problemas de bloqueio de arquivo e o upgrade pode falhar. Para que o upgrade seja bem-sucedido, não deixe nenhum arquivo aberto no diretório de instalação. Além disso, não deve haver nenhum shell no diretório de instalação. Em especial, se você iniciar o proxy na linha de comando (via `bin\edgeencryption.bat install/start`) enquanto estiver no diretório de instalação, feche esse shell ou remova-o do diretório de instalação posteriormente. Nenhum arquivo no diretório de instalação deve ser aberto por um editor ou por qualquer outra aplicação.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Bibliotecas de terceiros

Bibliotecas de terceiros, como a Gemalto, serão perdidas durante os upgrades de servidor proxy e de instância se forem mantidas no mesmo diretório. Para evitar a perda de bibliotecas de terceiros durante os upgrades, você pode:

1. Adicionar manualmente a seguinte propriedade a "edgeencryption.properties":

   ```
   edgeencryption.ekm.provider.classname =
   com.snc.edgeencryption.encryption.CloudEdgeNaeKeyProvider
   ```

2. Adicionar a propriedade de local da biblioteca do fornecedor *`edgeencryption.thirdparty.vendor.library.path`* e a definir como `/path/to/jars`.

   Por exemplo:

   ```
   edgeencryption.thirdparty.vendor.library.path = /app/servicenow/libs
   ```

3. Copie os JARs da SafeNet para esse caminho.

Depois de instalar as bibliotecas de terceiros fora da instalação Edge Encryption, elas não serão mais perdidas durante os upgrades.

Upgrades programados

Importante: Durante os upgrades da Instância ServiceNow, atualize também a versão do seu servidor proxy para se alinhar com a versão da instância e reduzir o risco de problemas de compatibilidade.

Programe um upgrade para permitir que a instância atualize o servidor proxy no horário programado. Esta funcionalidade estará disponível por padrão após a atualização. Um upgrade programado inclui os seguintes eventos:

1. O servidor proxy verifica com a instância para ver se há uma nova versão disponível para upgrade. Novas versões geralmente se tornam disponíveis quando a instância recebe upgrade.
2. O administrador recebe uma notificação ao fazer login quando uma nova versão do servidor proxy está disponível.
3. O administrador pode Programar um upgrade do servidor proxy do Edge Encryption para cada servidor proxy.

   Nota: Somente usuários com a função "security_admin" podem criar uma programação de upgrade por meio do servidor proxy.

4. Depois que o upgrade é programado, o servidor proxy recebe upgrade automaticamente no horário programado. Durante o upgrade, o servidor proxy fica off-line por apenas um curto período de tempo.

   Nota: Como o servidor proxy é reiniciado durante o upgrade, ele fica off-line por um curto período de tempo. A duração é determinada pelo seu ambiente e quanto tempo leva para parar e reiniciar o serviço de proxy.

5. Durante o upgrade programado, um novo diretório de proxy é criado, seus arquivos de configuração são copiados para ele e novas propriedades são gravadas no arquivo de propriedades existente. Os seguintes arquivos ou diretórios no seu diretório de proxy antigo são copiados para o novo diretório de proxy.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Diretório `/conf`
- Diretório `/keys`
- Diretório `/keystore`
- Arquivo `java/jre/lib/security/cacerts`

Como resultado, suas chaves, armazenamentos de chaves, configurações e certificados serão preservados.

Nota: Somente os arquivos acima são copiados para o novo diretório de proxy. Quaisquer outros arquivos personalizados no diretório do servidor proxy não são preservados durante um upgrade programado. O arquivo de log de atualização pode ser encontrado no diretório do proxy original na seguinte pasta: `<original-proxy-directory>/tmp/upgrade-wrapper/bin`.

Pré-requisitos para upgrades programados

Antes de programar um upgrade para um proxy de Edge Encryption, verifique o seguinte:

1. A variável de ambiente *JAVA_HOME* aponta para uma instalação Java na máquina que está fora da estrutura de diretórios do proxy de Edge Encryption.
2. A variável de ambiente *JAVA_HOME* aponta para uma instalação do java que está na versão 1.8_u144 ou superior.
3. O parâmetro *-Djava.io.tmpdir* no arquivo "wrapper.conf" do proxy de Edge Encryption aponta para um diretório que está FORA da estrutura de diretórios do proxy de Edge Encryption e o proxy tem permissões de leitura/gravação/execução no diretório. Como opção, você pode comentar todo o parâmetro para que o Java use a localização tmp padrão.

Upgrades manuais

Em vez de criar uma programação de upgrade, você pode fazer o upgrade manualmente cada servidor proxy por meio da linha de comando. Consulte Upgrade manual de um servidor proxy de Edge Encryption em execução no Linux ou Upgrade manual de um servidor proxy de Edge Encryption em execução no Windows.

Status de compilação de proxy

Você pode identificar facilmente se um servidor proxy está desatualizado navegando até **Configuração de Edge Encryption** > **Proxies** > **Todos**. O status da compilação de proxy é indicado na coluna **Compilação de proxy** pelas seguintes cores:

Verde

Seu servidor proxy está atualizado.

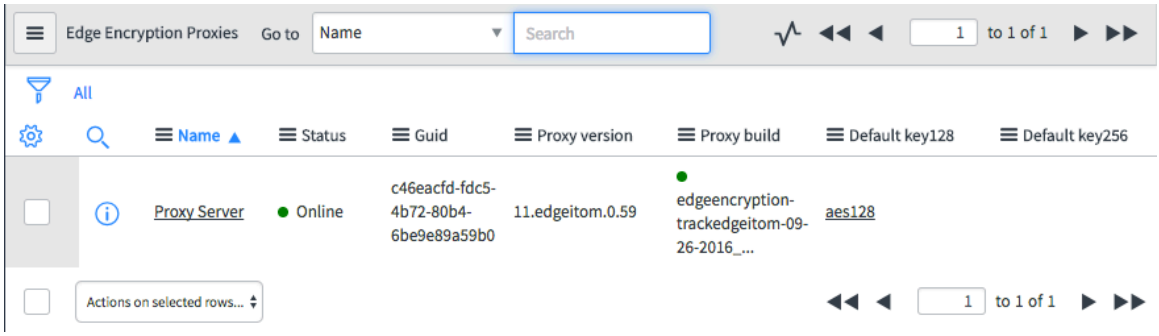
Amarelo

Seu servidor proxy está desatualizado e um upgrade é necessário.

Laranja

Falha no upgrade. O servidor proxy será revertido para a versão antiga para garantir que não haja tempo de inatividade.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Como solucionar problemas de falha no upgrade programado de proxy

Quando um upgrade programado de proxy falha, o servidor proxy é revertido para a versão que você possuía até o momento. Todos os dados, chaves e arquivos de configuração originais são preservados. Esse processo pode levar vários minutos. Entre em contato com Suporte e atendimento ao cliente para garantir um upgrade bem-sucedido.

Para determinar o motivo da falha, você pode verificar o **Motivo da falha** na programação de upgrade. Além disso, o diretório de instalação do upgrade com falha é mantido para que os arquivos de log estejam disponíveis para solução de problemas.

Nota: Antes de excluir qualquer diretório de proxy extra, sempre confirme qual diretório é o atual ao revisar os arquivos de log. Se os arquivos de log tiveram atividade recente, o proxy poderá estar conectado à sua instância.

Se um upgrade programado de proxy falhar repetidamente, você poderá atualizar seu servidor proxy manualmente. Consulte Upgrade manual de um servidor proxy de Edge Encryption em execução no Linux e Upgrade manual de um servidor proxy de Edge Encryption em execução no Windows.

Requisitos mínimos de Java

A máquina host que instala ou executa o servidor proxy Edge Encryption deve manter uma versão compatível do Java. As versões atualmente compatíveis são Java 11.0.6 ou posterior na série da versão 11.x

Nota: O Java 8 não será mais compatível a partir da versão Utah. Faça o upgrade do seu ambiente com o proxy Edge Encryption para Java 11 antes de tentar instalar a versão Utah do proxy Edge Encryption.

Se estiver usando a criptografia AES de 256 bits com o Java 8 atualização 141 (8u141) ou inferior, você deverá instalar os arquivos de política de jurisdição da Extensão de Criptografia Java (JCE), copiando-os no diretório inicial do Java do sistema de cada host do servidor proxy Edge Encryption. Adicione esses arquivos à pasta `<Java-home-directory>/jre/lib/security` antes de executar um upgrade programado ou manual. Para instalar os arquivos de política de criptografia do AES de 256 bits, consulte Configurar a chave de criptografia AES de 256 bits.

Ambientes com versões de proxy mistas

Embora não seja recomendado um ambiente que execute versões antigas e atualizadas do servidor proxy, ele será compatível se todos os servidores proxy estiverem na mesma família de versões da sua instância. Por exemplo, se você tiver uma instância na versão Xanadu, seu ambiente oferecerá suporte a servidores proxy de qualquer patch Xanadu ou hot fix. No entanto, as seguintes limitações se aplicam:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Se um servidor proxy oferecer suporte a uma funcionalidade que outro não oferece, você verá um comportamento inconsistente, dependendo de qual servidor proxy é usado.
- Se um servidor proxy estiver desatualizado, ele pode não incluir melhorias de segurança recentes.

Se um servidor proxy de uma versão anterior estiver registrado com uma versão mais recente da instância, você receberá notificações regulares de que o servidor proxy está desatualizado. Para garantir um ambiente ideal e seguro, ServiceNow recomenda sempre atualizar seu servidor proxy para a versão mais recente do software compatível com sua instância.

Como programar um upgrade do servidor proxy do Edge Encryption

Crie uma programação de upgrade para permitir que a instância atualize um servidor proxy desatualizado.

Antes de Iniciar

Para programar um upgrade, você deve estar conectado à sua instância por meio do servidor proxy.
Se estiver usando a criptografia AES de 256 bits com o Java 8 atualização 141 (8u141) ou inferior, você deverá instalar os arquivos de política de jurisdição da Extensão de Criptografia Java (JCE), copiando-os no diretório inicial do Java do sistema de cada host do servidor proxy Edge Encryption. Adicione esses arquivos à pasta `<Java-home-directory>/jre/lib/security` antes de executar um upgrade programado ou manual. Para instalar os arquivos de política de criptografia do AES de 256 bits, consulte Configurar a chave de criptografia AES de 256 bits.

Função necessária: security_admin

Por Que e Quando Desempenhar Esta Tarefa

Depois que o upgrade é programado, o servidor proxy é atualizado automaticamente no horário programado. Durante o upgrade, o servidor proxy fica off-line por apenas um curto período de tempo.

Nota: Como o servidor proxy é reiniciado durante o upgrade, ele fica off-line por um curto período de tempo. A duração é determinada pelo seu ambiente e quanto tempo leva para parar e reiniciar o serviço de proxy.

Durante o upgrade programado, um novo diretório de proxy é criado, seus arquivos de configuração são copiados para ele e novas propriedades são gravadas no arquivo de propriedades existente. Os seguintes arquivos ou diretórios no seu diretório de proxy antigo são copiados para o novo diretório de proxy.

- Diretório `/conf`
- Diretório `/keys`
- Diretório `/keystore`
- Arquivo `java/jre/lib/security/cacerts`

Como resultado, suas chaves, armazenamentos de chaves, configurações e certificados serão preservados.

Nota: Somente os arquivos acima são copiados para o novo diretório de proxy. Quaisquer outros arquivos personalizados no diretório do servidor proxy não serão preservados durante um upgrade programado. O arquivo de log de upgrade pode ser encontrado no diretório do proxy original na seguinte pasta: `<original-proxy-directory>/tmp/upgrade-wrapper/bin`.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Se vários servidores proxy estiverem desatualizados, você deverá programar um upgrade para cada servidor proxy individualmente.

Nota: Evite hospedar vários servidores proxy na mesma máquina. No entanto, se o seu ambiente incluir esta configuração, não programe upgrades para vários proxies ao mesmo tempo na mesma máquina.

Procedimento

1. Navegue até **Todos** > **Configuração do Edge Encryption** > **Proxies** > **Cronogramas de upgrades**.
2. Clique em **Nova**.
3. Preencha o formulário.

Formulário de programação de upgrade do proxy do Edge Encryption

Campo	Descrição
Servidor proxy	O servidor proxy que receberá upgrade.
Versão de destino	Versão para a qual você está atualizando seu servidor proxy. Este valor é somente leitura e está definido como a versão de proxy mais atualizada disponível para sua instância.
Hora de início programada	Data e hora de início do upgrade.
Ativo	Se o upgrade programado está ativo. Se este campo não for selecionado, o upgrade não será executado na data e hora programadas.
Status	O status do upgrade. Este valor é somente leitura. Os possíveis status incluem: ◦ Pendente ◦ Em execução ◦ Concluído ◦ Reprovado

4. Clique em **Enviar**.

O que Fazer Depois

O tempo normal para um upgrade é inferior a 15 minutos. Depois que um upgrade é executado, você pode ver os detalhes da atualização para saber mais sobre ele. Se o upgrade falhar, analise o **Motivo da falha** para determinar as próximas etapas.

Detalhes do upgrade

Campo	Descrição
Versão de origem	A versão que o servidor tinha até o momento do upgrade.
Versão de destino	A versão para a qual o servidor recebeu upgrade.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Detalhes do upgrade

Campo	Descrição
Hora de início real	Hora em que o upgrade começar.
Hora de término	Hora em que o upgrade terminar.
Motivo da falha	Motivo da falha no upgrade.

Upgrade manual de um servidor proxy de Edge Encryption em execução no Linux

Atualize um proxy em execução no Linux.

Antes de Iniciar

Se estiver usando a criptografia AES de 256 bits com o Java 8 atualização 141 (8u141) ou inferior, você deverá instalar os arquivos de política de jurisdição da Extensão de Criptografia Java (JCE), copiando-os no diretório inicial do Java do sistema de cada host do servidor proxy Edge Encryption. Adicione esses arquivos à pasta `<Java-home-directory>/jre/lib/security` antes de executar um upgrade programado ou manual. Para instalar os arquivos de política de criptografia do AES de 256 bits, consulte Configurar a chave de criptografia AES de 256 bits.

Função necessária: security_admin ou administrador local na máquina do host

Procedimento

1. Baixe o arquivo de atualização do proxy do Edge Encryption para o diretório de instalação.
   a. Navegue até **Configuração de Edge Encryption** > **Instalação e downloads** > **Downloads**
   b. Selecione o link **Baixar o instalador de linha de comando**.
   c. Quando o download começar, selecione o diretório de instalação como o local de download.
2. Mude para o diretório de instalação.
3. Execute o seguinte comando:

```
java -jar edgeencryption-dist-<version>-linux-x86-64.jar -m dist-upgrade
-c <proxy directory>
```

Opção	Descrição
diretório de proxy	O diretório no diretório de instalação em que o proxy foi instalado inicialmente. Este diretório é criado pela instalação.

Se deseja ver a tela de ajuda, execute este comando sem argumentos: `java -jar edgeencryption-dist-<version>-linux-x86-64.jar`

Um novo diretório de proxy é criado com um carimbo de data/hora atual. Um backup do diretório de proxy antigo é mantido como "backup.dist-upgrade_timestamp" no novo diretório de instalação do proxy. O proxy antigo é encerrado e o novo é inicializado. Todas as conexões/transações abertas no servidor proxy antigo são encerradas.

4. Verifique o log do proxy no novo diretório e a instância para confirmar se o novo proxy está em execução.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Upgrade manual de um servidor proxy de Edge Encryption em execução no Windows

Atualize um proxy em execução no Windows.

Antes de Iniciar

Se estiver usando a criptografia AES de 256 bits com o Java 8 atualização 141 (8u141) ou inferior, você deverá instalar os arquivos de política de jurisdição da Extensão de Criptografia Java (JCE), copiando-os no diretório inicial do Java do sistema de cada host do servidor proxy Edge Encryption. Adicione esses arquivos à pasta `<Java-home-directory>/jre/lib/security` antes de executar um upgrade programado ou manual. Para instalar os arquivos de política de criptografia do AES de 256 bits, consulte Configurar a chave de criptografia AES de 256 bits.

Função necessária: security_admin ou administrador local na máquina do host

Procedimento

1. Baixe o arquivo de atualização do proxy do Edge Encryption para o diretório de instalação.
   a. Navegue até **Configuração de Edge Encryption** > **Instalação e downloads** > **Downloads**
   b. Selecione o link **Baixar o instalador de linha de comando**.
   c. Quando o download começar, selecione o diretório de instalação como o local de download.
2. Inicie o programa de terminal "cmd" do Windows com privilégios de administrador.
3. Mude para o diretório de instalação.
4. Execute o seguinte comando:

```
java -jar edgeencryption-dist-<version>-all.jar -m dist-upgrade -c <proxy directory>
```

Opção	Descrição
diretório de proxy	O diretório no diretório de instalação em que o proxy foi instalado inicialmente. Este diretório é criado pela instalação.

Se deseja ver a tela de ajuda, execute este comando sem argumentos: `java -jar edgeencryption-dist-<version>-all.jar`

Um novo diretório de proxy é criado com um carimbo de data/hora atual. Um backup do diretório de proxy antigo é mantido como "backup.dist-upgrade_timestamp" no novo diretório de instalação do proxy. O proxy antigo é encerrado e o novo é inicializado. Todas as conexões/transações abertas no servidor proxy antigo são encerradas.

5. Verifique o log do proxy no novo diretório e a instância para confirmar se o proxy foi atualizado e está em execução.

Como reverter um upgrade do servidor proxy do Edge Encryption

Se um upgrade de proxy não for bem-sucedida, você poderá reverter para a versão anterior.

Antes de Iniciar

Função necessária: administrador

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

Se um upgrade falhar ao usar o recurso de upgrade programado na versão Xanadu, o servidor proxy reverterá automaticamente para a versão antiga. O servidor proxy antigo é armazenado sem modificações em um diretório de backup.

Se você quiser reverter um upgrade manual, siga estas etapas.

Procedimento

1. Encerre o proxy.
2. Exclua o novo diretório de proxy.
3. Renomeie o diretório de backup para o nome do proxy.
   O diretório de backup estará no diretório de instalação do proxy com o nome `<proxy name>_backup`
4. Inicie o proxy.
5. Verifique o log do proxy e a instância para confirmar se o proxy está on-line.

Configurando o Edge Encryption

Depois que o servidor proxy Edge Encryption estiver instalado e em execução, gerencie o Edge Encryption por meio do servidor proxy.

Você deve concluir todas as etapas de Instalando o Edge Encryption antes de criar configurações de criptografia e padrões de criptografia na instância.

Nota: Para acessar a configuração Edge Encryption, você deve fazer login por meio do servidor proxy e elevar para a função "security_admin".

Rotação de chaves de criptografia

Execute a rotação da chave de criptografia da instância. Adicione uma nova chave, mude a atribuição de chave padrão e programe uma rotação de chave em massa ou uma rotação de chave única.

Antes de definir uma chave de criptografia como a chave padrão, disponibilize-a para cada proxy. Isso garante que os proxies tenham a chave para criptografar dados quando ela for atribuída como padrão. Todos os proxies devem ter acesso a uma chave antes de ela ser atribuída como padrão.

Aviso: Antes de excluir uma chave do proxy, configure e execute um trabalho de rotação de chave em massa para garantir que nenhum dado na instância a use. Se alguma informação ainda estiver criptografada com essa chave, você não poderá descriptografar as informações depois de exclui-la.

Comportamento de classificação e filtragem de borda

Sempre que mudar as chaves padrão, certifique-se de executar uma rotação de chave (seja em massa ou única). Caso contrário, você poderá receber resultados inesperados ao classificar e filtrar registros. Como exemplo, considere o seguinte cenário:

1. Você cria registros criptografados usando uma chave de criptografia.
2. Você cria uma nova chave e a define como padrão.
3. Você cria um novo conjunto de registros criptografados usando a nova chave de criptografia.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Se filtrar por qualquer campo criptografado quando conectado por meio do proxy do Edge, todos os registros podem não ser filtrados corretamente ou podem aparecer inesperadamente. O filtro funciona somente para registros criptografados usando a chave padrão atual. Os registros criptografados usando a chave padrão anterior ainda aparecem na exibição de lista.

Se classificar por qualquer campo criptografado quando conectado por meio do proxy do Edge, você verá dois grupos de registros com o mesmo texto legível no campo criptografado.

Programação de trabalho de rotação de chave única

Programe um trabalho para localizar dados criptografados usando um alias de chave especificado e, em seguida, criptografar novamente os dados com a chave de criptografia padrão atual. Os dados são descriptografados antes de serem criptografados novamente com a chave padrão.

Antes de Iniciar

Função necessária: security_admin
Antes de programar este trabalho, atualize a chave padrão em **Configuração de Edge Encryption** > **Configuração de chave de criptografia** > **Definir Chaves Padrão**.

Procedimento

1. Navegue até **Configuração de Edge Encryption** > **Manutenção** > **Programar rotação de chave única**.
2. Preencha os campos do formulário, conforme apropriado.

Campo	Valor
Nome	Insira um nome descritivo.
Tipo de trabalho	Selecionar **Rotação de chave única**.
Chave	Insira a chave a ser descontinuada. Verifique se ela não será mais a chave padrão em **Configuração de Edge Encryption** > **Configuração de chave de criptografia** > **Definir chaves padrão**.
Estimar contagem de registros	Número estimado total de registros para processar. Indisponível ao executar uma rotação de chave única.
Processar registros históricos	Selecione para processar registros históricos na tabela Auditoria se o campo for auditado. Ao criptografar registros históricos para um campo na tabela Auditoria, os valores novos e antigos serão criptografados. Este campo é somente leitura e ativo. Para saber mais sobre os campos auditados, consulte Auditoria.
Estimar a contagem máxima de registros de auditoria	Número estimado máximo de registros auditados para processar. Indisponível ao executar uma rotação de chave única.
Ativo	Desmarque esta caixa de seleção se quiser desativar esse trabalho.
Executar	Selecione o período entre as execuções do trabalho.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Valor
Início	Insira a data e a hora para executar o trabalho pela primeira vez.

3. Clique no ícone de menu no cabeçalho do formulário e selecione **Salvar**.
   O campo **Estimar contagem de registros** não é compatível ao processar campos auditados.

Programação de trabalho de rotação de chave em massa

Programe um trabalho para localizar dados criptografados com qualquer chave anterior e, em seguida, criptografar novamente os dados com as chaves de criptografia padrão atuais. Os dados são descriptografados antes de serem criptografados novamente com a chave padrão atual.

Antes de Iniciar

Função necessária: security_admin

Procedimento

1. Navegue até **Todos** > **Configuração de Edge Encryption** > **Manutenção** > **Programar rotação de chave em massa**.
2. Preencha os campos do formulário, conforme apropriado.

Campo	Valor
Nome	Insira um nome descritivo.
Tipo de trabalho	Selecionar **Rotação de chave em massa**.
Estimar contagem de registros	Número estimado total de registros para processar. Não disponível ao executar uma rotação de chave em massa.
Processar registros históricos	Selecione para processar registros históricos na tabela Auditoria se o campo for auditado. Ao criptografar registros históricos para um campo na tabela Auditoria, os valores novos e antigos serão criptografados. Este campo é somente leitura e ativo. Para saber mais sobre os campos auditados, consulte Auditoria.
Estimar a contagem máxima de registros de auditoria	Número estimado máximo de registros auditados para processar. Não disponível ao executar uma rotação de chave em massa.
Ativo	Desmarque esta caixa de seleção para desativar esse trabalho.
Executar	Selecione o período entre as execuções do trabalho.
Início	Insira a data e a hora para executar o trabalho pela primeira vez.

3. Clique no ícone de menu no cabeçalho do formulário e selecione **Salvar**.
   O campo **Estimar contagem de registros** não é compatível ao processar campos auditados.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Programação de trabalho de rotação de chave de anexo

Programe um trabalho para localizar anexos criptografados usando um alias de chave especificado e, em seguida, criptografar novamente os anexos com a chave de criptografia padrão atual. Os anexos são descriptografados antes de serem criptografados novamente com a chave padrão.

Antes de Iniciar

Função necessária: security_admin

Procedimento

1. Navegue até **Todos** > **Configuração de Edge Encryption** > **Manutenção** > **Programar rotação de chave de anexo**.
2. Preencha os campos do formulário, conforme apropriado.

Campo	Valor
Nome	Insira um nome descritivo.
Tipo de trabalho	Selecione **Rotação de chave de anexo**
Ativo	Desmarque a marca de seleção se quiser desativar esse trabalho.
Tabela	Selecione uma tabela.
Executar	Selecione o período entre as execuções do trabalho.
Início	Insira a data e a hora para executar o trabalho pela primeira vez.

3. Clique no ícone de menu no cabeçalho do formulário e selecione **Salvar**.
4. Para visualizar uma contagem de registros estimada para ser atualizada, clique em **Contagem de registros estimada**.
5. Para executar o trabalho imediatamente, clique em **Executar agora**.

Como criptografar campos usando configurações de criptografia

Como criptografar campos criando configurações de criptografia.

Para configurar Edge Encryption, você deve estar conectado à instância por meio do proxy. Teste todas as mudanças em uma instância de não produção antes de aplicá-las à instância de produção.

Como definir chaves de criptografia

Depois de configurar um ou mais proxies e configurar uma chave de criptografia padrão, a instância verifica se as chaves estão disponíveis para todos os proxies. Você não pode tornar padrão uma chave de criptografia sem que todos os proxies tenham a chave. Depois que uma chave padrão é definida, você pode criar configurações de criptografia.

Como atribuir campos e anexos a serem criptografados

Atribuir campos e anexos a serem criptografados significa atribuir um tipo de criptografia ao campo ou anexo. Antes de marcar um campo como criptografado, avalie as seguintes questões.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Determine quais recursos do sistema podem ser afetados.
- Examine todos os scripts para uso do campo.
- Faça os ajustes desejados no tamanho do campo. Depois que um campo tiver sido configurado para criptografia, seu tamanho não poderá ser alterado.

Marcar um campo para ser criptografado expande seu tamanho para armazenamento dos dados criptografados. O processo de expansão do tamanho do campo pode levar muito tempo, dependendo do número de registros na tabela.

Suporte de API

O Criptografia em nível de coluna atualiza as APIs `setDisplayValue()` e `setValue()` para que possam inserir dados criptografados de campos criptografados. Ele também permite que `getDisplayValue()` e `getValue()` retornem valores de texto não criptografado.

O script a seguir ilustra essas mudanças de API quando a descrição resumida do incidente é criptografada:

```
var gr = new GlideRecord('incident'); //creates a new incident
gr.setValue('short_description','test123'); //sets the value to test123
var sys_ID = gr.insert(); //inserts the record in the Incident table.
gs.info(gr.getValue('short_description')); //displays the unencrypted
 value
```

Ao usar `getValue()` para obter texto criptografado, o script não retorna mais o texto cifrado. Seu script retorna o texto sem formatação, supondo que o usuário tenha acesso ao módulo criptográfico. Se o usuário não tiver acesso ao módulo criptográfico, `getValue()` retornará o texto cifrado.

Como criar uma configuração de Edge Encryption

Selecione os campos a serem criptografados e identifique o tipo de criptografia.

Antes de Iniciar

Função necessária: security_admin

Procedimento

1. Navegue até **Todos** > **Configuração de Edge Encryption** > **Configurações de criptografia** > **Criar novo**.
2. Preencha o formulário.

Campo	Descrição
Tabela	A tabela que contém o campo a ser criptografado.
Tipo	Se deve criptografar uma coluna de tabela ou anexos para a tabela. Selecionar **Coluna**.
Coluna	O campo a ser criptografado. Aparece somente quando o **Tipo** é **Coluna**. Somente os campos "Cadeia de caracteres", "Data", "Data/Hora", "Registro", "Entrada de registro" e "URL" são compatíveis.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	◦ **Campos "Cadeia de caracteres" e "URL"**: você pode adicionar uma configuração de criptografia a uma tabela primária ou secundária. ◦ **Campos "Data" e "Data/hora"**: você pode adicionar uma configuração de criptografia somente a uma tabela primária. Você não pode adicionar uma nova configuração de criptografia a uma tabela secundária. **Nota:** Dependendo do número de registros afetados pelos campos "Data" e "Data/Hora" que você está criptografando, pode levar alguns minutos para criar a configuração de criptografia. Certifique-se de criar a configuração de criptografia para esses dois campos quando o volume de transação na instância estiver baixo.
Tipo de criptografia	O tipo de criptografia a ser usado.

Nota: Uma combinação específica de tabela e campo pode ter apenas uma configuração ativa por vez.

3. Clique em **Enviar**.

O que Fazer Depois

Depois de adicionar o registro de configuração de criptografia, é possível criar um trabalho de criptografia para criptografar os dados existentes. Se você não executar um trabalho de criptografia, o Edge criptografará os dados existentes na próxima vez em que os dados forem alterados. Para obter detalhes, consulte Como programar um trabalho de criptografia.

Como criar uma configuração de criptografia de variável

Selecione as variáveis do catálogo de serviços serem criptografados e identifique o tipo de criptografia.

Antes de Iniciar

Função necessária: security_admin

Procedimento

1. Navegue até **Todos** > **Configuração do Edge Encryption** > **Configurações de criptografia de variável**.
2. Na lista **Configurações de variável do Edge Encryption**, clique em **Novo**.
3. Preencha o formulário.

Campo	Descrição
Variável	A variável a ser criptografada.
Tipo de criptografia	O tipo de criptografia a ser usado.

4. Clique em **Enviar**.

O que Fazer Depois

Depois de adicionar o registro de configuração de criptografia, é possível criar um trabalho de criptografia para criptografar os dados existentes. Se você não executar um trabalho

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

de criptografia, o Edge criptografará os dados existentes na próxima vez em que os dados forem alterados. Para obter detalhes, consulte Como programar um trabalho de criptografia.

Como desativar uma configuração de criptografia

Depois de configurar anexos de um campo ou de uma tabela a serem criptografados, você pode parar a criptografia desativando a configuração de criptografia. Depois de desativar a criptografia, é possível executar um trabalho de descriptografia para campos ou um trabalho de descriptografia de anexo para remover os dados criptografados da instância.

Antes de Iniciar
Função necessária: security_admin

Por Que e Quando Desempenhar Esta Tarefa

⚠ **Aviso:** Desativar uma configuração de criptografia não exclui o registro de criptografia e o tipo de criptografia não pode ser alterado.

Procedimento

1. Navegue até **Configuração de Edge Encryption** > **Configurações de Edge Encryption** > **Todos**.
   A lista **Configurações de Edge Encryption** será exibida.
2. Clique na configuração de criptografia a ser desativada.
   O formulário **Configuração de Edge Encryption** será exibido.
3. Clique na caixa **Ativo**.
   A caixa **Ativo** ficará desmarcada.
4. Clique em **Atualizar**.
   A lista **Configurações de Edge Encryption** será exibida.

O que Fazer Depois
Você pode executar um trabalho de descriptografia ou de descriptografia de anexo para descriptografar dados na instância. Se você não executar um trabalho, os dados criptografados serão descriptografados na próxima vez em que forem alterados.

Como programar um trabalho de criptografia

É possível programar um trabalho para localizar e criptografar dados não criptografados em um campo especificado ao usar a chave de criptografia padrão configurada para o campo. Se você não criar um trabalho de criptografia após configurar um campo para criptografia, somente os novos valores serão criptografados.

Antes de Iniciar
Função necessária: security_admin

Procedimento

1. Navegue até **Configuração de Edge Encryption** > **Configurações de criptografia** > **Todos** para criar um trabalho para um campo, ou **Configuração de Edge Encryption** > **Configuração de criptografia de variável** para criar um trabalho para uma variável.
2. Clique no campo para o qual você deseja programar um trabalho de criptografia.
3. Em **Links relacionados**, clique em **Programar trabalho de criptografia em massa**.

   O formulário **Trabalho de criptografia programado** é mostrado com todos os campos preenchidos. A parte inferior do formulário mostra registros de quaisquer execuções de trabalho anteriores.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Preencha os campos no formulário, conforme apropriado.

Campo	Valor
Nome	Insira um nome descritivo.
Ativo	Desmarque esta caixa de seleção se quiser desativar esse trabalho.
Tipo de trabalho	Selecione **Criptografia**.
Tabela	Selecione uma tabela.
Coluna	Selecione uma coluna.
Contagem de registro estimada	Número estimado total de registros para processar. Preenche depois de selecionar **Estimar a contagem de registros**.
Processar registros históricos	Selecione para processar registros históricos na tabela Auditoria se o campo for auditado. Ao criptografar registros históricos para um campo na tabela Auditoria, os valores novos e antigos serão criptografados. Para saber mais sobre os campos auditados, consulte Auditoria.
Estimar a contagem máxima de registros de auditoria	Número estimado máximo de registros auditados para processar. Preenche depois de selecionar **Estimar a contagem de registros**. Este campo só fica visível quando **Processar registros históricos** for selecionado. **Nota:** A estimativa pode ser maior do que o número real de registros processados.
Executar	Selecione o período entre as execuções do trabalho.
Início	Insira a data e a hora para executar o trabalho pela primeira vez.

5. Clique no ícone de menu no cabeçalho do formulário e selecione **Salvar**.
6. Para visualizar uma contagem de registros estimada para ser atualizada, clique em **Estimar contagem de registros**.
7. Para executar o trabalho imediatamente, clique em **Executar agora**.

Como programar um trabalho de descriptografia

Você pode programar um trabalho para descriptografar dados em um campo criptografado para armazenar dados limpos na instância.

Antes de Iniciar

Nota: Você deve marcar o registro de criptografia como inativo para o campo (desmarque a caixa **Ativo**) para executar o trabalho de descriptografia.

Função necessária: security_admin

Procedimento

1. Navegue até **Configuração de Edge Encryption** > **Configurações de criptografia** > **Todos** para criar um trabalho para um campo, ou **Configuração de Edge Encryption** > **Configuração de criptografia de variável** para criar um trabalho para uma variável.
2. Clique no campo que você deseja descriptografar.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Em **Links relacionados**, clique em **Programar trabalho de descriptografia em massa**.

   O formulário **Trabalho de criptografia programado** é mostrado com todos os campos preenchidos. A parte inferior do formulário mostra os registros de execuções de trabalho anteriores.

4. Preencha os campos no formulário, conforme apropriado.

Campo	Valor
Nome	Insira um nome descritivo.
Tipo de trabalho	Selecione **Descriptografia**.
Ativo	Desmarque esta caixa de seleção se quiser desativar esse trabalho.
Tabela	Selecione uma tabela.
Coluna	Selecione uma coluna.
Contagem de registro estimada	Número estimado total de registros para processar. Preenche depois de selecionar **Estimar a contagem de registros**.
Processar registros históricos	Selecione para processar registros históricos na tabela Auditoria se o campo for auditado. Ao criptografar registros históricos para um campo na tabela Auditoria, os valores novos e antigos serão criptografados. Para saber mais sobre os campos auditados, consulte Auditoria.
Estimar a contagem máxima de registros de auditoria	Número estimado máximo de registros auditados para processar. Preenche depois de selecionar **Estimar a contagem de registros**. Este campo só fica visível quando **Processar registros históricos** for selecionado. **Nota:** A estimativa pode ser maior do que o número real de registros processados.
Executar	Selecione o período entre as execuções do trabalho.
Início	Insira a data e a hora para executar o trabalho pela primeira vez.

5. Clique no ícone de menu no cabeçalho do formulário e selecione **Salvar**.
6. Para visualizar uma contagem de registros estimada para ser atualizada, clique em **Estimar contagem de registros**.
7. Para executar o trabalho imediatamente, clique em **Executar agora**.

Como criptografar anexos usando criptografia padrão

Você pode criptografar anexos para tabelas específicas.

Todos os anexos de uma tabela usam o mesmo tipo de criptografia. Os anexos criptografados não são pesquisados ao executar uma pesquisa de texto. Somente os tipos de criptografia padrão são permitidos para anexos. Os tipos de criptografia com preservação de pedido ou de igualdade não são permitidos.

Para uma sessão ignorar o proxy Edge Encryption :

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Em um registro com criptografia de anexo ativada:
  - O usuário pode ver que há anexos e os nomes dos anexos.
  - O usuário não pode adicionar novos anexos.
- Em um registro sem criptografia de anexo ativada:
  - O usuário pode abrir e baixar anexos existentes.
  - O usuário pode adicionar novos anexos.

Para uma sessão usando o proxy de criptografia, o usuário pode abrir e baixar anexos existentes e adicionar novos anexos.

Como configurar criptografia de anexo

Selecione as tabelas cujos anexos serão criptografados e identifique o tipo de criptografia.

Antes de Iniciar

Função necessária: security_admin

Procedimento

1. Navegue até **Todos** > **Configuração de Edge Encryption** > **Configurações de Edge Encryption** > **Criar novo**.
2. Preencha os campos no formulário, conforme apropriado.

Configuração de Edge Encryption

Campo	Descrição
Tabela	Selecione uma tabela cujos anexos serão criptografados.
Tipo	Se deve criptografar uma coluna de tabela ou anexos para a tabela. Selecionar **Anexo**.
Coluna	O campo da tabela a ser criptografado. Este campo aparece quando o **Tipo** é **Coluna**e não quando o **Tipo** é **Anexo**.
Tipo de criptografia	O tipo de criptografia a ser usado. Para anexos, somente o padrão AES128 e o padrão AES256 são permitidos.

3. Clique em **Enviar**.

O que Fazer Depois

Depois que o registro de criptografia for adicionado, você poderá criar um trabalho de criptografia de anexo para criptografar os anexos existentes. Se não executar esse trabalho, o sistema criptografará novos anexos quando você os anexar.

Nota: Se você marcar o *atributo edge_encryption_clear_attachment_allowed* como **verdadeiro** na entrada do Dicionário de Coleção da tabela, os anexos não criptografados serão adicionados a uma tabela usando o Edge Encryption para criptografar anexos. Se este atributo for habilitado, você deverá configurar um Trabalho de criptografia de anexo para que todos os anexos não criptografados adicionados sejam criptografados.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Como programar um trabalho de criptografia de anexos

É possível programar um trabalho para localizar e criptografar quaisquer anexos não criptografados em uma tabela especificada ao usar a chave de criptografia padrão configurada para a tabela.

Antes de Iniciar

Função necessária: security_admin

Procedimento

1. Navegue até **Configuração de Edge Encryption** > **Configurações de criptografia** > **Todos**.
2. Clique na tabela para a qual você deseja programar um trabalho de criptografia.
3. Em **Links relacionados**, clique em **Programar trabalho de criptografia em massa**.

   O formulário **Trabalho de criptografia programado** é mostrado com todos os campos preenchidos. A parte inferior do formulário mostra os registros de execuções de trabalho anteriores.
4. Preencha os campos no formulário, conforme apropriado.

Campo	Valor
Nome	Insira um nome descritivo.
Ativo	Desmarque esta caixa de seleção se quiser desativar esse trabalho.
Tipo de trabalho	Selecione **Criptografia de anexo**.
Tabela	Selecione uma tabela.
Executar	Selecione o período entre as execuções do trabalho.
Início	Insira a data e a hora para executar o trabalho pela primeira vez.

5. Clique no ícone de menu no cabeçalho do formulário e selecione **Salvar**.
6. Para visualizar uma contagem de registros estimada para ser atualizada, clique em **Estimar contagem de registros**.
7. Para executar o trabalho imediatamente, clique em **Executar agora**.

Como programar um trabalho de descriptografia de anexos

Você pode programar um trabalho para descriptografar quaisquer anexos criptografados de uma tabela especificada para armazenar anexos limpos na instância.

Antes de Iniciar

Nota: Você deve marcar o registro de criptografia da tabela como inativo (desmarque a caixa **Ativo**) antes de executar o trabalho de descriptografia. Caso contrário, nada será executado.

Função necessária: security_admin

Procedimento

1. Navegue até **Configuração de Edge Encryption** > **Configurações de criptografia** > **Todos**.
2. Clique na tabela com os anexos que você deseja descriptografar.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Em **Links relacionados**, clique em **Programar trabalho de descriptografia de anexos em massa**.

   O formulário **Trabalho de criptografia programado** é mostrado com todos os campos preenchidos. A parte inferior do formulário mostra os registros de execuções de trabalho anteriores.

4. Preencha os campos no formulário, conforme apropriado.

Campo	Valor
Nome	Insira um nome descritivo.
Tipo de trabalho	Selecione **Descriptografia de anexo**.
Ativo	Desmarque a marca de seleção se quiser desativar esse trabalho.
Tabela	Selecione uma tabela.
Executar	Selecione o período entre as execuções do trabalho.
Início	Insira a data e a hora para executar o trabalho pela primeira vez.

5. Clique no ícone de menu no cabeçalho do formulário e selecione **Salvar**.
6. Para visualizar uma contagem de registros estimada para ser atualizada, clique em **Estimar contagem de registros**.
7. Para executar o trabalho imediatamente, clique em **Executar agora**.

Como alterar o tipo de criptografia de um campo ou anexo

Você pode alterar o tipo de criptografia de um campo ou anexo selecionando um novo tipo de criptografia no registro de configuração de criptografia existente. Uma combinação específica de tabela e campo pode ter apenas uma configuração ativa por vez.

Antes de Iniciar

Função necessária: security_admin

Procedimento

1. Navegue até **Configuração de Edge Encryption** > **Configurações de criptografia** > **Todos**. A lista **Configurações de Edge Encryption** será exibida.
2. Abra o registro da configuração de criptografia a ser alterada.
3. Clique no menu suspenso **Tipo de criptografia** e selecione um novo tipo de criptografia.

   Nota: Para anexos, somente o padrão AES128 e o padrão AES256 são permitidos.

4. Se necessário, execute um trabalho de criptografia ou de criptografia de anexo.
   Não é necessário executar um trabalho de criptografia. Se você não executá-lo, o campo ou anexo será criptografado usando o novo tipo de criptografia na próxima vez em que o campo ou o anexo for alterado.

Como tokenizar cadeias de caracteres usando padrões de criptografia

Você pode substituir padrões de cadeia de caracteres por tokens antes de serem enviados e armazenados na instância.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Para usar padrões de criptografia, você deve instalar e configurar um banco de dados MySQL na sua rede. Este é o mesmo banco de dados usado para criptografia de preservação de pedido. Para criar ou editar padrões de criptografia, você deve estar conectado à instância por meio do proxy.

Função necessária: security_admin

Por Que e Quando Desempenhar Esta Tarefa

Você pode usar padrões de sistema de base ou criar seus próprios padrões. Os padrões do sistema base são padrões avançados. Os padrões de criptografia incluem as seguintes limitações.

- Não é permitido um padrão de todos os caracteres alfabéticos.
- O tamanho mínimo do padrão é de cinco caracteres. Você pode mudar esta configuração usando uma propriedade do sistema.
- Os quantificadores "*" e "+" são proibidos nos padrões de criptografia.
- Os padrões de criptografia correspondem a palavras completas, não a partes de cadeias de caracteres incorporadas em uma cadeia de caracteres maior. As palavras são definidas por espaços e caracteres não disponíveis para inclusão em um padrão.
- Se a mesma cadeia de caracteres for enviada para a instância várias vezes, ela será substituída pelo mesmo token.
- Há suporte para pesquisa de texto em correspondências exatas. A cadeia de caracteres de consulta é trocada por um token quando enviada para a instância. A pesquisa é realizada em tokens, e quando os resultados da pesquisa forem retornados para o servidor proxy, os tokens serão substituídos pelo texto não criptografado. Recursos como lematização não são compatíveis.

Ao usar padrões, o texto não criptografado nunca sai da rede. Quando o servidor proxy corresponde a um padrão em uma solicitação que vai para a instância, o proxy substitui a cadeia de caracteres por um token do mesmo tamanho. O token é enviado para a instância em vez da cadeia de caracteres de texto não criptografado. Quando a resposta é enviada da instância para o servidor proxy, o proxy substitui o token pela cadeia de caracteres. Quando exibida por meio do servidor proxy, a cadeia de caracteres é exibida como texto não criptografado.

Nota: Campos criptografados não são verificados quanto a padrões de criptografia.

Procedimento

1. Navegue até **Todos** > **Configuração de Edge Encryption** > **Padrões de criptografia** > **Criar novo**.
   Como alternativa, você pode navegar até **Padrões avançados** para ativar ou editar um padrão pré-configurado.
2. Insira o nome do padrão.
3. Defina o **Tipo de entrada de padrão do Edge**.

Opção	Descrição
Básico	Uma série de tipos de caracteres. Na guia **Entrada padrão básica**, clique em **Adicionar** e selecione um tipo de caractere. O **Exemplo de padrão** exibe o padrão conforme os caracteres são adicionados.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	Clique em **Novo bloco** para mover o próximo caractere para a linha seguinte. Isso permite agrupar caracteres em um padrão longo. Clique em **X** para excluir o último caractere do padrão.
Avançado	Uma expressão Java RegEx. Se "avançado" for selecionado, você não poderá mudar o tipo de entrada de volta para "básico". No campo **Exemplo de correspondência**, insira um exemplo de padrão para testar a expressão RegEx. No campo **Padrão**, insira uma expressão Java RegEx. Clique em **Validar** para verificar se a expressão corresponde ao exemplo de padrão.

O tipo de entrada define como você vai inserir o padrão. Não afeta o modo como ele será usado.

4. Clique em **Enviar**.

Como reparar ou recuperar dados criptografados de preservação de pedido

Se você tiver a função de administrador de segurança, poderá programar trabalhos realizados pelo proxy Edge Encryption para reparar ou recuperar campos que usam criptografia de preservação de pedido.

Programar trabalhos para:

- Reparar tokens de pedido.
- Recriar o banco de dados do proxy.

A execução desses trabalhos pode ser uma operação demorada, o que pode afetar o desempenho do proxy Edge Encryption. Programe esses trabalhos em um horário em que nenhum usuário ou um conjunto mínimo de usuários esteja usando o sistema, como à meia-noite no fim de semana.

Como programar um trabalho de reparo de token de pedido

Você pode programar um trabalho para localizar e reparar campos onde o token de pedido está ausente.

Antes de Iniciar
Função necessária: security_admin

Por Que e Quando Desempenhar Esta Tarefa
Use esses trabalhos para reparar campos individuais em uma tabela ou para reparar todos os campos usando a criptografia de preservação de pedido. Execute este trabalho quando o banco de dados do proxy estiver off-line durante a execução da instância, o que resulta em campos de preservação de pedido que não têm tokens de pedido.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegue até **Todos** > **Configuração de Edge Encryption** > **Manutenção** > **Programar reparo de token de pedido**.
2. Preencha os campos no formulário, conforme apropriado.

Campo	Valor
Nome	Insira um nome descritivo.
Tipo de trabalho	Selecione **Reparo de token de pedido**.
Todos os campos	Marque esta caixa de seleção para reparar todas as tabelas.
Tabela	Selecione uma tabela.
Coluna	Selecione uma coluna.
Ativo	Desmarque esta caixa de seleção se quiser desativar esse trabalho.
Executar	Selecione o período entre as execuções do trabalho.
Início	Insira a data e a hora para executar o trabalho pela primeira vez.

3. Clique no ícone de menu no cabeçalho do formulário e selecione **Salvar**.
4. Para visualizar uma contagem de registros estimada para ser atualizada, clique em **Contagem de registros estimada**.

Como programar um trabalho de recuperação de banco de dados do proxy

Execute este trabalho quando o banco de dados do proxy perder dados. Este trabalho encontra todos os registros que foram criptografados com um token (tipo de criptografia de preservação de pedido) e os envia para o proxy para que o banco de dados do proxy possa ser recriado.

Antes de Iniciar

Função necessária: security_admin

Procedimento

1. Navegue até **Todos** > **Configuração de Edge Encryption** > **Manutenção** > **Programar recuperação de banco de dados**.
2. Preencha os campos no formulário, conforme apropriado.

Campo	Valor
Nome	Insira um nome descritivo para este trabalho.
Tipo de trabalho	Selecione **Recuperação de banco de dados**.
Ativo	Desmarque esta caixa de seleção se quiser desativar esse trabalho.
Executar	Selecione o período entre as execuções do trabalho.
Início	Insira a data e a hora para executar este trabalho pela primeira vez.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Clique no ícone de menu no cabeçalho do formulário e selecione **Salvar**.
4. Para visualizar uma contagem de registros estimada para ser atualizada, clique em **Estimar contagem de registros**.

Como configurar a lista de proibições de endereços IP

Impeça que um endereço IP em sua rede envie solicitações para sua instância

Antes de Iniciar

Função necessária: security_admin
Como o servidor proxy Edge Encryption reside em sua rede, ele pode estar sujeito a verificações de vulnerabilidade por parte do software de rede. Para impedir que o scanner IP ou outras solicitações sejam encaminhadas para sua instância ServiceNow, você pode adicionar endereços IP, intervalos de IP ou máscaras de rede a uma lista de proibições. Qualquer conexão com o servidor proxy de um endereço listado como proibição é encerrada e não é encaminhada para sua instância.

Para inserir um endereço IP em uma lista de proibições, você deve logar na sua instância por meio do servidor proxy.

Importante: Certifique-se de compreender a topologia da rede antes de adicionar endereços IP na sua rede a uma lista de proibições. Se um endereço IP for adicionado à lista de proibições, qualquer usuário com esse endereço IP será impedido de acessar o servidor proxy Edge Encryption.

Procedimento

1. Navegue até **Todos** > **Configuração de Edge Encryption** > **Manutenção** > **Endereços IP na lista de proibições**.
   A exibição de lista "Lista de proibições de IP de proxy de criptografia" [edge_encryption_ip_blacklist] é aberta.
2. Clique em **Nova**.
3. Preencha o formulário.

Campo	Descrição
Servidor proxy	O servidor proxy Edge Encryption que está impedido de encaminhar solicitações de endereços na lista de proibições.
IP, intervalo de IPs ou máscara de rede	As solicitações deste endereço IP, intervalo ou máscara de rede não são encaminhadas para sua instância ServiceNow. Os valores de exemplo incluem: ◦ Endereço IP: 10.10.10.5 ◦ Intervalo de IP: 10.10.10.1-15 ◦ Máscara de rede: 10.10.10.0/24 **Nota:** Você pode usar endereços IPv4 ou IPv6
Ativo	Se o registro está ativo. Somente endereços IP de registros ativos são impedidos de enviar solicitações para a instância.
Descrição	Descrição do registro da lista de proibições.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Clique em **Enviar**.
5. Repita essas etapas para todos os outros proxies para os quais um endereço IP deve ser proibido.

Resultados

O servidor proxy Edge Encryption encerra qualquer conexão de endereços IP, intervalos ou máscaras de rede na lista de proibições e não pode encaminhar a solicitação para a instância.

Como criptografar dados de um produtor de registro

Crie regras de criptografia a partir do registro do produtor de registro para configurar o seu servidor proxy Edge Encryption para permitir inserções de um produtor de registro.

Antes de Iniciar

Função necessária: security_admin

Os produtores de registro permitem que os usuários finais criem registros baseados em tarefas, como registros de incidentes, a partir de Catálogo de serviços e de Portal de serviços. Se um produtor de registro tentar inserir dados em um campo marcado para criptografia, uma mensagem de inserção inválida será exibida e os dados não serão salvos no campo.

A criptografia de dados de um produtor de registro requer uma configuração de criptografia definida para o campo de destino. Verifique se você criou uma configuração de criptografia para o campo de destino e a tabela antes de criar uma regra de criptografia de um produtor de registro. Consulte Como criar uma configuração de Edge Encryption. Para criptografar anexos de um produtor de registro, Como configurar criptografia de anexo.

Procedimento

1. Faça login na sua instância por meio do servidor proxy Edge Encryption.
2. Navegue até **Catálogo de serviços** > **Definições do catálogo** > **Produtores de registro**.
3. Criar um produtor de registro ou abrir um registro de produtor de registro existente.
4. Em **Links relacionados**, selecione **Criar regra de Edge Encryption**.
   Duas regras de criptografia inativas são criadas automaticamente para criptografar dados enviados do produtor de registro para o campo marcado para criptografia.

Regra de criptografia	Descrição
<RecordProducerName>	Regra criada para processar parâmetros POST do Catálogo de serviços e mapear variáveis para campos na instância.
<RecordProducerName>Json	Regra criada para processar uma carga JSON do Portal de serviços e mapear variáveis para campos na instância.

5. Ative as regras de criptografia necessárias criadas pelo produtor de registro.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Navegue até **Configuração de Edge Encryption** > **Regras** > **Todos**.

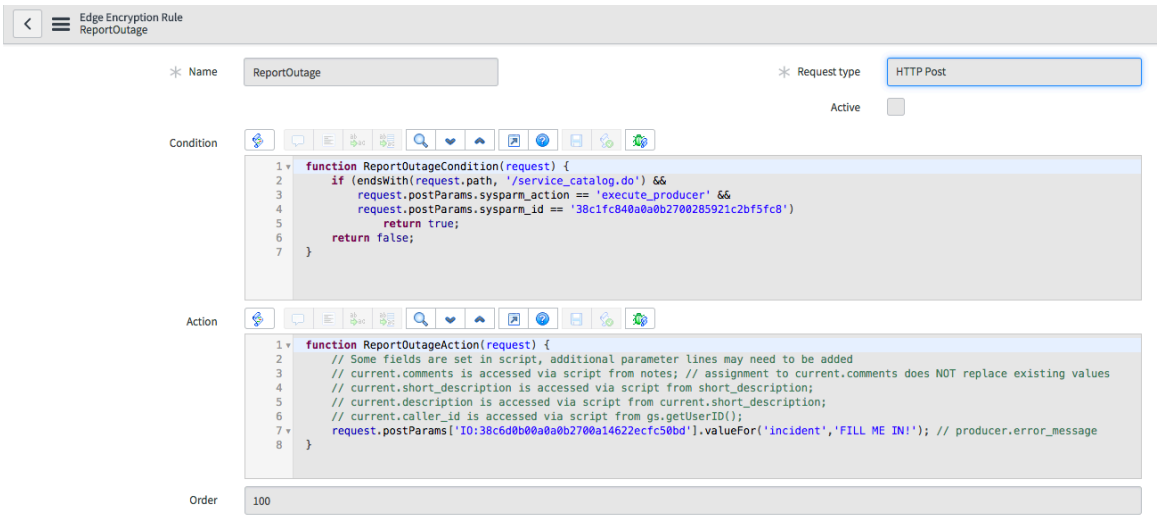
b. Dependendo de onde o produtor de registro será usado, abra a regra de criptografia associada criada pelo produtor de registro e selecione o sinalizador **Ativo**.
Se estiver usando o produtor de registro em Catálogo de serviços, ative a regra de criptografia <RecordProducerName>. Se estiver usando o produtor de registro em Portal de serviços, ative a regra de criptografia <RecordProducerName>Json.

6. Opcional: Examine o campo **Ação** da regra de criptografia e adicione os nomes de campo ou as instruções necessárias.

(Optional) Se um produtor de registro mapeia diretamente uma variável para um campo em uma tabela, a regra de criptografia mapeia automaticamente a variável para o campo correto. No entanto, se uma variável for mapeada indiretamente por meio de vários scripts na plataforma, talvez seja necessário atualizar as regras para mapear cada variável para o campo correto.

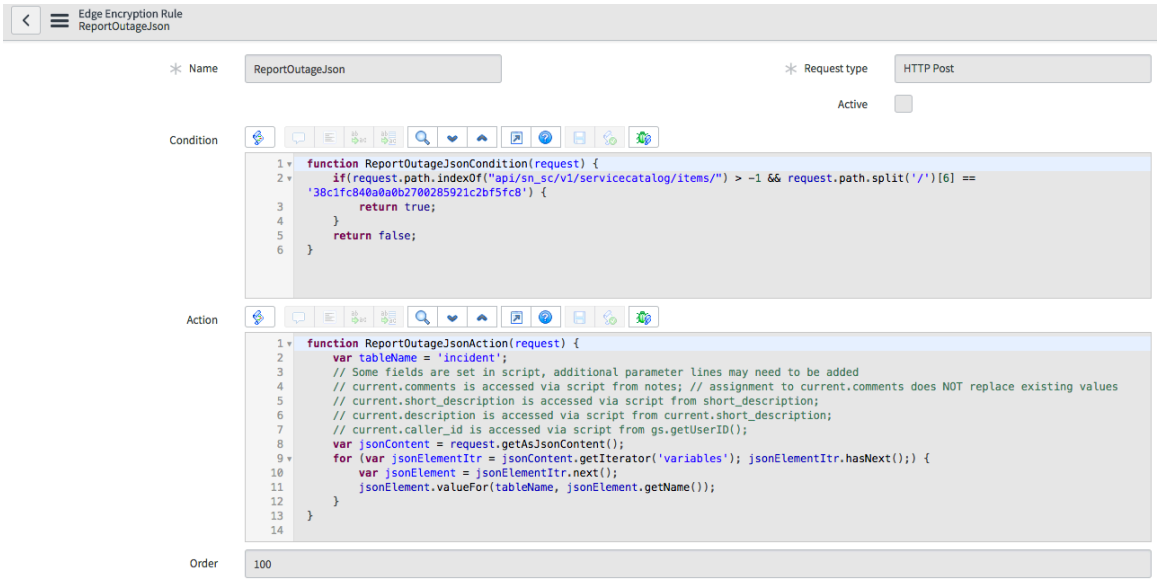
Example

(Optional) A regra de criptografia abaixo foi criada a partir do produtor de registro "Indisponibilidade do relatório" e processa os parâmetros POST do Catálogo de serviços para mapear variáveis para campos na instância. Substitua `"FILL ME IN"` pelo campo de destino.



A regra de criptografia abaixo foi criada a partir do produtor de registro "Indisponibilidade do relatório" e processa uma carga JSON de Portal de serviços para mapear variáveis para campos na instância. Adicione outras instruções para mapear quaisquer variáveis de script para os campos de destino.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Quando a carga do produtor de registro for examinada, o elemento "error_message" irá conter o valor do campo "short_description". Ao adicionar a instrução a seguir, você poderá mapear a variável de script "error_message" para o campo "short_description".

```
if (jsonElement.getName() == 'error_message')
        jsonElement.valueFor(tableName, 'short_description');
```

O valor do campo **Ação** se torna:

```
function ReportOutageJsonAction(request) {
 var tableName = 'incident';
 // Some fields are set in script, additional parameter lines may need
 to be added
 // current.comments is accessed via script from notes; // assignment
 to current.comments does NOT replace existing values
 // current.short_description is accessed via script from
 short_description;
 // current.description is accessed via script from
 current.short_description;
 // current.caller_id is accessed via script from gs.getUserID();
 var jsonContent = request.getAsJsonContent();
 for (var jsonElementItr = jsonContent.getIterator('variables');
 jsonElementItr.hasNext();;) {
  var jsonElement = jsonElementItr.next();
  if (jsonElement.getName() == 'error_message')
   jsonElement.valueFor(tableName, 'short_description');
              } else {
          jsonElement.valueFor(tableName, jsonElement.getName());
 }
}
```

Resultados

As duas regras de criptografia permitem que o produtor de registro insira valores em campos marcados para criptografia do Catálogo de serviços ou do Portal de serviços.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Como definir uma regra de criptografia personalizada

Pode ser necessário identificar e criptografar informações confidenciais em solicitações HTTP no caminho para sua instância. Você pode gravar regras de criptografia para identificar, interpretar e criptografar dados nessas solicitações, mapeando campos na solicitação para nomes de campo de tabela em sua instância.

O que é uma regra de criptografia?

Regras de criptografia são scripts executados no servidor proxy Edge Encryption para mapear campos em uma solicitação para campos em uma tabela em sua instância ServiceNow. Uma regra de criptografia informa ao servidor proxy Edge Encryption como criptografar dados em cargas personalizadas.

Nota: As regras de criptografia são compatíveis somente com o ECMAScript 3 e versões anteriores.

Quando usar regras personalizadas

Um conjunto de regras de criptografia está incluído como parte do plug-in Edge Encryption. Essas regras tratam de muitos casos de uso da plataforma principal, como:

- Editar um campo no formulário de edição de lista
- Atualizar um registro no formulário de registro
- Gerenciar um serviço web direto
- Processar dados da REST API (Application Program Interface, interface de programação de aplicação)

As aplicações criadas usando formulários e listas padrão devem funcionar sem regras de criptografia personalizadas.

Se você desenvolver scripts que contenham dados que devem ser criptografados, crie regras de criptografia para localizar e mapear esses dados para nomes de campo de tabela do Glide. Por exemplo:

- Processadores com script
- Serviços da web com script
- Scripted REST APIs, IUs ou scripts Ajax

Formato de uma regra de criptografia

As regras incluem três partes:

- **Condição**: identifica o tipo de solicitação.
- **Ação**: mapeia campos na solicitação para campos em uma tabela, criptografando valores que são mapeados para campos com configurações de criptografia definidas.
- **Ordem**: prioridade da regra. A regra de prioridade mais baixa com uma condição atendida é a única regra executada. Como as regras de negócios, elas são executadas da menor para a maior.

Com exceção das solicitações de anexo, as solicitações HTTP são avaliadas pelo servidor proxy Edge Encryption. O servidor proxy Edge Encryption avalia todas as condições de regra de criptografia em ordem de prioridade até que todas as condições retornem falsas ou uma condição retorne verdadeira. Quando uma condição retorna verdadeira, a ação é executada na solicitação, e o resultado é encaminhado para a instância. Nenhuma outra

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

condição será avaliada. Como resultado, as condições da regra de criptografia devem ser as mais específicas possível. Uma regra genérica pode ser avaliada como verdadeira para uma solicitação destinada a ser processada por outra regra, fazendo com que a solicitação seja processada pela ação incorreta. Se uma condição genérica for inevitável, a regra deverá ser marcada com um valor de ordem alto para que regras mais específicas sejam avaliadas primeiro.

Diretrizes para criação de regras de criptografia

Criar regras de criptografia eficientes e otimizadas pode reduzir o tempo de processamento para validação de script.

Diretriz geral: quando as regras ficarem longas, faça o possível para minimizar o número de blocos e as divida sempre que possível. O ideal é que as regras personalizadas se apliquem a casos de uso específicos, em vez de abranger vários casos, com instruções `ifs` ou switch no script de ação.

1. Divida as regras sempre que possível. Por exemplo,
   - Crie regras diferentes para tabelas diferentes e certifique-se de que cada regra seja executada somente em sua respectiva tabela.
   - Crie regras diferentes para cada produtor de registro de destino ou pelo menos para cada subconjunto de produtores de registro. Em vez de uma regra direcionada a dezenas de `sys_ids`, você pode criar várias regras diferentes direcionadas a subconjuntos menores de produtores de registro ou até mesmo criar uma regra por `sys_id`.

     Nota: Criar várias regras requer mais manutenção. A vantagem é que várias regras mais simples podem ser validadas com mais eficiência do que regras mais longas e complexas.

2. Minimize o número de blocos. Como o mecanismo de processamento verifica cada bloco ao avaliar os scripts, um grande número de blocos causa atrasos na validação. Por exemplo,
   - Substitua todos os blocos `if` por uma pesquisa de matriz e substitua todos os blocos na pesquisa de matriz por apenas um bloco `if`.
   - Combine os blocos `if` sempre que for possível agrupá-los.

APIs da regra de criptografia

As regras de criptografia são gravadas em JavaScript e utilizam APIs de Edge Encryption para localizar e criptografar informações confidenciais no corpo de uma solicitação. A API usa expressões semelhantes ao xPath para navegar pelo conteúdo JSON e XML.

As APIs de Edge Encryption processam a solicitação fora do fluxo conforme é gravada no fluxo de saída. A análise de fluxo permite que as regras de criptografia tenham um bom desempenho na rede. No entanto, buscar e analisar o conteúdo do corpo várias vezes pode levar a resultados inesperados. Para evitar esse possível problema, as solicitações devem ser processadas pela ação em uma única passagem.

Ao criar regras de criptografia, você não pode usar APIs do Glide, inclusões de script, regras de negócio ou quaisquer parâmetros globais, como *`current`*. Como as regras são criadas para objetos HTTP, um objeto *`request`* global está disponível.

Ao criar regras de criptografia, você não pode usar APIs do gerenciador de lista de permissões ou aplicações com escopo.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tratamento de erros

Se uma condição ou ação de regra de criptografia gerar uma exceção, verifique o log do proxy para obter informações sobre a solução de problemas.

Inspeção da solicitação do cliente

Antes de criar uma regra de criptografia personalizada, você deve determinar o formato da solicitação do cliente que entra no servidor proxy Edge Encryption.

Antes de Iniciar
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa
Como as regras de criptografia iteram nas solicitações do cliente e determinam o que precisa ser criptografado, você deve entender o tipo de solicitação para a qual uma regra está sendo criada. O formato da solicitação do cliente determina a estrutura da regra de criptografia e as APIs disponíveis para uso na regra.

Procedimento

1. Inspecione a solicitação do cliente

   Dependendo da origem da solicitação, as ferramentas a seguir estão disponíveis para inspecionar a solicitação e determinar o formato.

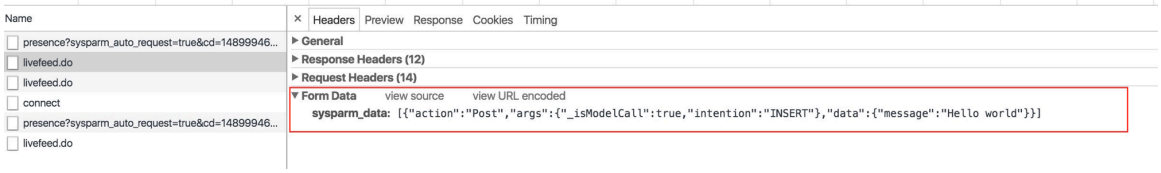
Origem da solicitação	Ferramentas disponíveis
Navegador do cliente	Use o console do desenvolvedor no seu navegador para inspecionar a solicitação do cliente. Ferramentas úteis incluem: ◦ Monitor de rede do Firefox ◦ Painel de rede do Chrome
Fonte externa/de terceiros	Use um analisador de protocolo HTTP para inspecionar a solicitação. Ferramentas úteis incluem: ◦ Wireshark ◦ Obtenção de HTTP Como alternativa, você geralmente pode usar documentação da origem externa para determinar o formato da solicitação.

2. Na solicitação do cliente, inspecione o pacote e determine:
   - O método de solicitação do cliente
   - O caminho do URL da solicitação
   - Os parâmetros de URL

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Os parâmetros POST, se houver
- O formato do corpo da solicitação, se incluído

Example



Resultados

A inspeção da solicitação fornece uma compreensão dos campos que você precisa filtrar e iterar em sua regra de criptografia. Para entender os campos no objeto `request`, consulte Objeto "request".

Criação de uma nova regra de criptografia

Regras de criptografia são usadas pelo proxy para encontrar conteúdo em solicitações HTTP que devem ser criptografadas.

Antes de Iniciar

Função necessária: security_admin
Antes de criar uma regra de criptografia, você deve fazer a Inspeção da solicitação do cliente para determinar o formato.

Por Que e Quando Desempenhar Esta Tarefa

Para criar ou editar regras de criptografia, você deve estar conectado à instância por meio de um proxy de criptografia.

Procedimento

1. Navegue até **Todos** > **Configuração de Edge Encryption** > **Regras** > **Criar novo**.
2. Na caixa **Nome**, insira um nome.
3. Em **Tipo de solicitação**, selecione um método HTTP.
   - **HTTP Post**
   - **HTTP Get**
   - **HTTP Put**
   - **Patch HTTP**
   - **HTTP Delete**

   Nota: As instâncias pré-Jakarta permitem somente os métodos **HTTP Get** e **HTTP Post**.
4. Na caixa **Condição**, insira uma instrução JavaScript que defina quando a regra deve ser executada.
5. Na caixa **Ação**, insira uma função JavaScript a ser executada quando a condição for verdadeira.
6. Na caixa **Ordem**, insira a prioridade relativa da regra.
7. Clique em **Enviar** ou salve o formulário.

Condições da regra de criptografia

As condições da regra de criptografia determinam se a regra deve ser executada.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Uma condição de regra de criptografia deve retornar como verdadeira se a regra for para lidar com a solicitação HTTP; caso contrário, ela deve retornar como falsa.

Ao criar sua condição, lembre-se de que somente uma regra é executada por solicitação. Como resultado, a condição deve ser tão geral ou específica quanto necessário para executar nas circunstâncias pretendidas.

Nota: Tenha cuidado ao executar verificações no conteúdo da condição. Verificações excessivas podem ser caras para o servidor proxy e aumentar a latência ao lidar com solicitações complexas.

A condição pode usar o tipo de método, o tipo de conteúdo, o caminho de URL ou qualquer parâmetro de cadeia de caracteres de consulta de URL para determinar se a regra deve processar a solicitação. A condição tem acesso a esses campos por meio do objeto Objeto "request". Antes de criar uma condição de regra de criptografia, certifique-se de ter inspecionado a solicitação do cliente e compreendido as condições necessárias para acionar a regra.

Nota: Para criar regras eficientes, considere maneiras fáceis de descartar solicitações que você não deseja que sejam avaliadas por uma regra. Primeiramente, crie sua condição para retornar falso para essas solicitações. Este método aumenta o desempenho e roteia rapidamente a solicitação para a regra correta.

APIs e objetos da regra de criptografia são disponíveis para as condições da regra de criptografia.

Exemplo usando "path" e "postParams"

```
/*This condition checks if the request coming in has a path ending in
"/sample_processor.do" and if a post parameter exists in that request
 called myPostParam */

function SampleCondition(request) {
   if (endsWith(request.path, "/sample_processor.do") &&
 request.postParams.myPostParam) {
       return true;
   }
   return false;
}
```

Exemplo usando "urlParams" e "contentType"

```
/* This condition checks if a url parameter exists in the query called
myUrlParam and if the content type contains 'xml'
(if so, you can expect the body to be an XML payload).
Then, it checks if the xml payload contains myXmlTag */

function SampleCondition2(request) {
   if (request.urlParams.myUrlParam && request.contentType.indexOf('xml')
 > -1 && request.xmlContains('myXmlTag')) {
       return true;
   }
 return false;
}
```

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Ações da regra de criptografia

Uma regra de criptografia mapeia campos em uma solicitação do cliente para campos em uma tabela na sua instância e identifica os campos marcados para criptografia.

Uma ação de regra de criptografia é executada somente quando a condição dessa regra retorna verdadeira. Uma regra de criptografia identifica os dados a serem criptografados em sua carga de solicitação. Como a regra itera sobre o conteúdo do objeto de solicitação, você deve compreender o formulário e a estrutura do corpo da solicitação e determinar o que deve ser criptografado na solicitação. Os dados a serem criptografados podem estar localizados em:

- Um parâmetro POST ou URL.
- Conteúdo JSON ou XML em um parâmetro POST ou URL.
- Uma carga JSON.
- Uma carga XML.

Antes de gravar uma ação de regra de criptografia, certifique-se de fazer a:

- Inspeção da solicitação do cliente.
- Identificação de onde os dados confidenciais estão localizados no objeto request.
- Determinação do campo e o nome da tabela para inserir dados ou compreender como extrair isso dinamicamente da solicitação.

APIs e objetos da regra de criptografia estão disponíveis para as condições e ações da regra de criptografia.

APIs e objetos da regra de criptografia

Use APIs da regra de criptografia para analisar e criptografar valores em solicitações que se movem por meio do servidor proxy Edge Encryption para a instância.

As APIs disponíveis para sua regra de criptografia dependem do formato do objeto "request". Por exemplo, se o parâmetro "contentType" do objeto "request" for XML, você poderá usar XML APIs para analisar e criptografar valores na carga. Depois de determinar o tipo de objeto em sua solicitação, você pode criar uma regra de criptografia usando as APIs disponíveis.

As APIs de regra de criptografia estão disponíveis nos scripts de ação e condição da regra de criptografia.

Objeto "request"

O objeto `request` é um objeto global disponível nos scripts de ação e condição da regra do Edge Encryption.

O objeto `request` é um objeto JavaScript que representa a solicitação do cliente que chega ao servidor proxy Edge Encryption. Você deve criar sua regra de criptografia para analisar o objeto `request`, mapear valores do objeto `request` para campos em uma tabela na instância e criptografar todos os dados confidenciais no objeto `request`.

O objeto `request` inclui os seguintes atributos e dados da solicitação do cliente:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campos do objeto "request"

Campo	Descrição
path	A parte do caminho do URL.
requestMethod	GET, POST, PUT, PATCH, DELETE.
contentType	O campo de cabeçalho "Content-Type".
urlParams	Os parâmetros na cadeia de caracteres de consulta. Isso também pode ser avaliado para uma cadeia de caracteres.
postParams	Se for uma publicação de formulário, conterá os parâmetros de publicação.

request – getAsJsonContent()

Retorna a solicitação como um objeto iterável do tipo `JsonNode`.

Este método está disponível somente em uma regra de Edge Encryption se o corpo da solicitação for uma carga JSON válida. Se você não tiver certeza de qual formato o corpo da solicitação inclui, verifique o campo "contentType" no objeto `request`.

Depois que a solicitação é retornada como um objeto `JsonNode`, você pode usar JSON APIs para iterar no objeto e criptografar os campos.

Parâmetros

Nome	Tipo	Descrição
Nenhum		

Retorna

Tipo	Descrição
JsonNode	A solicitação como um `JsonNode` iterável.

request – getAsXmlContent()

Retorna o conteúdo da solicitação como um objeto iterável do tipo `XMLContent`.

Este método está disponível somente em uma regra de Edge Encryption se o corpo da solicitação for uma carga XML válida. Se você não tiver certeza de qual formato o corpo da solicitação inclui, verifique o campo "contentType" no objeto `request`.

Depois que a solicitação é retornada como um objeto `XMLContent`, você pode usar o XML APIs para iterar no objeto e criptografar os campos.

Parâmetros

Nome	Tipo	Descrição
Nenhum		

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Retorna

Tipo	Descrição
XMLContent	A solicitação como um objeto iterável do tipo *XMLContent*.

request – XMLContains (cadeia de caracteres "path")

Retorna verdadeiro se o caminho fornecido existir no DOM XML.

Este método está disponível somente se o corpo da solicitação for uma carga XML válida. Se você não tiver certeza de qual formato o corpo da solicitação inclui, verifique o campo "contentType" no objeto *request*.

Parâmetros

Nome	Tipo	Descrição
path	Cadeia de caracteres	Instrução XPath que você está procurando.

Retorna

Tipo	Descrição
Booliano	Se o caminho fornecido existir ou não no DOM XML.

APIs de parâmetro POST e URL

Os parâmetros POST e URL podem ser acessados como propriedades do objeto *request* usando `request.postParams` e `request.urlParams`.

Qualquer parâmetro único pode ser acessado como uma propriedade dos objetos primários *postParams* e *urlParams* chamando `request.postParams.myParam`. Qualquer parâmetro acessado dessa forma é um objeto da classe subjacente *ParameterValue*. Quaisquer APIs nessa classe podem ser chamadas em qualquer parâmetro.

Depois de fazer a Inspeção da solicitação do cliente, pode ser necessário acessar e criptografar os valores de parâmetro do objeto *request*. Dependendo dos dados na solicitação do cliente, você pode criptografar valores e mapeá-los para campos na instância de várias maneiras.

Como criptografar o valor de uma tabela e campo conhecidos

Se você souber o nome da tabela de instância e do campo que conterá os dados criptografados, poderá defini-los explicitamente na regra de criptografia. Por exemplo, você sabe que a solicitação será processada na instância para criar um incidente e deseja criptografar o parâmetro **text** no campo de descrição. Nesse caso, você pode criar a ação a seguir.

```
function SampleAction1() {
    request.postParams.text.valueFor('incident', 'description');
}
```

Como criptografar o valor de uma tabela e campo definidos dinamicamente

Por outro lado, se você não souber o nome do campo que os dados criptografados preencherão, poderá defini-los dinamicamente usando **tableName** e **fieldName**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O exemplo abaixo processa uma solicitação genérica que pode armazenar dados em diferentes tabelas de tarefa (como incidente, problema e change_request) na instância.

```
function SampleAction2() {
    var tableName = request.urlParams.table;
    for (var parameter in request.postParams) {
        var currentParam = request.postParams[parameter];
        var fieldName = currentParam.toString();
        if (fieldName == 'text') {
            currentParam.valueFor(tableName, 'description')
        } else {
            currentParam.valueFor(tableName, fieldName);
        }
    }
}
```

Esta ação:

- Obtém a tabela de destino dos parâmetros de URL.
- Itera sobre os parâmetros de URL.
- Solicita ao servidor proxy Edge Encryption para criptografar qualquer parâmetro de URL com um nome que corresponda a um campo marcado para criptografia.
- Pesquisa um parâmetro específico chamado *text* e solicita que o proxy Edge Encryption criptografe o valor com base na configuração de Edge Encryption de descrição na tabela de incidentes.

Neste exemplo, o método valueFor() não está executando nenhuma criptografia. Em vez disso, o método solicita ao servidor proxy Edge Encryption para verificar se o par de tabela/campo no objeto "request" está marcado para criptografia com uma configuração de criptografia e, se aplicável, criptografá-lo.

Como criptografar JSON ou XML em um parâmetro

Um parâmetro POST ou URL pode incluir conteúdo JSON ou XML. Nesse caso, você pode processar o conteúdo do parâmetro, iterar os valores e criptografar os campos obrigatórios. Neste exemplo, o **tableName** ainda é acessado de um parâmetro POST, mas o valor do campo são os **dados**do objeto JSON.

```
function SampleAction3() {
    var tableName = request.postParams.table;
    var data = request.postParams.data;
    var dataIterator = data.getAsJsonContent().iterator();
    while (dataIterator.hasNext()) {
        var jsonElement = dataIterator.next();
        var fieldName = jsonElement.getName();
        if (fieldName == 'text') {
            jsonElement.valueFor(tableName, 'description');
        } else {
            jsonElement.valueFor(tableName, fieldName);
        }
    }
}
```

Um exemplo de uma ação de regra de criptografia que processa XML em um parâmetro POST.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

```
function SampleAction4() {
    var tableName = request.postParams.table;
    var data = request.postParams.data;
    var dataIterator =
 data.getAsXmlContent().getIteratorOverAllChildren();
    while (dataIterator.hasNext()) {
        var jsonElement = dataIterator.next();
        var fieldName = jsonElement.getName();
        if (fieldName == 'text') {
            jsonElement.valueFor(tableName, 'description');
        } else {
            jsonElement.valueFor(tableName, fieldName);
        }
    }
}
```

Como criptografar uma consulta

Você pode encontrar uma consulta codificada em um parâmetro na solicitação do cliente que contém dados confidenciais. Para corresponder um campo em uma consulta a um valor criptografado no banco de dados da instância, é preciso criar uma regra de criptografia que peça ao proxy para verificar se um campo na consulta está marcado para criptografia. O método encodedQueryFor() analisa uma consulta codificada em uma determinada tabela e verifica se algum campo na consulta tem configurações de criptografia.

Neste exemplo, a regra itera sobre os parâmetros procurando o parâmetro **filter**, que deve ser uma consulta codificada do Glide.

```
function SampleAction5() {
    var tableName = request.urlParams.table;
    for (var parameter in request.postParams) {
        var currentParam = request.postParams[parameter];
        var fieldName = currentParam.toString();
        if (fieldName == 'filter') {
            currentParam.encodedQueryFor(tableName);
        } else {
            currentParam.valueFor(tableName, fieldName);
        }
    }
}
```

Por exemplo, se o valor do **filter** for `short_description=My sensitive information^number=INC000056^category=Outage`, a consulta se tornará `short_description=<Encrypted(My sensitive information)>^number=INC000056^category=Outage` na instância.

ParameterValue "toString()"

Converte o valor do parâmetro POST ou URL para uma cadeia de caracteres.

Parâmetros

Nome	Tipo	Descrição
Nenhum		

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Retorna

Tipo	Descrição
Cadeia de caracteres	O valor do parâmetro como uma cadeia de caracteres.

ParameterValue "getAsJsonContent()"

Retorna a solicitação como um objeto iterável do tipo `JsonNode`.

Este método está disponível somente em uma regra de Edge Encryption se o corpo da solicitação for uma carga JSON válida. Se você não tiver certeza de qual formato o corpo da solicitação inclui, verifique o campo "contentType" no objeto `request`.

Depois que a solicitação é retornada como um objeto `JsonNode`, você pode usar JSON APIs para iterar no objeto e criptografar os campos.

Parâmetros

Nome	Tipo	Descrição
Nenhum		

Retorna

Tipo	Descrição
JsonNode	A solicitação como um `JsonNode` iterável.

ParameterValue "getAsXmlContent()"

Retorna o conteúdo da solicitação como um objeto iterável do tipo `XMLContent`.

Este método está disponível somente em uma regra Edge Encryption e assume que o corpo da solicitação é uma carga XML válida. Você pode verificar o "contentType" para se certificar.

Depois que a solicitação é retornada como um objeto `XMLContent`, você pode usar o XML APIs para iterar no objeto e criptografar os campos.

Parâmetros

Nome	Tipo	Descrição
Nenhum		

Retorna

Tipo	Descrição
XMLContent	A solicitação como um objeto iterável do tipo `XMLContent`.

ParameterValue "encodedQueryFor(cadeia de caracteres "tableName")"

Especifica que o valor do elemento é uma consulta codificada na tabela especificada.

Chamar esta função em um parâmetro informa ao proxy que o valor do parâmetro é uma Cadeia de caracteres de consulta codificada na tabela especificada. O proxy analisa a consulta codificada e criptografa os campos dessa consulta que devem ser criptografados.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Parâmetros

Nome	Tipo	Descrição
tableName	Cadeia de caracteres	A tabela na qual você espera que a consulta seja executada.

Retorna

Tipo	Descrição
vazio	

ParameterValue – valueFor(cadeia de caracteres "tableName", cadeia de caracteres "fieldName")

Especifica que o valor do elemento seja mapeado para o campo especificado na tabela especificada.

Chamar este método em um valor de elemento informa ao proxy que o valor desse elemento é mapeado para o campo especificado na tabela especificada. Dessa forma, o proxy verifica se o campo deve ser criptografado.

Parâmetros

Nome	Tipo	Descrição
tableName	Cadeia de caracteres	O nome da tabela.
fieldName	Cadeia de caracteres	O nome do campo.

Retorna

Tipo	Descrição
vazio	

XML APIs

As XML APIs podem ser usadas depois de chamar `getAsXmlContent()` no objeto `request` ou em uma propriedade `ParameterValue`.

Ao usar XML APIs para gravar sua regra de criptografia, você pode seguir um formato geral:

1. Chame `getAsXmlContent()` no objeto `request` ou em uma propriedade `ParameterValue`. Isso retorna um objeto iterável da classe `XMLContent` subjacente.
2. Chame `getIterator()` ou `getIterator(cadeia de caracteres "xPath")` no objeto `XMLContent`. Isso retorna um objeto `XMLElementIterator` que pode ser usado para iterar em elementos "XML".
3. Chame o método `hasNext()` no objeto `XMLElementIterator` para determinar se outro elemento está disponível.
4. Chame `next()` no objeto `XMLElementIterator` para retornar o próximo elemento "XML". Você não pode chamar `next()` sem primeiro chamar `hasNext()`.
5. Chame `valueFor(cadeia de caracteres "tableName", cadeia de caracteres "fieldName")` no elemento "XML". Este método informa ao proxy que o valor desse

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

elemento é mapeado para o campo especificado na tabela especificada. Dessa forma, o proxy verifica se o campo deve ser criptografado.

Nota: Para determinar se você deseja chamar *`valueFor(cadeia de caracteres "tableName", cadeia de caracteres "fieldName")`* em um elemento "XML", você pode usar o método *`getName()`* para retornar o nome do elemento.

Mapeamento para um campo-tabela conhecido na instância

Neste exemplo, a carga XML será processada na instância para inserir registros na tabela de incidentes. O campo de descrição preencherá "short_description" no incidente.

```
<data>
    <record>
        <name>'Test Record 1'</name>
        <description>'Test Record 1 Description'</description>
        <tag>critical</tag>
    </record>
    <record>
        <name>'Test Record 2'</name>
        <description>'Test Record 2 Description'</description>
        <tag>security</tag>
    </record>
</data>
```

A seguinte ação de regra de criptografia pode ser aplicada:

```
function sampleXmlAction1() {
    var xmlContent = request.getAsXmlContent();
    // This loop iterates over all description tags that match the given
 path
    var xmlElementIterator =
 xmlContent.getIterator('data/record/description');
    while (xmlElementIterator.hasNext()) {
        var xmlElement = xmlElementIterator.next();
        xmlElement.valueFor('incident', 'short_decription');
    }
}
```

Esta ação itera por meio de marcadores **description** e solicita que o servidor proxy criptografe os valores e os insira em "incident.short_description" na instância.

Nota: Esta regra encontra todos os marcadores **description** em todos os marcadores **record** na carga XML. Se houver apenas uma ocorrência de um marcador para criptografar, a regra ainda usará a estrutura "xPath" e "iterador". No entanto, ele itera apenas uma vez no loop.

Mapeamento para um campo-tabela desconhecido na instância

Neste exemplo, a regra itera sobre os marcadores **record**, mas não sabe quais marcadores esperar no marcador **record**. O único conhecido é que os marcadores nos marcadores **record** correspondem aos nomes das colunas especificadas no parâmetro de URL da tabela.

A regra também especifica que, se a tabela for incidente, os dados no marcador **description** devem ser criptografados e armazenados no campo "short_description" na instância.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

```
function sampleXmlAction2() {
    var xmlContent = request.getAsXmlContent();
    var tableName = request.urlParam.table;
    // This first iterator will iterate over all record elements
    var xmlElementIterator = xmlContent.getIterator('data/record');
    while (xmlElementIterator.hasNext()) {
        encryptFieldsInRecord(xmlElementIterator.next());
    }
}
function encryptFieldsInRecord(xmlElement) {
    //Then, iterate over all tags representing fields in the table
    var fieldIterator = xmlElement.getIteratorOverAllChildren();
    while (fieldIterator.hasNext()) {
        var field = fieldIterator.next();
        var fieldName = childElement.getName();
        //if table is incident, then description is encrypted for the
 short_description field
        if (tableName == 'incident' && fieldName == 'description') {
            field.valueFor(tableName, 'short_description');
        } else {
            //if table is not incident, ask the proxy to check if the
 given field is encrypted for the given table
            field.valueFor(tableName, fieldName);
        }
    }
}
```

Na função *encryptFieldsInRecord()*, o método *valueFor()* é chamado em uma tabela e em um campo que são atribuídos dinamicamente com base na solicitação. Mesmo que os nomes da tabela e do campo possam mudar, a regra solicita que o proxy verifique se o campo na tabela deve ser criptografado com base nas configurações de criptografia definidas.

Se o campo não estiver configurado para criptografia ou se o marcador não corresponder a um campo na tabela, o proxy ignorará esse marcador. Se o marcador corresponder a um campo marcado para criptografia, o servidor proxy Edge Encryption criptografará o valor.

Uso de uma consulta codificada

Neste exemplo, todos os marcadores têm o atributo **filter**, que indica se o marcador contém uma consulta codificada.

```
<data>
    <record>
        <name filter="false">'Test Record 1'</name>
        <description filter="false">'Test Record 1
 Description'</description>
        <query filter="true">category=1^name=edge</query>
    </record>
    <record>
        <name filter="false">'Test Record 2'</name>
        <description filter="false">'Test Record 2
 Description'</description>
        <query filter="true">category=2^severity=3</query>
   </record>
</data>
```

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A seguinte ação de regra de criptografia pode ser aplicada:

```
function sampleXmlAction3() {
   var xmlContent = request.getAsXmlContent();
   var tableName = request.urlParam.table;
   // This first iterator will iterate over all record elements
   var xmlElementIterator = xmlContent.getIterator('data/record');
   while (xmlElementIterator.hasNext()) {
       encryptFieldsInRecord(xmlElementIterator.next());
   }
}
function encryptFieldsInRecord(xmlElement) {
   //this time we want to iterate over all tags representing fields in
 the table
   var fieldIterator = xmlElement.getIteratorOverAllChildren();
   while (fieldIterator.hasNext()) {
       var field = fieldIterator.next();
       var fieldname = childElement.getName();
       //let's look at the filter attribute, if true, then encrypt as
 encoded query
       if (field.getAttributeValue('filter') == 'true') {
           field.encodedQueryFor(tableName);
       } else {
           //if it is false then check if the field should be encrypted
           field.valueFor(tableName, fieldName);
       }
   }
}
```

Se o valor do atributo **filter** for verdadeiro, a regra solicitará que o servidor proxy criptografe os valores na consulta codificada. Se for falso, a regra solicitará que o proxy verifique se o campo deve ser criptografado.

XMLContent

Um objeto global que fornece métodos para iterar no conteúdo XML.

Você pode acessar um objeto *`XMLContent`* chamando getAsXmlContent() em um objeto *`request`*.

Você acessa dados XML em um parâmetro POST ou URL chamando `request.postParams.<parameter name>.getAsXmlContent()` ou `request.urlParams.<parameter name>.getAsXmlContent()`.

XMLContent – getIterator()

Retorna um objeto *`XMLElementIterator`* para o conteúdo XML.

Parâmetros

Nome	Tipo	Descrição
Nenhum		

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Retorna

Tipo	Descrição
XMLElementIterator	Um objeto que pode ser usado para iterar elementos no objeto *XMLContent*.

XMLContent – getIterator(cadeia de caracteres "xPath")

Retorna um objeto *XMLElementIterator* para o conteúdo XML com base no parâmetro especificado.

Parâmetros

Nome	Tipo	Descrição
xPath	Cadeia de caracteres	Uma expressão semelhante a xPath que especifica onde iniciar no objeto *XMLContent*.

Retorna

Tipo	Descrição
XMLElementIterator	Um objeto que pode ser usado para iterar elementos no objeto *XMLContent*.

XMLElementIterator

Fornece métodos para iterar elementos "XML".

Você obtém um objeto *XMLElementIterator* chamando o método *getIterator()* da classe *XMLContent*.

XMLElementIterator – hasNext()

Determina se há outro elemento disponível.

Parâmetros

Nome	Tipo	Descrição
Nenhum		

Retorna

Tipo	Descrição
Booliano	Verdadeiro se outro elemento estiver disponível.

XMLElementIterator – next()

Retorna o próximo elemento no iterador.

Você não pode chamar *next()* sem primeiro chamar *hasNext()*.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Parâmetros

Nome	Tipo	Descrição
Nenhum		

Retorna

Tipo	Descrição
XMLElement	O próximo elemento XML.

XMLElement

Fornece métodos para iterar por meio de elementos "XML" e mapear valores para campos em uma tabela.

Você obtém um objeto `XMLElement` chamando o método `next()` de um objeto `XMLElementIterator`.

XMLElement – getIterator(cadeia de caracteres "xPath")

Retorna um objeto `XMLElementIterator` para o elemento "XML" com base no parâmetro especificado.

Parâmetros

Nome	Tipo	Descrição
xPath	Cadeia de caracteres	Uma expressão semelhante a xPath que especifica onde iniciar no objeto `XMLElement`.

Retorna

Tipo	Descrição
XMLElementIterator	Um objeto que pode ser usado para iterar elementos no objeto `XMLElement`.

XMLElement – getIteratorOverAllChildren()

Retorna um objeto `XMLElementIterator` que inclui todos os subelementos para o elemento "XML" com base no parâmetro especificado.

Parâmetros

Nome	Tipo	Descrição
Nenhum		

Retorna

Tipo	Descrição
XMLElementIterator	Um objeto que pode ser usado para iterar elementos no objeto `XMLElement`.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

XMLElement – valueFor(cadeia de caracteres "tableName", cadeia de caracteres "fieldName")

Especifica que o valor do elemento seja mapeado para o campo especificado na tabela especificada.

Chamar este método em um valor de elemento informa ao proxy que o valor desse elemento é mapeado para o campo especificado na tabela especificada. Dessa forma, o proxy verifica se o campo deve ser criptografado. Se o nomes da tabela e do campo forem desconhecidos, você pode chamar o método `valueFor()` em uma tabela e em um campo que serão atribuídos dinamicamente com base na solicitação.

Parâmetros

Nome	Tipo	Descrição
tableName	Cadeia de caracteres	O nome da tabela.
fieldName	Cadeia de caracteres	O nome do campo.

Retorna

Tipo	Descrição
vazio	

XMLElement – encodedQueryFor(cadeia de caracteres "tableName")

Especifica que o valor do elemento é uma consulta codificada para a tabela especificada.

Chamar esta função em um elemento informa ao proxy que o valor do elemento é uma Cadeia de caracteres de consulta codificada para a tabela especificada. O proxy analisa a consulta codificada e criptografa os campos dessa consulta que devem ser criptografados.

Parâmetros

Nome	Tipo	Descrição
tableName	Cadeia de caracteres	A tabela na qual você espera que a consulta seja executada.

Retorna

Tipo	Descrição
vazio	

XMLElement – getName()

Retorna o nome do elemento.

Parâmetros

Nome	Tipo	Descrição
Nenhum		

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Retorna

Tipo	Descrição
Cadeia de caracteres	O nome do elemento.

XMLElement – getAttributeValue(cadeia de caracteres "attribute")

Retorna o valor do atributo especificado.

Parâmetros

Nome	Tipo	Descrição
attribute	Cadeia de caracteres	Nome do atributo.

Retorna

Tipo	Descrição
Cadeia de caracteres	O valor do atributo.

JSON APIs

As JSON APIs podem ser usadas depois de chamar `getAsJsonContent()` no objeto `request` ou em uma propriedade `ParameterValue`.

Ao usar JSON APIs para gravar sua regra de criptografia, você pode seguir um formato geral:

1. Chame `getAsJsonContent()` no objeto `request`. Isso retorna um objeto iterável da classe `JsonNode` subjacente.
2. Chame `iterator()` ou `getIterator(cadeia de caracteres "xPath")` no objeto `JsonNode`. Isso retorna um objeto `JsonNodeIterator` que pode ser usado para iterar nós no objeto "JSON".
3. Chame o método `hasNext()` no objeto `JsonNodeIterator` para determinar se outro elemento está disponível.
4. Chame `next()` no objeto `JsonNodeIterator` para retornar o próximo elemento "JSON". Você não pode chamar `next()` sem primeiro chamar `hasNext()`.
5. Chame `valueFor(cadeia de caracteres "tableName", cadeia de caracteres "fieldName")` no elemento "JSON". Este método informa ao proxy que o valor desse elemento é mapeado para o campo especificado na tabela especificada. Dessa forma, o proxy verifica se o campo deve ou não ser criptografado.

> **Nota:** Para determinar se você deseja chamar `valueFor(cadeia de caracteres "tableName", cadeia de caracteres "fieldName")` em um elemento "JSON", você pode usar o método `getName()` para retornar o nome do elemento.

Mapeamento para um campo-tabela conhecido na instância

Neste exemplo, a carga JSON é processada na instância para inserir registros na tabela de incidentes. O campo de descrição preenche "short_description" no incidente.

```
{
    data: {
        records: [
```

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

```
            {
                "name": "Test Record 1",
                "description": "Test Record 1 Description",
                "tag": "security"
            },
            {
                "name": "Test Record 1",
                "description": "Test Record 1 Description",
                "tag": "security"
            }],
        "query":
 "assigned_to=3D4860165813e63a00d00abd322244b092^category=vulnerability"
    },
    "source": "10.11.13.14"
}
```

A seguinte regra pode ser aplicada:

```
function sampleJsonAction1() {
    var jsonContent = request.getAsJsonContent();
    // This loop iterates over all description elements in the records
 array
    var jsonNodeIterator =
 jsonContent.getIterator('/data/records/description');
    while (jsonNodeIterator.hasNext()) {
        var jsonNode = jsonNodeIterator.next();
        jsonNode.valueFor('incident', 'short_decription');
    }
}
```

Esta ação itera por meio de nós **description** e solicita que o servidor proxy criptografe os valores e os insira em "incident.short_description" na instância.

Nota: Esta regra encontra todos os nós **description** dentro da carga JSON. Se houver apenas uma ocorrência de um nó para criptografar, a regra ainda usará a estrutura "xPath" e "iterador". No entanto, ele itera apenas uma vez no loop.

Mapeamento para um campo-tabela desconhecido na instância

Neste exemplo, a regra itera sobre os **records**, mas não tem certeza de quais nós esperar. O único conhecido é que para cada objeto em **records**, os nós correspondem aos nomes das colunas especificadas no parâmetro de URL da tabela.

A regra também especifica que, se a tabela for incidente, os dados no nó **description** devem ser criptografados e armazenados no campo "short_description" na instância.

```
function sampleJsonAction2() {
    var jsonContent = request.getAsJsonContent();
    var tableName = request.urlParam.table;
    // This first iterator will iterate over all record elements
    var jsonNodeIterator = jsonContent.getIterator('data/records');
    while (jsonNodeIterator.hasNext()) {
            encryptFieldsInRecord(jsonNodeIterator.next());
    }
}
function encryptFieldsInRecord(jsonNode) {
    //this time we want to iterate over all nodes
```

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

```
    var fieldIterator = jsonNode.iterator();
    while (fieldIterator.hasNext()) {
            var field = fieldIterator.next();
            var fieldname = childElement.getName();
            if (fieldName == 'description') {
                field.valueFor(tableName, 'short_description');
            } else {
                field.valueFor(tableName, fieldName);
            }
    }
}
```

Na função *encryptFieldsInRecord()*, o método *valueFor()* é chamado em uma tabela e em um campo que são atribuídos dinamicamente com base na solicitação. Mesmo que os nomes da tabela e do campo possam mudar, a regra solicita que o proxy verifique se o campo na tabela deve ser criptografado com base nas configurações de criptografia definidas.

Se o campo não estiver configurado para criptografia ou se o nome do nó não corresponder a um campo na tabela, o proxy ignorará esse nó. Se o nome do nó corresponder a um campo marcado para criptografia, o proxy criptografará o valor.

Uso de uma consulta codificada

```
function sampleJsonAction3() {
    var jsonContent = request.getAsJsonContent();
    var tableName = request.urlParam.table;
    // This first iterator will iterate over all record elements
    var jsonNodeIterator = jsonContent.getIterator('data');
    while (jsonNodeIterator.hasNext()) {
        var jsonNode = jsonNodeIterator.next();
        if (jsonNode.getName() == 'records')
            encryptRecors(jsonNodeIterator.next());
        else if (jsonNode.getName() == 'query')
            jsonNode.encodedQueryFor(tableName);
    }
}
function encryptRecords(jsonNode) {
    //we iterate over all fields in the node
    var recordIterator = jsonNode.iterator();
    while (recordIterator.hasNext()) {
        encryptFieldsInRecord(recordIterator.next());
    }
}
function encryptFieldsInRecord(jsonNode) {
    //this time we want to iterate over all nodes
    var fieldIterator = jsonNode.iterator();
    while (fieldIterator.hasNext()) {
            var field = fieldIterator.next();
            var fieldname = childElement.getName();
            field.valueFor(tableName, fieldName);
    }
}
```

Neste exemplo, a regra itera sobre **data**. Ao encontrar **records**, ele executa a mesma lógica do segundo exemplo, iterando sobre os campos em cada nó. Quando encontra

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

o nó **query**, ele chama *encodedQueryFor()* para criptografar valores que devem ser criptografados na consulta.

JsonNode

Um objeto global que fornece métodos para iterar no conteúdo JSON.

Você pode acessar um objeto *JsonNode* chamando getAsJsonContent() em um objeto *request*.

Você acessa um conteúdo JSON em um parâmetro POST ou URL chamando `request.postParms.<parameter name>.getAsJsonContent()` ou `request.urlParms.<parameter name>.getAsJsonContent()`.

JsonNode – getIterator(cadeia de caracteres "xPath")

Retorna um objeto *JsonNodeIterator* para o conteúdo JSON.

Este método só pode ser usado no nó raiz, mas pode ser usado para percorrer profundamente o objeto JSON. As travessias subsequentes devem usar o método *iterator()*.

Parâmetros

Nome	Tipo	Descrição
xPath	Cadeia de caracteres	Uma expressão xPath.

Retorna

Tipo	Descrição
JsonNodeIterator	Um objeto que pode iterar nós no objeto "JSON".

JsonNode – iterator()

Retorna um objeto *JsonNodeIterator* que itera em todos os nós secundários do nó atual.

Parâmetros

Nome	Tipo	Descrição
Nenhum		

Retorna

Tipo	Descrição
JsonNodeIterator	Um objeto que pode iterar nós no objeto "JSON".

JsonNode – getAsString()

Retorna o valor do nó atual como uma cadeia de caracteres.

Parâmetros

Nome	Tipo	Descrição
Nenhum		

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Retorna

Tipo	Descrição
Cadeia de caracteres	O valor do nó atual.

JsonNode – getAsString(cadeia de caracteres "propertyName")

Retorna o valor da cadeia de caracteres à propriedade especificada.

Parâmetros

Nome	Tipo	Descrição
propertyName	Cadeia de caracteres	Nome da propriedade.

Retorna

Tipo	Descrição
Cadeia de caracteres	O valor da propriedade.

JsonNode – getName()

Retorna o nome do atual nó JSON.

Parâmetros

Nome	Tipo	Descrição
Nenhum		

Retorna

Tipo	Descrição
Cadeia de caracteres	Nome do atual nó JSON.

JsonNode – valueFor(cadeia de caracteres "tableName", cadeia de caracteres "fieldName")

Especifica que a propriedade JSON seja mapeada para o campo especificado na tabela especificada.

Chamar este método em uma propriedade JSON informa ao proxy que o valor dessa propriedade é mapeado para o campo especificado na tabela especificada. Dessa forma, o proxy decide se o campo deve ser criptografado. Se o nomes da tabela e do campo forem desconhecidos, você pode chamar o método `valueFor()` em uma tabela e em um campo que serão atribuídos dinamicamente com base na solicitação.

Parâmetros

Nome	Tipo	Descrição
tableName	Cadeia de caracteres	O nome da tabela.
fieldName	Cadeia de caracteres	O nome do campo.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Retorna

Tipo	Descrição
vazio	

JsonNode – encodedQueryFor(cadeia de caracteres "tableName")

Especifica que o valor da propriedade JSON é uma consulta codificada para a tabela especificada.

Chamar esta função em um nó JSON informa ao proxy que o valor é uma Cadeia de caracteres de consulta codificada para a tabela especificada. O proxy analisa a consulta codificada e criptografa os valores para os campos dessa consulta que devem ser criptografados.

Parâmetros

Nome	Tipo	Descrição
tableName	Cadeia de caracteres	A tabela na qual você espera que a consulta seja executada.

Retorna

Tipo	Descrição
vazio	

JsonNodeIterator

Você obtém um objeto `JsonNodeIterator` chamando os `métodos getIterator()` ou `iterator()` da classe `JsonNode`.

JsonNodeIterator – hasNext()

Determina se há outra propriedade disponível.

Parâmetros

Nome	Tipo	Descrição
Nenhum		

Retorna

Tipo	Descrição
Booliano	Verdadeiro se outra propriedade estiver disponível.

JsonNodeIterator – next()

Retorna a próxima propriedade no iterador.

Você não pode chamar `next()` sem primeiro chamar `hasNext()`.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Parâmetros

Nome	Tipo	Descrição
Nenhum		

Retorna

Tipo	Descrição
JsonNode	O próximo *JsonNode*.

print(cadeia de caracteres "message")

Imprime uma mensagem no arquivo de log do wrapper: `<proxy server directory>/logs/wrapper_<date>.log`.

Este método está disponível somente em um script de ação de regra Edge Encryption.

Parâmetros

Nome	Tipo	Descrição
message	Cadeia de caracteres	A mensagem a ser gravada no arquivo de log do wrapper.

Retorna

Tipo	Descrição
vazio	

Palavras-chave proibidas

O proxy Edge Encryption valida scripts de regra de criptografia antes de salvar a regra. Muitas palavras-chave JavaScript não são permitidas em scripts de regra de criptografia.

Palavras-chave proibidas

Palavra-chave
__DIR__
__FILE__
__LINE__
__parent__
__proto__
Error
eval
getClass
getPrototypeOf
Java

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Palavras-chave proibidas

Palavra-chave
javax
javafx
JavaImporter
load
loadWithNewGlobal
new
Packages
Object
prototype
RegExp
setPrototypeOf
this
throw

Atributos do dicionário do Edge Encryption

Adicione atributos de dicionário a tabelas e campos para controlar como eles funcionam com o Edge Encryption.

Para definir um atributo do dicionário como verdadeiro, você deve inserir `attribute=true` no campo **Atributos**. Para adicionar um atributo de dicionário a um registro, consulte Como alterar tabelas e campos usando atributos de dicionário.

Edge Encryption excluído [edge_encryption_excluded]

Determina se o campo é excluído da criptografia.

Quando definido como `verdadeiro`, o campo ou a tabela não podem ser criptografados. Quando definido como `falso`, o campo ou a tabela podem ser criptografados.

- Valor: verdadeiro/falso
- Elemento de destino: campo ou tabela
- Valor padrão: falso

Edge Encryption habilitado [edge_encryption_enabled]

Determina se o campo está qualificado para criptografia por meio de uma configuração de criptografia.

Quando definido como `verdadeiro`, o campo está qualificado para criptografia. Quando definido como `falso`, o campo não está qualificado para criptografia. Como esse atributo é usado pelo sistema e não pode ser modificado, ele não é exibido para o usuário.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Esse atributo não indica que um campo está criptografado nem aciona nenhuma lógica de criptografia no campo. Em vez disso, o atributo determina a possibilidade de o campo ser criptografado por um usuário.

- Valor: verdadeiro/falso
- Elemento de destino: campo
- Valor padrão: verdadeiro para campos de cadeia de caracteres

Texto não criptografado do Edge Encryption permitido [edge_encryption_clear_text_allowed]

Determina se os scripts do lado do servidor podem anexar dados não criptografados a uma cadeia de caracteres criptografada no campo para ações do usuário realizadas por meio do servidor proxy ou qualquer script automatizado do lado do servidor, como trabalhos agendados.

Quando definido como `verdadeiro`, é permitido anexar dados. Quando definido como `falso`, não é permitido anexar dados.

- Valor: verdadeiro/falso
- Elemento de destino: campo
- Valor padrão: falso

Separação de domínio e Edge Encryption

A separação de domínio é compatível em circunstâncias limitadas com Edge Encryption. Edge Encryption fornece a capacidade de criptografar dados de dentro do ambiente do cliente por meio do uso de configurações, regras e chaves específicas definidas no proxy Edge Encryption. O proxy Edge Encryption não reconhece o domínio e não é compatível a configurações específicas do domínio. O Domain Separation permite separar dados, processos e tarefas administrativas em agrupamentos lógicos chamados de domínios. Você pode controlar vários aspectos dessa separação, incluindo quais usuários podem ver e acessar os dados.

Nível de suporte: Sem suporte

- O campo de domínio pode existir em tabelas de dados, mas não há lógica de negócios para gerenciar os dados.
- Este nível não é considerado separado por domínio.

Para obter mais informações sobre os níveis de suporte, consulte Suporte de aplicação para separação de domínio.

Como a separação de domínio funciona no Edge Encryption

O Edge Encryption pode ser usado onde não são necessárias chaves, configurações e regras específicas de domínio.

Informações relacionadas

Domain Separation para provedores de serviço

Integração de dados com Edge Encryption

Para integrar dados de terceiros com uma instância usando Edge Encryption, você deve rotear os dados por meio do servidor proxy Edge Encryption usando integrações

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

compatíveis. As integrações compatíveis usam regras de criptografia do sistema de base que mapeiam dados em cada carga para campos em uma tabela.

Como carregar dados em campos marcados para criptografia

Edge Encryption não são compatíveis à importação ou exportação de dados para o Excel, CSV, XML ou outros tipos de arquivo de ou para campos com configurações de criptografia definidas.

ODBC Driver

Criptografe as solicitações e consulte os dados por meio do servidor proxy Edge Encryption usando o ODBC Driver.

Saiba mais: Integração do ODBC Driver do Edge Encryption

MID Server

Você pode configurar o MID Server para rotear dados por meio de um servidor proxy Edge Encryption. No entanto, algumas restrições se aplicam.

Saiba mais: Integração do MID Server do Edge Encryption

Serviços Web REST/SOAP

Use os serviços web SOAP/REST para atualizar ou recuperar dados de registro por meio do servidor proxy Edge Encryption.

Saiba mais: Serviços Web

Serviço Web JSONv2

Use as APIs do serviço Web JSONv2 para atualizar ou recuperar dados de registro por meio do servidor proxy Edge Encryption. As regras de criptografia do sistema base são compatíveis com APIs de recuperação e modificação de dados.

- Para inserir um único registro usando a API de modificação de dados, use os métodos `insert()` ou `insertMutiple()`.
- Para inserir múltiplos registros usando a API de modificação de dados, use o método `insertMutiple()`.

Saiba mais: Serviço Web JSONv2

Para criptografar dados de integrações de terceiros personalizadas não listadas acima, crie regras de criptografia personalizadas. Consulte Como definir uma regra de criptografia personalizada.

Como carregar anexos em registros marcados para criptografia

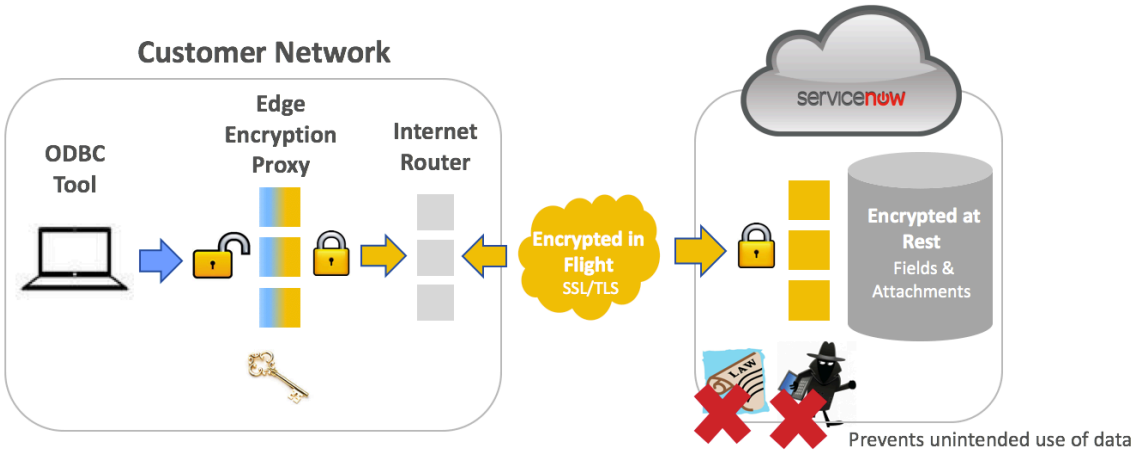
Os anexos podem ser carregados para tabelas com criptografia de anexo configurada usando serviços Web REST e SOAP.

Integração do ODBC Driver do Edge Encryption

Configure o ODBC Driver para consultar dados criptografados por Edge Encryption. O servidor proxy Edge Encryption criptografa as solicitações do ODBC Driver para a instância ServiceNow quando Edge Encryption está integrado ao ODBC Driver.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

As respostas criptografadas da instância são descriptografadas por meio do servidor proxy Edge Encryption antes de passar para o ODBC Driver em sua rede.



Para uma integração bem-sucedida, o ODBC Driver deve confiar no certificado do servidor proxy Edge Encryption . Se o certificado do servidor proxy Edge Encryption for assinado por uma autoridade de certificação confiável para o ODBC Driver, o servidor proxy Edge Encryption será automaticamente confiável. No entanto, se uma autoridade de certificação confiável para o ODBC Driver não tiver assinado o certificado do servidor proxy Edge Encryption, você deverá importar o certificado autoassinado para o armazenamento confiável do ODBC.

Como importar um certificado autoassinado para o armazenamento confiável ODBC

Se uma autoridade de certificação confiável para o ODBC Driver não tiver assinado o certificado do servidor proxy Edge Encryption, você deverá importar um certificado autoassinado para o armazenamento confiável do ODBC. Você pode exportar o certificado do servidor proxy Edge Encryption e importá-lo para o armazenamento confiável do ODBC.

Antes de Iniciar

Função necessária: administrador

Para determinar se uma autoridade de certificação confiável pelo ODBC Driver assinou o certificado do servidor proxy Edge Encryption, execute o seguinte comando no diretório de armazenamento de chaves no diretório inicial do proxy para exibir uma lista de autoridades de certificação confiáveis pelo ODBC Driver:

```
keytool -keystore "<ODBC directory>\ip\Java\jre\lib\security\cacerts"
 -list
```

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

Na maioria dos casos, o cliente se conecta aos proxies Edge Encryption por meio de um balanceador de carga, portanto, o certificado seria o certificado configurado no balanceador de carga.

No caso em que não há balanceador de carga entre o cliente e o servidor proxy de borda, o certificado é o certificado apresentado pelo Edge Proxy e está configurado no arquivo *edgeencryption.properties*.

```
edgeencryption.proxy.https.port = 9090
edgeencryption.proxy.https.keystore.path = keystore/keystore
edgeencryption.proxy.https.keystore.password = password
edgeencryption.proxy.https.cert.alias = jetty
```

Para obter detalhes sobre como editar as propriedades, consulte Configurar propriedades adicionais no arquivo de propriedades do Edge Encryption

Procedimento

1. Mude para o diretório de armazenamento de chaves no diretório inicial do proxy.
2. Verifique o armazenamento de chaves do certificado autoassinado.

   a. Para verificar o armazenamento de chaves do certificado, você pode executar o seguinte comando para listar todos os itens no armazenamento de chaves.

   ```
   keytool -list -keystore keystore.jceks -storetype jceks -v
   ```

   b. Localize o alias de chave na lista de itens.

3. Usando o alias de chave, exporte o certificado para um arquivo .cer.

   ```
   keytool -export -alias <key alias> -keystore keystore.jceks -storetype
    jceks -rfc -file <file name>.cer
   ```

4. Mude para o seu diretório de armazenamento confiável do ODBC: `ODBC\ip\Java\jre\lib\security\cacerts`.
5. Importe o certificado para o seu armazenamento confiável ODBC.

   ```
   keytool -keystore cacerts -importcert -alias $<key alias> -file <file
    name>.cer
   ```

Como definir as propriedades do ODBC Driver

Defina as propriedades do ODBC Driver para rotear solicitações por meio do servidor proxy Edge Encryption.

Antes de Iniciar

Função necessária: administrador

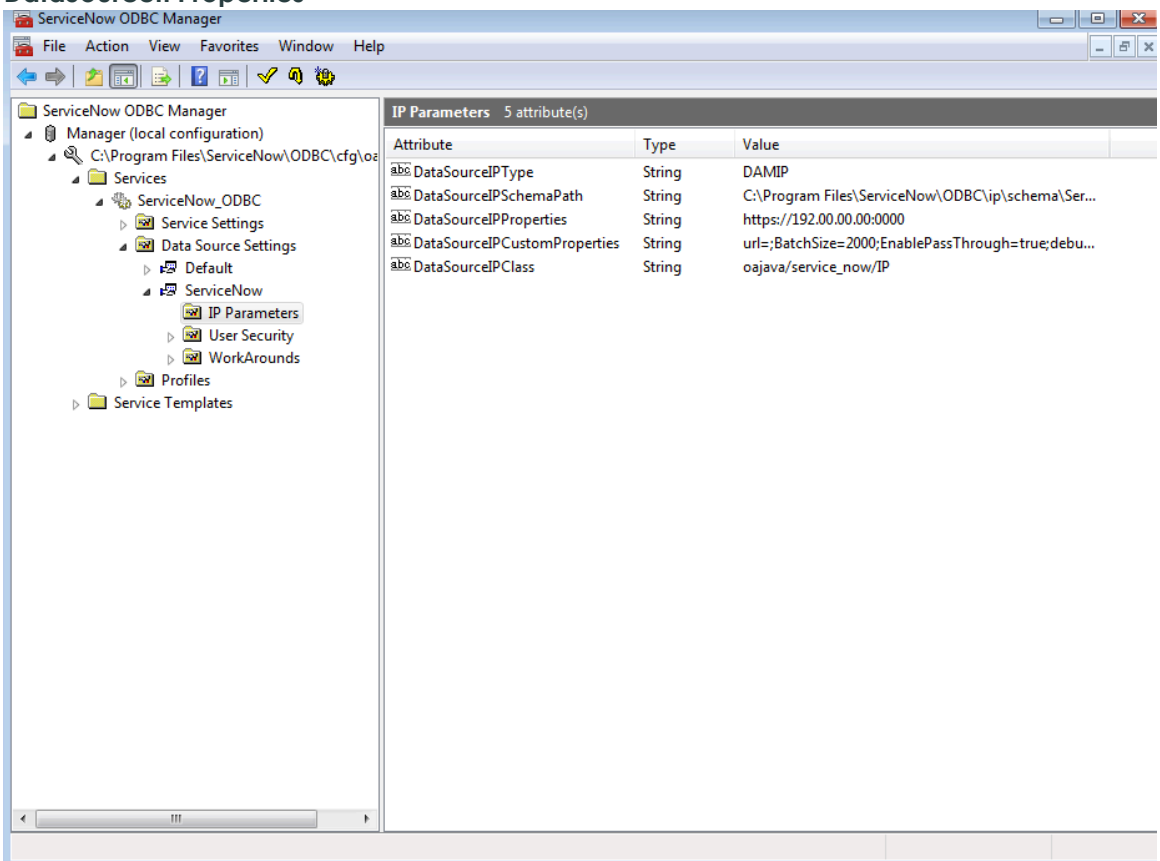
Procedimento

1. No Windows, navegue até **Iniciar** > **Programas** > **ServiceNow ODBC Management Console**.
2. Expanda a raiz da árvore do console para: `ServiceNow ODBC Manager\Manager\<installation location>\Services\ServiceNow_ODBC\Data Source Settings\ServiceNow\IP Parameters`.
3. Clique duas vezes no atributo **DataSourceIPProperties**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Altere o **valor** para o URL do servidor proxy Edge Encryption, como `https://<IP address>:<port>`

DataSourceIPProperties



5. Clique em **OK**.

O que Fazer Depois

O ODBC Driver agora está configurado para rotear solicitações para a instância por meio do servidor proxy Edge Encryption.

Integração do MID Server do Edge Encryption

Configure o MID Server para rotear dados por meio de um servidor proxy Edge Encryption.

Quando integrado ao MID Server, o servidor proxy Edge Encryption atua como endpoint do MID Server. Dessa forma, o servidor proxy Edge Encryption criptografa e descriptografa os dados que passam entre a instância ServiceNow e o MID Server.

Limitações ao integrar com o MID Server

Quando os dados do MID Server são configurados para passar pelo servidor proxy Edge Encryption, as seguintes limitações se aplicam:

- A criptografia dos campos de Fila do ECC não é compatível.
- Os dados criptografados não podem ser usados com Descoberta ou Mapeamento de serviços.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Como apontar o MID Server para o servidor proxy Edge Encryption

Para passar dados de MID Server por meio do servidor proxy Edge Encryption, atualize o arquivo de configuração MID Server para apontar MID Server para o servidor proxy Edge Encryption.

Antes de Iniciar
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa
Ao configurar MID Server para passar pelo servidor proxy Edge Encryption, você não pode usar as propriedades do proxy da Web no arquivo de configuração MID Server para rotear o tráfego por meio do servidor proxy Edge Encryption para sua instância. Em vez disso, você deve definir o servidor proxy Edge Encryption como o endpoint de MID Server.

Procedimento

1. Navegue até o seu diretório local MID Server e abra o arquivo `config.xml`.
2. Encontre o elemento `<parameter name="url" value="https://YOUR_INSTANCE.service-now.com" />` e mude a propriedade de valor para o URL do seu servidor proxy Edge Encryption.
   Por exemplo, `http://hostname.mycompany.com:8081`
   Essa etapa direciona MID Server para passar o tráfego para o servidor proxy Edge Encryption em vez da instância. O servidor proxy Edge Encryption, por sua vez, criptografa todos os campos necessários e passa a carga para a instância.
3. Salve e feche o arquivo.
4. Se estiver em execução, reinicie MID Server.

Diagnóstico e desempenho do Edge Encryption

Monitore as tendências de desempenho do servidor proxy Edge Encryption e analise os erros gerados pelo servidor proxy Edge Encryption.

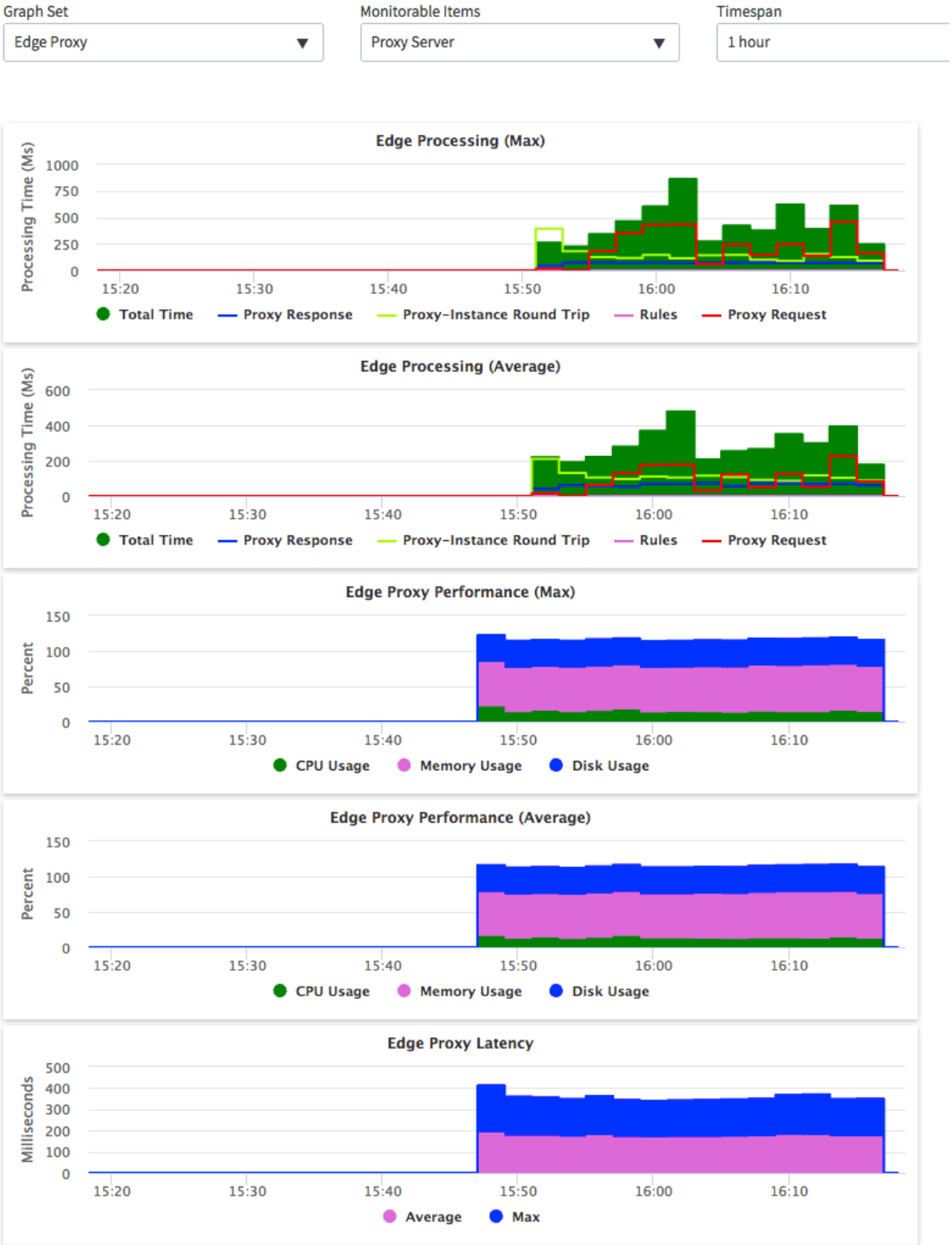
Desempenho do proxy de borda

Veja tendências-chave de desempenho do servidor proxy Edge Encryption usando o gráfico de proxy de borda definido na página inicial de desempenho ServiceNow. As tendências monitoradas incluem:

- Tempos de resposta máximo e médio entre o cliente, o servidor proxy e a instância.
- CPU, espaço em disco e uso de memória da máquina host.
- Latência máxima e média da rede entre o servidor proxy e a instância ServiceNow.

Nota: Edge Encryption servidores proxy com nomes duplicados não reportam tendências de desempenho.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Processamento de borda (máximo e médio)

Tempo máximo e médio em milissegundos para processar uma solicitação. Esses pontos de dados são tendências gerais ao longo do tempo.

- **Tempo total**: tempo para o servidor proxy receber uma solicitação de um cliente e enviar uma resposta. Esse ponto de dados é a soma dos pontos de dados subsequentes.
- **Resposta do proxy**: tempo para o servidor proxy processar uma resposta da instância.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- **Viagem de ida e volta entre instância e proxy**: tempo para o servidor proxy enviar uma solicitação para a instância e receber uma resposta. Inclui a latência de rede entre o servidor proxy e a instância e o tempo gasto pela instância para processar a solicitação.
- **Regras**: tempo para o servidor proxy avaliar uma solicitação usando regras de criptografia definidas.
- **Solicitação de proxy**: tempo para o servidor proxy processar uma solicitação do cliente e encaminhá-la para a instância.

Desempenho do proxy de borda (máximo e médio)

Percentual máximo e médio de recursos usados na máquina host.

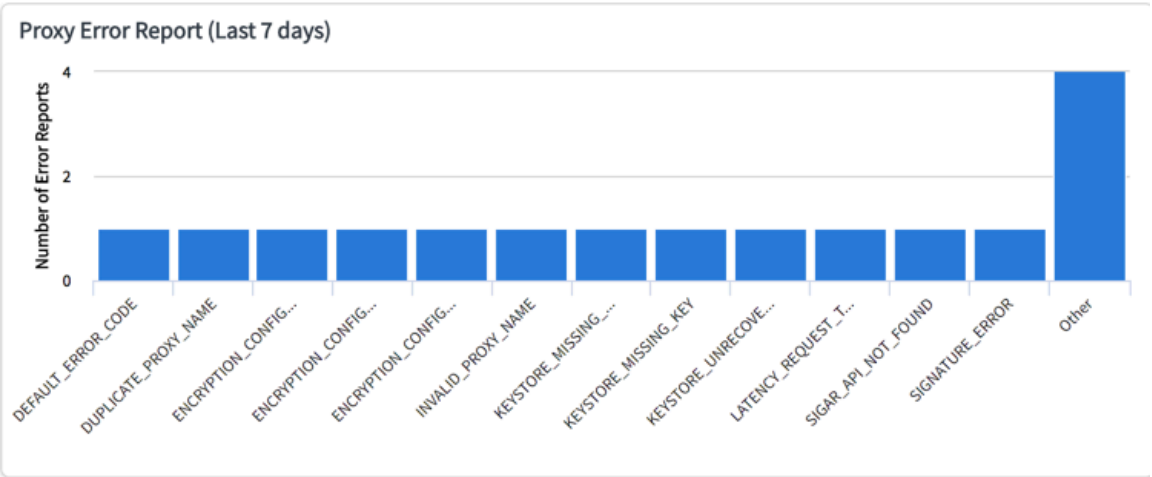
- Uso de CPU
- Uso da memória
- Uso de disco

Latência do proxy de borda

Latência máxima e média da rede em milissegundos em um determinado ponto no tempo. A latência é determinada pelo tempo de ida e volta para um servidor proxy enviar um ping simples para a instância e receber uma resposta.

Relatórios de erro de proxy

Navegue até o **Configuração de Edge Encryption** > **Diagnóstico e solução de problemas** > **Relatórios de erro de proxy** para exibir todos os erros do servidor proxy coletados nos últimos sete dias.



Os erros são coletados durante um período de um minuto. A cada minuto, um relatório de erro é gerado. O eixo vertical exibe o número de relatórios de erro nos últimos sete dias que incluem cada erro. Por exemplo, mesmo se o erro "DEFAULT_ERROR_CODE" for gerado várias vezes ao longo de um período de relatório de um minuto, a barra "DEFAULT_ERROR_CODE" atingirá apenas o número um no eixo **Número de relatórios de erro**.

Nessa exibição, você pode:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Clicar em cada barra de código de erro de proxy para ver o relatório sobre um único erro para cada servidor proxy. Nessa exibição, você pode clicar novamente na barra para exibir o texto de erro na tabela Estatística de proxy Edge Encryption [edge_encryption_stat]. Siga os links no texto de erro para ver mais informações e possíveis etapas de correção.
- Clique em **Outro** para ver a página dois do relatório de erro.

Nota: Se você tiver mais de um servidor proxy com o mesmo nome, será exibido um único erro "DUPLICATE_PROXY_NAME" no Relatório de erro de proxy. Nenhum outro erro é relatado para servidores proxy com nomes duplicados. Se você encontrar este erro, certifique-se de que todos os servidores proxy tenham nomes exclusivos.

Recursos adicionais de monitoramento

A instância rastreia todos os proxies de criptografia. Cada servidor proxy Edge Encryption é registrado ao ser inicializado. A instância é notificada quando:

- Um novo servidor proxy Edge Encryption é inicializado.
- Um servidor proxy Edge Encryption foi encerrado intencionalmente.

Se um servidor proxy Edge Encryption tentar registrar-se com uma instância que não tenha Edge Encryption instalado, o proxy não será iniciado.

Todos os arquivos de configuração de criptografia são auditados. Os registros excluídos são auditados em todos os arquivos de configuração de criptografia. Os registros de auditoria são adicionados na tabela "sys_audit". Para exibir o histórico de um registro de configuração específico, abra o registro e clique em **Histórico** > **Lista** no menu. O Trabalho de criptografia em massa não é auditado.

Use os seguintes recursos adicionais para monitorar seus servidores proxy.

Tabela	Descrição
Tentativas de inserção inválidas [sys_edge_encryption_invalid_insert_log]	Lista de tentativas de salvar os seguintes dados em campos criptografados: • Dados não criptografados. • Dados que não vieram de um proxy Edge Encryption. A instância rejeita e registra qualquer tentativa de salvar esses dados. Se você tiver a função de administrador de segurança, poderá exibir os logs na lista Tentativas de inserção inválidas.
Falhas de trabalho [sys_encryption_job_execution]	Uma lista de trabalhos que não foram executados com sucesso.
Logs do sistema	A instância verifica periodicamente se há mensagens de cada servidor proxy registrado. Se um servidor proxy não tiver enviado uma mensagem no intervalo de tempo necessário, um erro será registrado. A mensagem de log contém informações sobre o proxy de criptografia e a última vez em que o proxy fez ping na instância. Se a instância determinar que nenhum dos proxies de

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Descrição
	criptografia está online, uma mensagem será registrada. Essas mensagens são adicionadas ao log do sistema.

Como desabilitar ou reduzir a coleta de estatísticas do Edge Proxy

Impeça que o servidor proxy Edge Encryption envie estatísticas do Conjunto de gráficos do Edge Proxy para a página inicial de Desempenho ServiceNow ou reduza a frequência da coleta de estatísticas.

Antes de Iniciar
Função necessária: admin ou security_admin

Por Que e Quando Desempenhar Esta Tarefa
Ao adicionar propriedades no arquivo de configuração `edgeencryption.properties`, você pode:

- Desabilitar o conjunto de gráficos do Edge Proxy.
- Alterar o intervalo durante o qual as estatísticas são coletadas pelo servidor proxy Edge Encryption. Por padrão, as estatísticas são coletadas a cada 30 segundos.

Procedimento

1. No diretório de instalação do servidor proxy, abra o arquivo de configuração `edgeencryption.properties` localizado na pasta `<installation directory>/conf/`.
2. Adicione uma das Propriedades do servidor proxy do Edge Encryption.
3. Reinicie o servidor proxy.

Como aumentar a depuração do registro em log para o proxy Edge Encryption

Aumente o nível de registro em log para interpretar os logs e depurar problemas com o proxy.

No momento, há três opções para aumentar a depuração do registro em log no proxy Edge Encryption. Aumentar o nível de registro em log para depurar problemas fornece informações ao suporte técnico para analisar o problema com o benefício de declarações de log mais detalhadas.

Dependendo do problema que está sendo depurado, configure a depuração do registro em log de uma das três maneiras:

- Depuração de problemas diferentes da conectividade SSL
- Métricas de tempo de registro em log para solicitações por meio do proxy
- Depuração de problemas com conectividade SSL entre o proxy Edge Encryption e a instância

Para todos os casos de depuração, você pode exibir e interpretar os logs por conta própria ou abrir um incidente para obter uma interpretação do suporte técnico da ServiceNow fornecendo a descrição do problema e como ele é reproduzido.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Depuração de problemas com a aplicação Edge Encryption diferente da conectividade SSL

Use este método para depurar problemas com a aplicação Edge Encryption, sem parar e reiniciar o proxy. Essas etapas aumentam o nível de registro em log e ajudam a solucionar problemas de causa raiz com mais declarações de log detalhadas.

Antes de Iniciar

Função necessária: admin

Nota: As mudanças feitas no arquivo `$proxy_installation_location/conf/log4j2.properties` são aceitas pelo proxy em cerca de 60 segundos após você fazer suas mudanças. Você não precisa reiniciar os proxies.

Procedimento

1. No arquivo `$proxy_installation_location/conf/log4j2.properties`, localize a seguinte linha.

```
logger.edge.level=info
```

2. Mude a linha acima para:

```
logger.edge.level=debug
```

3. Salve a mudança.
   Pode levar até 60 segundos para que a mudança seja aplicada, mas isso não requer uma reinicialização do proxy.
4. Reproduza seu problema.
5. Verifique se há declarações de log de depuração relacionadas à aplicação no arquivo `$proxy_installation_location/logs/edgeencryption.log`.

Resultados

Depois de fazer a mudança de propriedade, você pode ver detalhes adicionais no arquivo `$proxy_installation_location/logs/edgeencryption.log`. Quando terminar a depuração, reverta a mudança feita no arquivo `$proxy_installation_location/conf/log4j2.properties`.

Métricas de tempo de registro em log para solicitações por meio do proxy

Habilite uma métrica de tempo de registro em log para adicionar uma declaração de métrica para cada solicitação tratada pelo proxy Edge Encryption. Cada uma dessas declarações de métrica de tempo de registro em log contém informações úteis sobre a solicitação, como tempos de processamento e qual regra de criptografia foi usada.

Antes de Iniciar

Função necessária: administrador

Nota:

As demais configurações de registro em log são adicionadas ao arquivo `$proxy_installation_location/conf/log4j2.properties`. As mudanças feitas são aceitas dinamicamente pelo proxy em cerca de um minuto após as mudanças no arquivo serem feitas. Dessa forma, você não precisa reiniciar os proxies.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Modifique o arquivo `$proxy_installation_location/conf/log4j2.properties` adicionando as seguintes linhas no fim do arquivo

```
appender.timinglog.type=RollingFile
appender.timinglog.name=TimingLog
appender.timinglog.fileName=../logs/edgenetwork.log
appender.timinglog.filePattern=../logs/$
${date:yyyy-MM}/edgenetwork-%d{yyyy-MM-dd-HH}-%i.log.gz
appender.timinglog.layout.type=PatternLayout
appender.timinglog.layout.pattern=%d [%t] %-5p %m%n
appender.timinglog.policies.type=Policies
appender.timinglog.policies.size.type=SizeBasedTriggeringPolicy
appender.timinglog.policies.size.size=500MB
appender.timinglog.strategy.type=DefaultRolloverStrategy
appender.timinglog.strategy.max=4

logger.timing.name=com.snc.edgeencryption.metrics.EdgeEncryptionTimingM
etricCache
logger.timing.level=debug
logger.timing.additivity=false
logger.timing.appenderRef.rolling.ref=TimingLog
```

2. Salve o arquivo.

Resultados

Depois que o arquivo `log4j.properties` é salvo, os seguintes tipos de mensagens aparecem no arquivo de log `$proxy_installation_location/logs/edgenetwork.log` para tempos de rede.

```
2022-07-21 12:56:15,783 [qtp1971991758-7700] DEBUG
 com.snc.edgeencryption.metrics.EdgeEncryptionTimingMetricCache -
 request_uri=/api/now/ui/presencesysparm_auto_request=true&cd=1658433375
754 request_method=POST client_request_received="2022-07-21 12:56:15,015"
 proxy_request_processing_time=6 all_rules_processing_time=0
 rule_executed="REST JSON" rule_execution_time=1
 proxy_instance_round_trip=14 proxy_response_processing_time=1
 total_time_from_proxy=21 reponse_code=201
 glide_user=SCv3_1:BAz1ZK7ee9XoroG2nvMlixHpgTvsT4fY2bwQvnH2WdU=:y5HGsTTqo
3Pjq6G0xk4LoazCwCiWRJk4/6SpbXuBzqg=:6816f79cc0a8016401c5a33be04be441
 jsessionid_suffix=037A66
```

Os valores nas mensagens de log são os seguintes:

```
request_uri: The URI being requested

request_method: The HTTP method being used, for example, GET, POST, PUT,
 PATCH, DELETE

client_request_received: The timestamp noting when the HTTP client
 request arrived at the Edge proxy

proxy_request_processing_time: How long the Edge proxy took to process
 the request in milliseconds

all_rules_processing_time: Total time it took to execute all of the Edge
 Encryption rules for the request in milliseconds
```

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

```
rule_executed: The name of the encryption rule that was executed

rule_execution_time: How long it took to execute listed rule_executed in
 milliseconds

proxy_instance_round_trip: The time from when the Edge proxy sent the
 request to the instance until the instance sent the response and was
 received by the edge proxy in milliseconds

proxy_response_processing_time: How long the Edge proxy took to process
 the response in milliseconds

total_time_from_proxy: The total time from when the Edge proxy received
 the request from the client and returned the response to the client in
 milliseconds

response_code: HTTP response code

glide_user: The glide_user cookie value

jsessionid_suffix: The JSession cookie suffix associated with the request
```

Como depurar problemas com conectividade SSL entre o proxy Edge Encryption e a instância

Use este método para depurar problemas com conectividade SSL entre o proxy Edge Encryption e sua instância, como falha de acesso à instância por meio do proxy. Essas etapas aumentam o registro em log e ajudam a encontrar declarações de log detalhadas.

Antes de Iniciar

Função necessária: admin

Nota: A depuração de conectividade SSL só é relevante ao solucionar problemas do tipo de conectividade TLS. Na prática, isso não é comum e raramente necessário.

Procedimento

1. Interrompa o servidor proxy.
2. Adicione a seguinte linha ao arquivo `$proxy_installation_location/conf/wrapper.conf`, que é uma propriedade de inicialização do Java:

   ```
   wrapper.java.additional.<next available number in sequence> =
    -Djavax.net.debug=all
   ```

   Por exemplo:

   ```
   For example: wrapper.java.additional.4 = -Djavax.net.debug=all
   ```

3. Salve a mudança e reinicie o servidor proxy.
4. Reproduza seu problema de conectividade.

Resultados

Depois de reproduzir a depuração do problema, as declarações do log relacionadas à troca de SSL podem ser encontradas no arquivo `$proxy_installation_location/logs/wrapper_<current date>.log`. Quando terminar a depuração, você pode remotamente

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

fazer o registro em log adicional removendo ou comentando a linha criada nas etapas anteriores.

Criptografia de banco de dados

A ServiceNow® oferece criptografia de banco de dados (DBE) e métodos de criptografia de disco completo para clientes com obrigações estatutárias de proteção de dados que podem exigir proteção em repouso para todos os dados.

Importante: A partir da versão Washington DC, o Database Encryption está sendo preparado para descontinuação futura. A Criptografia da nuvem é a solução de substituição para criptografia de dados em repouso. Para obter detalhes, consulte Criptografia da nuvem com gerenciamento de chave

Explorar Conheça os recursos e o valor comercial do Database Encryption.	Requisição Saiba mais sobre como solicitar a rotação de chave do banco de dados.
Referência A DBE-CCS (Database Encryption with Customer-Controlled Switch, Criptografia de banco de dados com switch controlado pelo cliente) é uma solução de criptografia que criptografa todos os dados em repouso quando eles não estão em uso no banco de dados.	

Explorando a criptografia de banco de dados

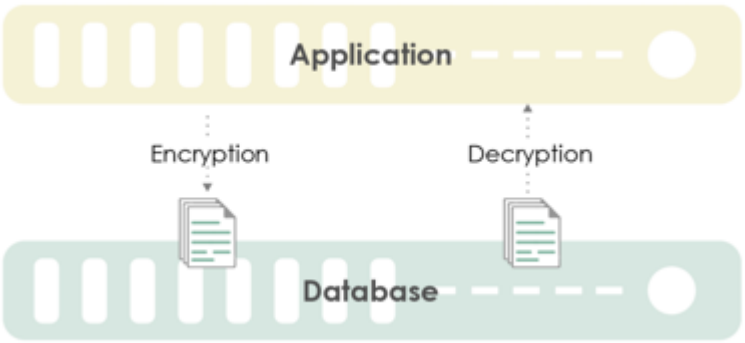
A ServiceNow® oferece criptografia de banco de dados (DBE) e métodos de criptografia de disco completo para clientes com obrigações estatutárias de proteção de dados que podem exigir proteção em repouso para todos os dados.

Importante: A partir da versão Washington DC, o Database Encryption está sendo preparado para descontinuação futura. A Criptografia da nuvem é a solução de substituição para criptografia de dados em repouso. Para obter detalhes, consulte Criptografia da nuvem com gerenciamento de chave

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A Criptografia de banco de dados permite que todos os dados sejam protegidos com criptografia AES-256 simétrica, esteja o banco de dados online ou offline. Da perspectiva da Now Platform, todos os fluxos de dados são descriptografados.

- A Criptografia de banco de dados oferece suporte a todos os dados armazenados para serem criptografados em tempo real, fornecendo proteção para os dados on-line e off-line sem perda de funcionalidade.
- A criptografia de disco completo protege os dados off-line em caso de perda ou roubo de disco.

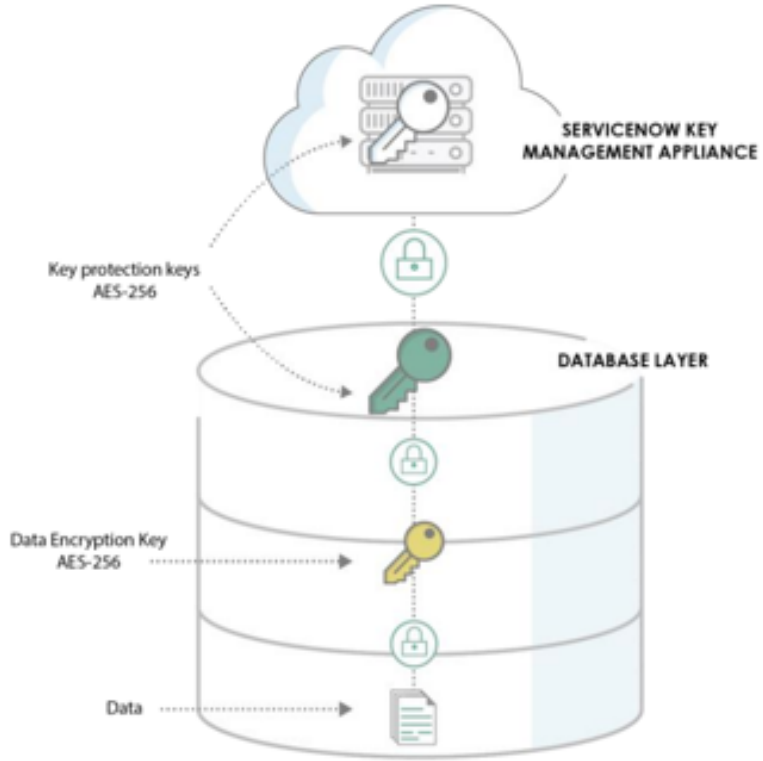


Com a criptografia de banco de dados, todos os dados armazenados são criptografados e os registros ou tabelas individuais são descriptografados na memória enquanto são acessados. Os dados novos ou alterados são criptografados conforme são inseridos em uma tabela e os arquivos de log de atividade associados (bin, refazer, desfazer e erro) também são criptografados.

A criptografia de banco de dados é transparente para os usuários, sem perda de funcionalidade. Ao usar este recurso, todas as instâncias são criptografadas, junto com o tráfego de replicação e os backups. A clonagem de instância ainda está disponível com um impacto mínimo no desempenho de até 5% para usar a Criptografia de banco de dados. As instâncias novas e existentes em versões compatíveis do Now Platform podem aproveitar a criptografia do banco de dados.

Conforme ilustrado, ServiceNow armazena e gerencia chaves usando uma hierarquia de chave de três níveis:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



1. Uma chave AES-256 específica do cliente é criada pelo mecanismo de banco de dados e é usada para criptografar os dados.
2. Uma segunda chave AES-256 específica do cliente é criada pelo mecanismo de banco de dados e usada para proteger a chave de primeiro nível.
3. Uma terceira chave AES-256 é criada e armazenada nos dispositivos de gerenciamento de chaves validados FIPS 140 nos datacenters da ServiceNow. Esta chave protege a chave de segundo nível e é exclusiva por instância de cliente.

A Now Platform também oferece suporte à criptografia de banco de dados com um comutador fornecido pelo cliente, DBE com CCS. Essa é uma solução de criptografia que criptografa todos os dados em repouso quando não estão em uso no banco de dados. Ela usa criptografia AES padrão do setor sem afetar a funcionalidade. O banco de dados criptografa os dados conforme eles são gravados no disco e descriptografa os dados conforme eles são lidos do disco. Isso significa que as aplicações sempre terão os dados em um estado não criptografado para executar a lógica e as funções necessárias.

Nota: A criptografia de banco de dados não é compatível com instâncias no local.

Se estiver usando suas próprias chaves de criptografia de banco de dados, consulte Criptografia de banco de dados com comutador controlado pelo cliente.

Solicitar rotação de chaves do banco de dados

Gire a chave do banco de dados anualmente ou conforme necessário enviando uma solicitação ao suporte.

Antes de Iniciar
Função necessária: administrador

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Importante: A partir da versão Washington DC, o Database Encryption está sendo preparado para descontinuação futura. A Criptografia da nuvem é a solução de substituição para criptografia de dados em repouso. Para obter detalhes, consulte Criptografia da nuvem com gerenciamento de chave

Por Que e Quando Desempenhar Esta Tarefa
A rotação de chave ocorre à noite nas 24 horas anteriores à data de expiração e não interrompe o serviço da instância.

Nota: Atualmente, a rotação de chave está disponível somente nos ambientes ServiceNow Comercial, GCC (Government Community Cloud), França e Cingapura.

Procedimento

Entre em contato com o Suporte e atendimento ao cliente para solicitar qualquer uma das seguintes ações de rotação:

- Inscrever-se para executar a rotação anual de chaves em todas as instâncias designadas.
- Obter um relatório histórico das últimas três rotações de chave contendo:
  - Nome da instância
  - Nome e versão da chave.
  - Datas e horários de rotação.
- Programar uma rotação de chave antecipada fora da rotação anual programada.

Criptografia de banco de dados com comutador controlado pelo cliente

A DBE-CCS (Database Encryption with Customer-Controlled Switch, Criptografia de banco de dados com switch controlado pelo cliente) é uma solução de criptografia que criptografa todos os dados em repouso quando eles não estão em uso no banco de dados.

Visão geral

A Criptografia de banco de dados com switch controlado pelo cliente usa a criptografia AES padrão do setor, sem impactos na funcionalidade. O banco de dados criptografa os dados conforme eles são gravados no disco e são descriptografados pelo banco de dados conforme são lidos do disco. As aplicações sempre têm os dados em um estado não criptografado para executar a lógica e as funções necessárias.

O DBE-CCS utiliza tecnologia nativa do banco de dados, geralmente chamada de Tablespace Encryption ou Transparent Data Encryption. Para obter mais detalhes sobre a tecnologia, consulte o site MariaDB em "Criptografia de Tablespace".

O DBE-CCS requer que você configure um endpoint REST HTTPS que fornece periodicamente a chave secreta para a instância ServiceNow. O endpoint do CCS retorna a chave secreta do cliente criptografada com a chave pública da instância do banco de dados.

Endpoint do cliente

Importante: Sua organização é a única responsável pela configuração e manutenção do endpoint do CCS. A especificação do endpoint do cliente é fornecida em KB0789788.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Um parceiro de tecnologia da ServiceNow, Fortanix, está disponível para implementar o endpoint do cliente para você. Entre em contato diretamente com o parceiro de tecnologia para obter detalhes da integração. Para saber mais, consulte Como usar o Fortanix Data Security Manager com a ServiceNow.

Compatível com várias versões ServiceNow

Importante: A Criptografia de Banco de Dados é uma oferta de infraestrutura paga independente de versão. Ela pode ser aplicada a qualquer versão com suporte e a instâncias novas ou existentes.

Outras referências

Consulte essas referências para obter informações adicionais sobre DBE com CCS:

Referência	Descrição
KB0993681	Architecture of Database Encryption Customer Controlled Switch (Arquitetura da criptografia de banco de dados com comutador controlado pelo cliente)
KB0789788	Guia de implementação da DBE com CCS

Nota: Para acessar artigos da base de conhecimento, você deve primeiro realizar a autenticação em Now Support.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Gestão de acessos

O Gerenciamento de acesso permite que você tenha acesso à instância do ServiceNow® com segurança.

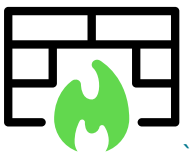
Zero Trust Access

O Zero Trust Access garante que todos os acessos a aplicações e dados sejam concedidos com base em privilégio mínimo, após a verificação da identidade do usuário e uma avaliação de risco.

Separação de domínios

Com a Plataforma ServiceNow, os SPs (Service providers, provedores de serviço) podem oferecer aos clientes uma integração mais rápida, atender às exigências de conformidade e proteger dados usando a separação de domínios.

Autenticação

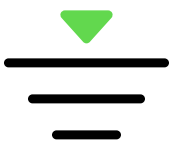


A autenticação da ServiceNow valida a identidade de um usuário que acessa uma instância e, em seguida, autoriza o usuário a acessar recursos que correspondem à função do usuário ou à função de trabalho.

ACL

As regras das listas de controle de acesso (ACLs) restringem o acesso aos dados exigindo que os usuários passem por um conjunto de requisitos antes de interagir com eles.

Filtragem de dados



Use a filtragem de dados para controlar o acesso a tabelas e registros com base nos atributos do assunto ao executar consultas de leitura.

Funções de segurança

Funções de segurança fornecem segurança extra, de forma que cada usuário deve ter pelo menos uma função para que a instância possa distinguir entre usuários internos e externos.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Conexões e credenciais

As credenciais e as informações de conexão são necessárias para obter acesso a um computador ou dispositivo de rede para Descoberta, Mapeamento de serviços e Gestão de nuvem ou para executar o trabalho usando Orquestração.

Controle de acesso da ServiceNow

O plug-in Controle de acesso de SNC permite que você controle quais funcionários de Suporte e atendimento ao cliente podem acessar sua instância e quando.

Zero Trust Access

O ZTA (Zero Trust Access, acesso de confiança zero) é um modelo de segurança que pressupõe que nenhum usuário ou dispositivo é confiável por padrão.

Explorar

Conheça os recursos e o valor comercial do Zero Trust Access.

Ativar

Entenda como ativar o acesso Zero Trust.

Configurar

Referência - Propriedades

Conheça as propriedades do Zero Trust Access.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Explorar o Zero Trust Access

O ZTA (Zero Trust Access, acesso de confiança zero) é um modelo de segurança que pressupõe que nenhum usuário ou dispositivo é confiável por padrão.

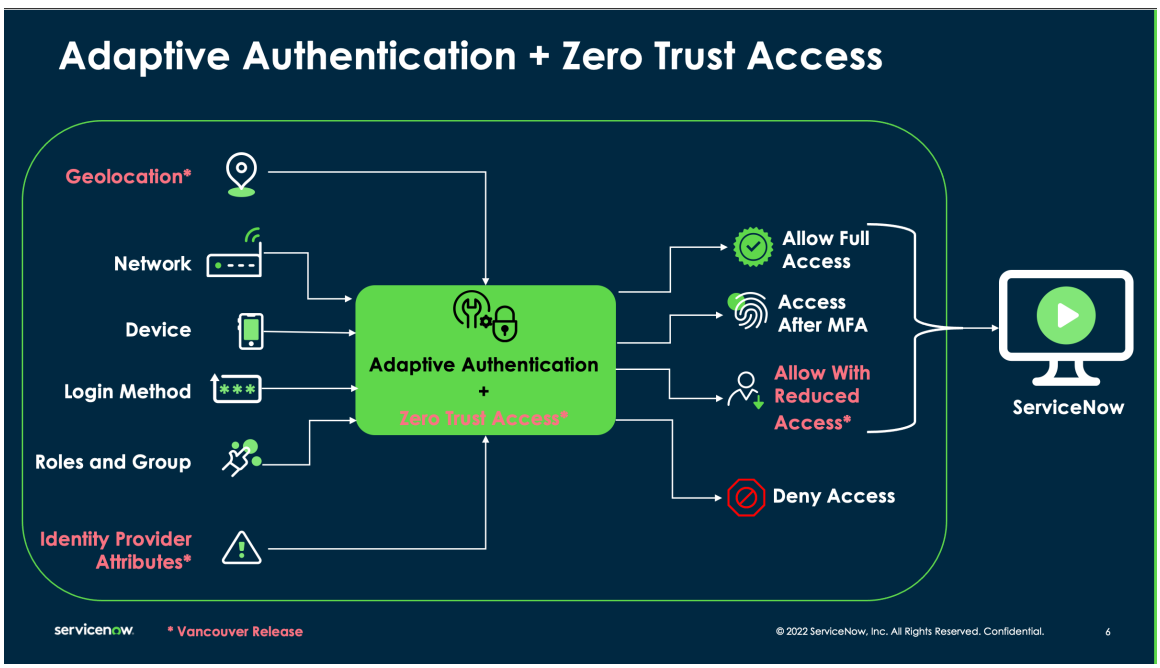
O ZTA garante que todos os acessos a aplicações e dados sejam concedidos com base em privilégio mínimo, após a verificação da identidade do usuário e uma avaliação de risco.

Política de acesso à sessão baseada em confiança zero

ServiceNowA Política de acesso à sessão baseada em confiança zero permite que as organizações reduzam dinamicamente os privilégios do usuário em uma sessão da Web com base em vários fatores, incluindo endereço IP, localização, método de autenticação, funções do usuário, grupo, presença de MFA e atributos compartilhados pelo Provedor de identidade (IDP). Isso pode ajudar a proteger as organizações contra acessos não autorizados e violações de dados, mesmo quando usuários com altos privilégios acessam aplicativos a partir de dispositivos ou locais não confiáveis.

Zero Trust - acesso à sessão baseada em política

Permite que os administradores de segurança reduzam o acesso dos usuários a sessões baseados em endereço IP, localidade, atributos do Provedor de identidade e atributos de usuários usando políticas de autenticação adaptável.



© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

- As configurações de Acesso à sessão só podem ser realizadas com a função `security_admin`. Promova sua função para `security_admin`.
- O Acesso à sessão não é compatível com integrações.
- O Acesso à sessão não tem impacto se a função reduzida ou limitada não for atribuída a um usuário. Nesse caso não haverá mudanças na sessão conectada. O usuário continuará acessando a instância com os privilégios atribuídos.
- O Acesso à sessão não tem impacto enquanto o usuário estiver conectado à instância e, simultaneamente, o administrador configurar a política. O usuário precisa encerrar a sessão para que a política seja aplicada.
- O acesso à sessão não é impactado quando o usuário está em uma rede confiável e, posteriormente, muda para uma VPN (mudança de local ou rede) em uma sessão.
- O Acesso à sessão é imposto no momento do login. Mudanças nos parâmetros de risco durante a sessão não resultarão na redução do acesso. Por exemplo, um usuário que sair da rede corporativa para uma rede não confiável após estabelecer a sessão não terá seu acesso reduzido. Isso é, a menos que o usuário encerre a sessão e faça login novamente.

Caso de uso

A seguir você encontrará alguns casos de uso do Zero Trust Access:

- Reduza os privilégios com base no risco associado à sessão. Por exemplo, um usuário com função de executante que faz login de fora da rede confiável pode ser configurado para ter somente a função de solicitante para a sessão.
- Reduza o acesso com base na resposta do IDP para uma sessão de usuário se ele estiver usando um dispositivo não confiável. Para obter mais informações, consulte Configurar atributo IDP para acesso à sessão.

Esse rebaixamento de função garante que o usuário não tenha outras permissões em uma sessão. Quando o usuário fizer login de uma rede confiável, todas as permissões serão atribuídas a essa sessão.

Várias condições de IP e várias atribuições de função ou grupo podem ser definidas como parte da política.

Zero Trust Access - Dispositivos móveis

Você pode usar a política Zero Trust Access - Acesso à sessão na política Autenticação adaptável para reduzir as funções ou os privilégios da sessão específica em dispositivos móveis.

Você pode ativar o Zero Trust Access – Acesso à sessão em dispositivos móveis habilitando **glide.authenticate.session_access.mobile.enabled** na tabela de propriedades do sistema.

Para usar o Zero Trust Access – Acesso à sessão em dispositivos móveis com os atributos de IDP, basta configurar o campo **glide.authenticate.session_access.mobile.refresh_token_interval**. Isso permitirá que os administradores controlem com eficácia o acesso à sessão com base no token de atualização.

Para obter mais informações, consulte Configurar acesso Zero Trust para dispositivos móveis.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Ativar Zero Trust Access

Ative a política de **Zero Trust - Acesso de sessão baseado na política** (`com.snc.zero_trust_session_access`) para permitir que os administradores de segurança reduzam ou limitem o acesso do usuário em uma sessão com base no endereço IP, no local, nos atributos do provedor de identidade e nos atributos do usuário usando políticas de autenticação adaptável.

Antes de Iniciar

Função necessária: admin

Procedimento

1. Navegue até **Todos** > **Aplicações do sistema** > **Todas as aplicações disponíveis** > **Todas**.
2. Encontre o plug-in **Zero Trust - Acesso de sessão baseado na política** (`com.snc.zero_trust_location_access`) usando os critérios de filtro e a barra de pesquisa.

   Pesquise o plug-in pelo nome ou ID. Se não conseguir encontrar um plug-in, talvez seja necessário solicitá-lo ao pessoal ServiceNow.
3. Selecione **Instalar** para iniciar o processo de instalação.

   Nota: Quando a separação de domínio e o administrador delegado estão habilitados em uma instância, o usuário administrativo deve estar no domínio **global**. Caso contrário, será exibido o seguinte erro: `A instalação da aplicação não está disponível porque há outra operação em execução: ativação de plug-in para <plugin name>.`

   Você verá uma mensagem após a conclusão da instalação.

Configurar função de acesso à sessão

Configure o Acesso à sessão para reduzir o acesso de usuários a sessões baseadas em IP, localidade, atributos do Provedor de identidade e atributos de usuários usando políticas de autenticação adaptável.

Antes de Iniciar

Função necessária: security_admin

Nota:

- As configurações de Acesso à sessão só podem ser realizadas com a função `security_admin`. Promova sua função para `security_admin`.
- O Acesso à sessão não é compatível com integrações.
- O Acesso à sessão não tem impacto se a função reduzida ou limitada não for atribuída a um usuário. Nesse caso não haverá mudanças na sessão conectada. O usuário ainda continuará acessando a instância com os privilégios atribuídos.
- O Acesso à sessão não tem impacto enquanto o usuário estiver conectado à instância e, simultaneamente, o administrador configurar a política. O usuário precisa encerrar a sessão para que a política seja aplicada.
- O Acesso à sessão é imposto no momento do login. Mudanças nos parâmetros de risco durante a sessão não resultarão na redução do acesso. Por exemplo, um usuário que sair da rede corporativa para uma rede não confiável após estabelecer a sessão não terá seu acesso reduzido. Isso é, a menos que o usuário encerre a sessão e faça login novamente.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegue até **"Todos"** > **"Acesso de confiança zero"** > **"Configurações de função de acesso à sessão"**.
2. Para criar uma configuração de função de acesso à sessão, selecione **"Novo"**.
3. No formulário, preencha os campos:

Configuração de função de acesso à sessão

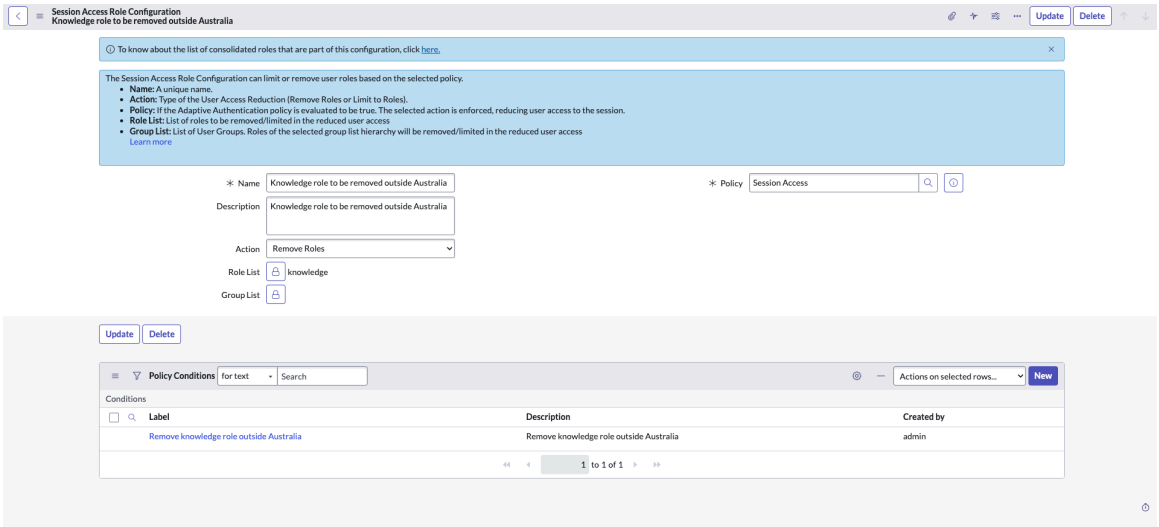
Campo	Descrição
Nome	Nome da configuração
Descrição	Descrição resumida da configuração
Política	Escolha a política de autenticação adaptável. Use o ícone de pesquisa para exibir a lista de políticas.
Ação	**"Remover funções"** ou **"Limitar funções"**. ◦ **Remover funções**: quando o usuário configurado está conectado, a lista de funções fornecida na função ou na Lista agrupada é removida da sessão. ◦ **Limitar a funções**: quando o usuário configurado está conectado, somente as funções selecionadas são fornecidas ao usuário e todas as outras funções são removidas da sessão.
Lista de funções	Escolha as funções na lista de funções.
Lista agrupada	Escolha as funções na Lista agrupada que você deseja remover ou limitar ao usuário.

4. Selecione **"Enviar"**.

O login para usuários com base nos países configurados ocorre da seguinte forma:

- Em **Remover funções**, os usuários dos países configurados com as funções selecionadas não mais têm essas funções para a sessão.
- Em **Limitar funções**, os usuários dos países configurados com as funções selecionadas só têm essas funções para a sessão.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

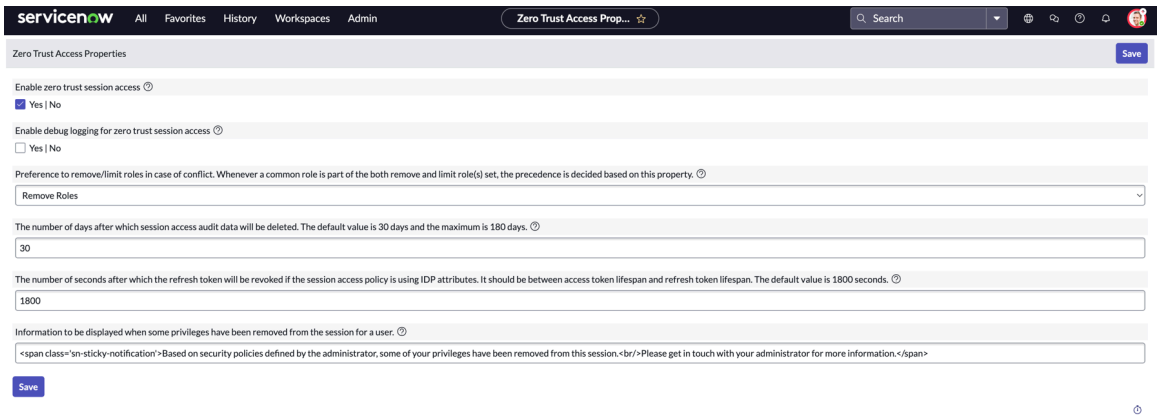


Para aprender mais sobre como remover ou limitar funções de uma sessão com um exemplo de caso de uso, consulte Tutorial: usar o acesso Zero Trust.

Propriedades do sistema de acesso Zero Trust

Use as propriedades do sistema para habilitar e personalizar o acesso Zero Trust para atender aos seus requisitos de segurança.

Propriedades



Propriedades do sistema de acesso Zero Trust

Propriedade	Descrição
Habilitar o acesso à sessão Zero Trust	Opção que permite que administradores usem o recurso de Acesso à sessão Zero Trust. O valor padrão é `falso`.
Habilitar registro em log de depuração para Acesso à sessão de Zero Trust	Opção para habilitar registro em log de depuração para acesso à sessão Zero Trust.
Preferência para remover/limitar funções em caso de conflito. Sempre que uma função comum fizer parte do conjunto de	**Remover funções** ou **Limitar funções**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Propriedades do sistema de acesso Zero Trust

Propriedade	Descrição
funções de remover e limitar, a precedência será decidida com base nessa propriedade.	
O número de dias após o qual os dados de auditoria de acesso à sessão serão excluídos. O valor padrão é 30 dias e o máximo é de 180 dias.	Por padrão, são 30 dias.
O número de segundos após os quais o token de atualização será revogado se a política de acesso à sessão estiver usando atributos de IdP. Deve ser um valor entre a vida útil do token de acesso e a vida útil do token de atualização. O valor padrão é de 1.800 segundos.	O valor padrão é de 1.800 segundos.
Informações a serem exibidas quando alguns privilégios forem removidos da sessão de um usuário.	Descrição que você deseja exibir para os usuários em relação à limitação ou remoção de privilégios. Descrição de exemplo: `Com base nas políticas de segurança definidas pelo administrador, algumas de suas funções foram removidas desta sessão. Entre em contato com o administrador para obter mais informações.`

Auditorias de acesso à sessão

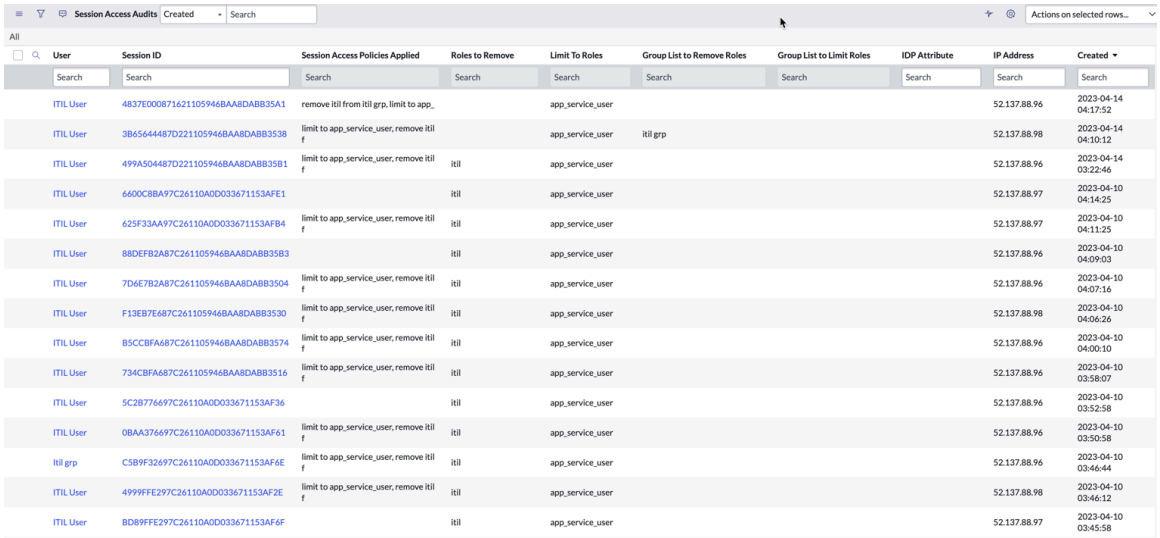
As auditorias de acesso à sessão exibem os logs de Acesso à sessão e as informações relacionadas à sessão de um usuário.

Auditorias

A auditoria de Acesso à sessão exibe as informações de auditoria da seguinte forma:

Nota: Use a propriedade `glide.authenticate.session_access.log_audit_event` para preencher as informações de auditoria.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Auditorias de acesso à sessão

Campo	Descrição
Usuário	Detalhes do usuário.
ID da Sessão	Detalhes sobre a sessão exibidos como um ID exclusivo.
Cliente Mobile	Os detalhes do cliente móvel. **ServiceNow Agent** (Now Agent) e **Solicitação da ServiceNow** (Now Mobile).
Políticas de acesso à sessão aplicadas	A políticas de Acesso à sessão que é aplicada.
Funções a serem removidas	Funções que foram removidas do usuário durante o registro em log.
Limitar às funções	Funções que foram limitadas para o usuário durante o registro em log.
Lista agrupada para remover funções	Informações sobre o grupo que removeu as funções do usuário.
Lista agrupada para limitar funções	Informações sobre o grupo que limitou as funções do usuário.
Cliente Mobile	Detalhes do usuário conectado pelo dispositivo móvel que teve o acesso reduzido ou removido.
Atributo de IdP	O IDP que foi usado para essa sessão.
Endereço IP	Detalhes do endereço IP usado pelo usuário para fazer login.
Criado em	Detalhes da data e hora do registro do usuário criado.

Tutorial: usar o acesso Zero Trust

Procedimento para usar o recurso acesso Zero Trust em um caso de uso de ponta a ponta.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Função necessária: security_admin

Habilite a propriedade **habilitar acesso à sessão**.

Nota:

- As configurações de Acesso à sessão só podem ser realizadas com a função `security_admin`. Promova sua função para `security_admin`.
- O Acesso à sessão não é compatível com integrações.
- O Acesso à sessão não tem impacto se a função reduzida ou limitada não for atribuída a um usuário. Nesse caso não haverá mudanças na sessão conectada. O usuário ainda continuará acessando a instância com os privilégios atribuídos.
- O Acesso à sessão não tem impacto enquanto o usuário estiver conectado à instância e, simultaneamente, o administrador configurar a política. O usuário precisa encerrar a sessão para que a política seja aplicada.
- O Acesso à sessão é imposto no momento do login. Mudanças nos parâmetros de risco durante a sessão não resultarão na redução do acesso. Por exemplo, um usuário que sair da rede corporativa para uma rede não confiável após estabelecer a sessão não terá seu acesso reduzido. Isso é, a menos que o usuário encerre a sessão e faça login novamente.

O Acesso à sessão é um recurso que permite aos administradores reduzir ou restringir dinamicamente um conjunto de funções para o usuário quando ele estiver tentando fazer login na instância a partir de ambientes diferentes, como logins de redes não confiáveis, dispositivos diferentes e assim por diante.

O acesso à sessão pode ser controlado pela política criada e pela ação selecionada ao executar a configuração. Estes são alguns dos cenários:

- Quando a política for verdadeira e a ação de funções estiver definida como **"Remover funções"**, as funções selecionadas e as funções secundárias associadas serão removidas para o usuário ao tentar fazer login na instância.
- Quando a política for verdadeira e a ação de funções estiver definida como **"Limitar às funções"** somente as funções selecionadas e suas funções secundárias associadas serão atribuídas ao usuário ao tentar fazer login na instância.

O procedimento a seguir explica uma configuração ponta a ponta da configuração de acesso à sessão com base na qual a função é limitada ao usuário que está fazendo login na instância. Da mesma forma, você também pode remover funções selecionando a opção **"Remover funções"** durante a configuração.

Procedimento

1. Navegue até **"Todos"** > **"Acesso à sessão"** > **"Configurações de função de acesso à sessão"**.
2. Na página "Configurações de função de acesso à sessão", selecione **"Novo"**.
3. Para limitar qualquer função do usuário, preencha os campos a seguir no formulário:
   - Nome
   - Descrição
   - Política
   - Ação

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Lista de funções
- Lista agrupada

a. Escolha **"Limitar às funções"** para limitar as funções do usuário.
Por exemplo: **itil**.

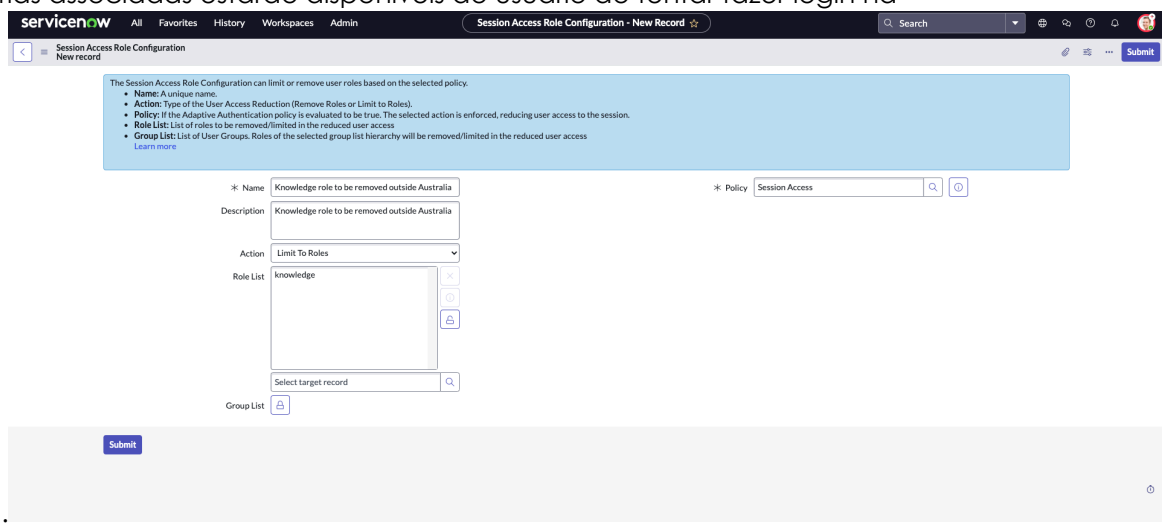
b. Escolha a função **conhecimento** na lista de funções.

c. Escolha a **Política**.

Você pode criar a política de Acesso à sessão usando uma política de autenticação e critérios de filtro (função, grupo, IP, local) com políticas de entrada e condições.

Use a política na configuração de Acesso à sessão. Por exemplo, se quiser limitar a função (conhecimento) do usuário que faz login fora do local (nesse caso, Austrália).

d. Escolha a Ação como **"Limitar às funções"**.
Quando a política for verdadeira, somente as funções selecionadas e suas funções secundárias associadas estarão disponíveis ao usuário ao tentar fazer login na instância.



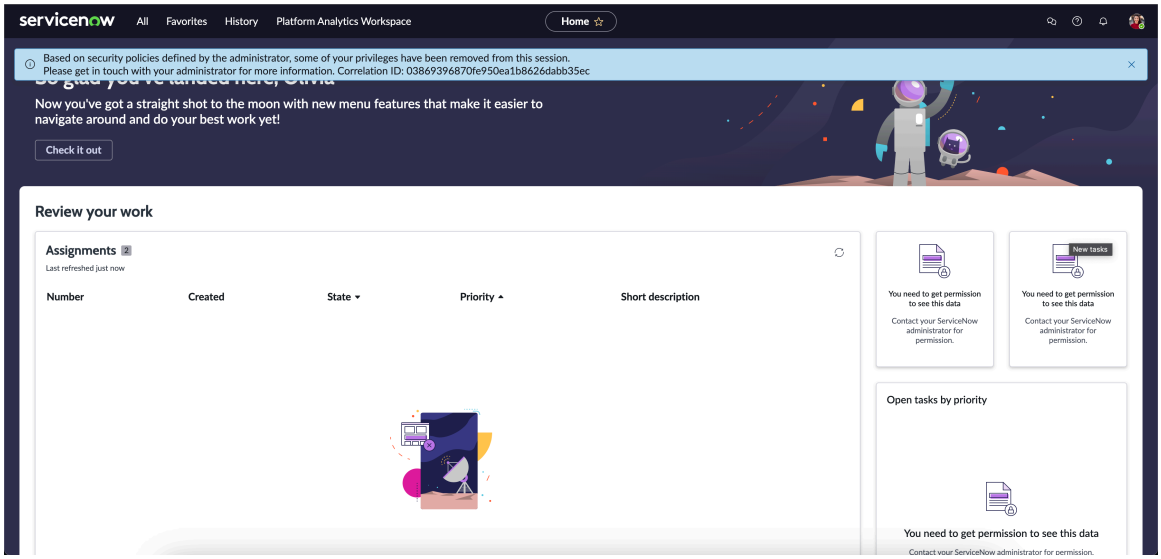
e. Selecione **Enviar**.

Da mesma forma, você pode escolher o grupo na Lista agrupada para restringir ou remover funções dos usuários dentro do grupo.

Quando o usuário faz login na instância fora da Austrália, somente a função de **Conhecimento** e suas funções secundárias associadas são atribuídas à sessão registrada e outras funções do usuário são restritas.

Após o login, o usuário receberá a seguinte mensagem de erro na plataforma no seu perfil:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



O usuário deve entrar em contato com os administradores e fornecer o ID de correlação para averiguação.

Nota: O ID de correlação é o sys_id do registro de auditoria correspondente na tabela de auditoria de acesso à sessão.

Configurar atributo IDP para acesso à sessão

Use o atributo Provedor de identidade (IDP) criado a partir da resposta do SAML (Security Assertion Markup Language, Linguagem de marcação de segurança) para remover ou restringir o acesso do usuário à sessão da instância.

Antes de Iniciar

Função necessária: security_admin

Habilite a **propriedade habilitar acesso à sessão**.

Nota: Para usar a configuração de função de acesso à sessão, se promova como `security_admin`.

O acesso à sessão pode ser controlado pela política criada e pela ação selecionada ao executar a configuração. Estes são alguns dos cenários:

- Quando a política for verdadeira e a ação de funções estiver definida como **Remover funções** junto com a entrada e a condição do atributo IDP, as funções selecionadas e suas funções secundárias associadas serão removidas para o usuário ao tentar fazer login na instância.
- Quando a política for verdadeira e a ação de funções estiver definida como **Limitar às funções** junto com a entrada e a condição do atributo IDP, as funções selecionadas e suas funções secundárias associadas serão atribuídas ao usuário ao tentar fazer login na instância.

O procedimento a seguir mostra as etapas para configurar o atributo IDP a partir da resposta do SAML, uma entrada de política para controlar o acesso à sessão.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegue até **"Todos"** > **"Acesso à sessão"** > **"Configurações de função de acesso à sessão"**.
2. Na página "Configurações de função de acesso à sessão", selecione **"Novo"**.
3. Para remover qualquer função do usuário, preencha os campos a seguir no formulário:
   - Nome
   - Descrição
   - Política
   - Ação
   - Lista de funções
   - Lista agrupada

a. Escolha **"Remover funções"** para remover funções do usuário.
Por exemplo: **itil**.

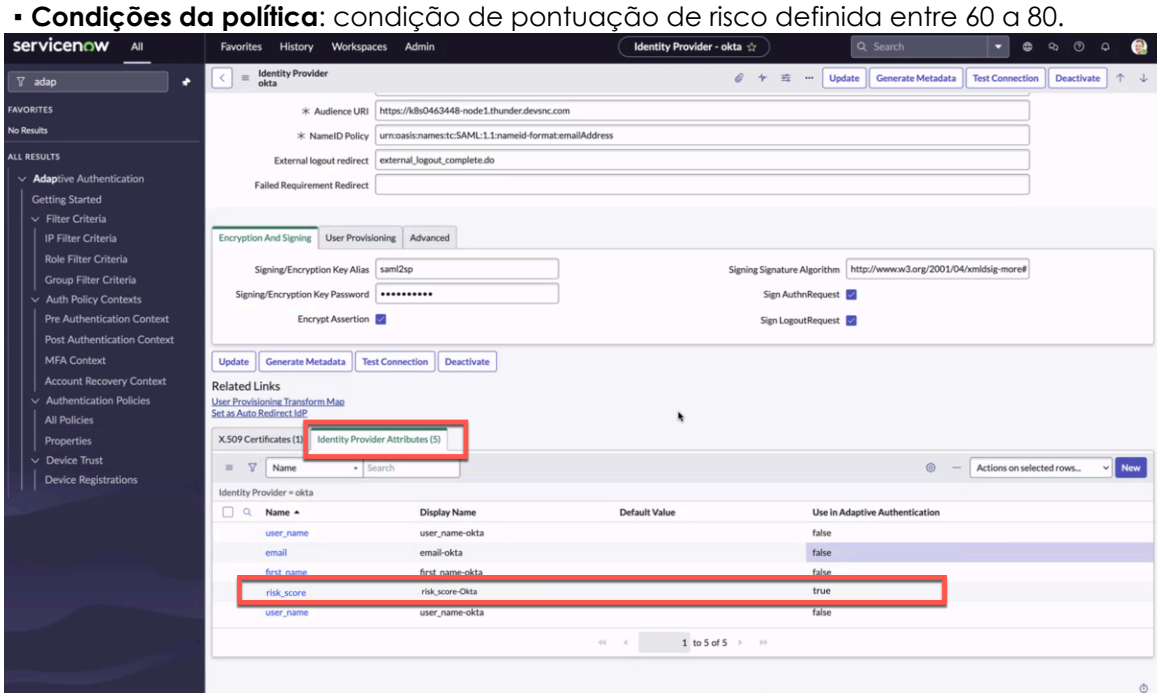
b. Escolha a função **itil** na lista de funções.

c. Escolha a **Política**.
Para saber mais sobre como criar políticas usando diferentes critérios de filtro com a criação de política de Autenticação adaptável, consulte Critérios de filtro.

d. Escolha Ação como "Remover funções".
Quando a política for verdadeira e a ação de funções estiver definida como **"Remover funções"**, as funções selecionadas serão removidas para o usuário ao tentar fazer login na instância.

e. Na Entrada de política, crie a Entrada de política e a Condição de política.
Por exemplo:

- **Entrada de política**: atributo de pontuação de risco do Okta (IDP).
- **Condições da política**: condição de pontuação de risco definida entre 60 a 80.



© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Com base nesta configuração, quando o valor do atributo de pontuação de risco do Okta (IDP) passar de 80, o usuário não será autenticado com as funções (**funcionário**) e suas funções secundárias que foram removidas da instância, sendo autenticado somente com outras funções atribuídas. Se a pontuação de risco estiver entre 60 e 80, o usuário será autenticado na instância com todas as funções.

Para obter mais informações sobre como criar a Política do contexto de pós-autenticação com políticas de entrada e condição, consulte Contexto de pós-autenticação.

Nota: Se a propriedade **Habilitar acesso à sessão** estiver inativa, a configuração de Acesso à sessão não restringirá ou removerá as funções do usuário.

f. Selecione **Enviar**.

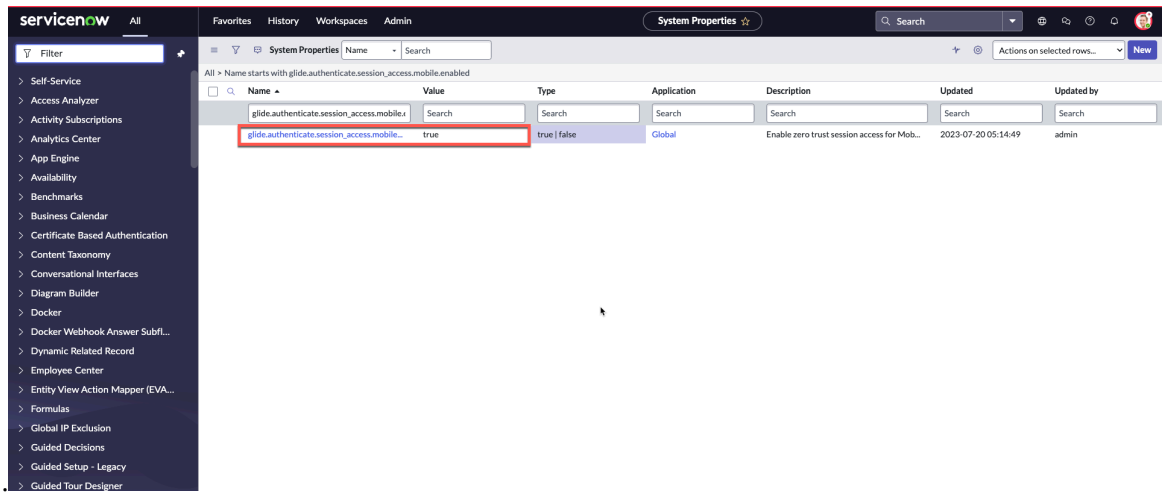
Zero Trust Access para dispositivos móveis

O ZTA (Zero Trust Access, acesso de confiança zero) é um modelo de segurança que pressupõe que nenhum usuário ou dispositivo é confiável por padrão.

Você pode usar a política Zero Trust Access - Acesso à sessão na política Autenticação adaptável para reduzir as funções ou os privilégios da sessão específica dos usuários em dispositivos móveis.

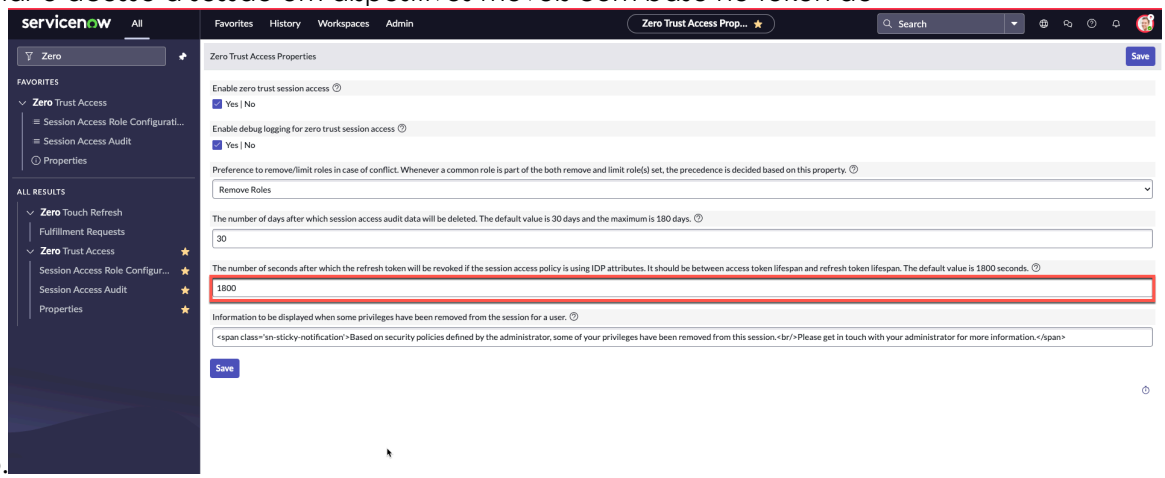
Para habilitar o Zero Trust Access no dispositivo móvel, você deve executar as seguintes tarefas:

- As configurações de Acesso à sessão só podem ser realizadas com a função `security_admin`. Promova sua função para `security_admin`.
- Ative a **Zero Trust - Acesso à sessão baseado em política** `com.snc.zero_trust_session_access`.
- Habilite o **glide.authenticate.session_access.mobile.enabled** na tabela de propriedades do sistema.



© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Configure o campo **glide.authenticate.session_access.mobile.refresh_token_interval** para controlar o acesso à sessão em dispositivos móveis com base no token de atualização.



Nota: Você deve configurar os segundos do token de atualização ao usar um IDP para logins por aplicativo para celular. Por padrão, os usuários são desconectados dos aplicativos para celular após 1.800 segundos (30 minutos).

- A opção Habilitar Zero Trust Access está habilitada em **Registros de aplicações** para a aplicação para celular do cliente (cliente OAuth). Nesse caso, **ServiceNow Agent** (Now Agent) e **ServiceNow Request** (Now Mobile).

- Configure a função de Acesso à sessão para reduzir ou remover funções dos usuários que fazem login com base nas entradas e condições da política. Para saber mais sobre a configuração, consulte Configurar função de acesso à sessão.

A configuração avalia o login para reduzir ou remover as funções dos usuários que acessam sua instância ServiceNow® com base nos filtros e nas condições da política. Para obter mais informações, consulte Configurar acesso Zero Trust para dispositivos móveis.

Domain Separation para provedores de serviço

Com a ServiceNow Plataforma, os provedores de serviço (SPs) podem fornecer a seus clientes uma integração mais rápida, atender à conformidade e proteger seus dados usando o Domain Separation. Você pode separar dados de cliente, processos e relatórios

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

em agrupamentos lógicos chamados de domínios. Os SPs controlam quem vê e acessa qual conteúdo.

Explorar Conheça a Separação de domínios.	Configurar Configure a Separação de domínios.
Consulta Veja os detalhes da Separação de domínios.	Analisar Saiba mais sobre como analisar a Separação de domínios

Explorando o Domain Separation

Com o Domain Separation, é possível separar dados, processos e tarefas administrativas em domínios definidos logicamente.

O Domain Separation é melhor para os clientes que:

- Precisam impor a segregação de dados absoluta entre entidades de negócios (separação de dados).
- Personalizam as definições do processo de negócios e as interfaces do usuário para cada domínio (administração delegada).
- Mantêm alguns processos e emissão de relatórios globais em uma única instância.
- Separam dados entre provedores de serviço, clientes, parceiros ou sub-organizações.
- Têm diferenças de processo pequenas ou moderadas entre os clientes.

O Domain Separation em comparação a instâncias separadas

Embora o Domain Separation forneça suporte a vários locatários, a multilocação ainda está contida em uma única instância. Algumas propriedades, dados e processos globais são compartilhados em todos os domínios. Por exemplo, ter o sistema *Lembrar minhas informações* na página de login do sistema é global e não pode ser especificado por domínio.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Se você precisar da separação completa e total de todas as propriedades do sistema e não precisar de emissão de relatórios globais ou processos globais, instâncias separadas são a melhor opção.

Separação de dados

Os membros de um domínio veem somente os dados contidos em seu domínio ou os domínios secundários que estão abaixo na hierarquia de domínio. Por padrão, todos os usuários e todos os registros são membros do domínio global, a menos que um administrador os atribua a um domínio específico. Depois que você atribui um usuário ou registro a um domínio, a instância compara o domínio do usuário ao domínio do registro para determinar se o usuário pode exibir o registro.

As aplicações da ServiceNow são definidas com os seguintes níveis de suporte incremental. Esses níveis são baseados na perspectiva de casos de uso reais e personas.

Separação de dados: os locatários veem somente os dados que eles têm permissão para ver. Os locatários podem ter acesso a outros dados do locatário, mas não podem consultar os dados do locatário se não tiverem acesso.

Separação de IU: oferece suporte a uma experiência específica de locatário para elementos de IU, como exibições, listas, rótulos e assim por diante.

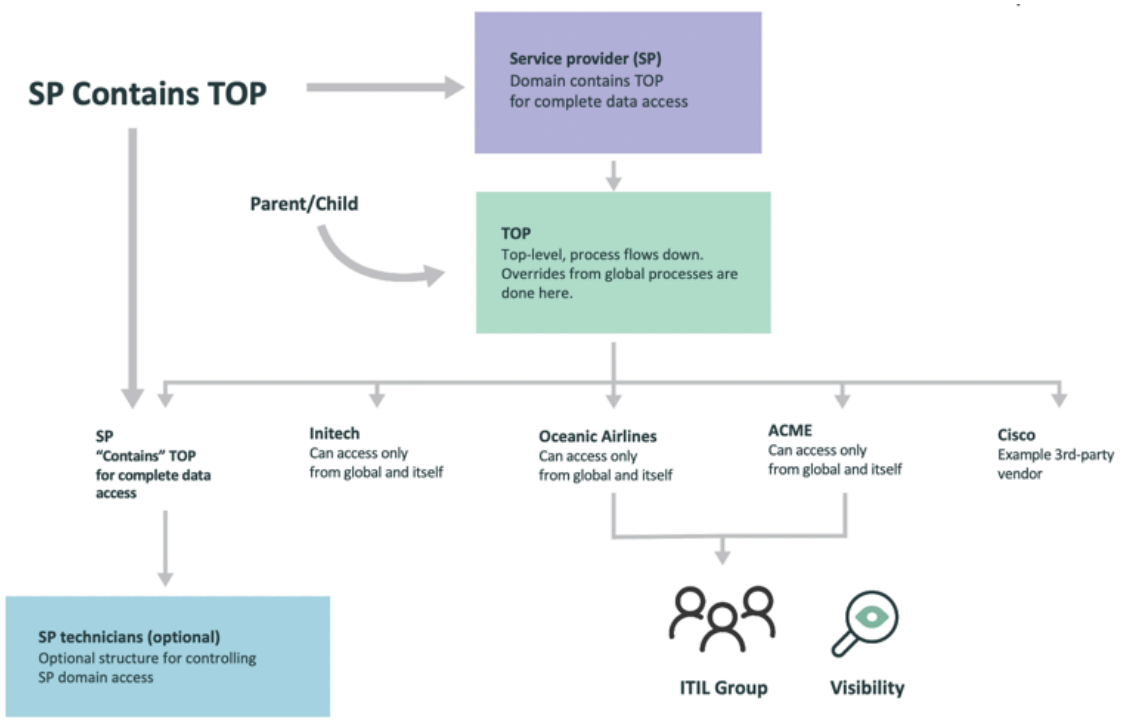
Separação de lógica de negócios: é possível criar políticas de sistema específicas de locatário, como notificações por e-mail, regras de negócio, scripts de cliente, política de IU e ações de IU.

Modelagem hierárquica: vários locatários aninhados para que os locatários primários possam acessar recursos de locatários secundários. A lógica de negócios para locatários primários é executada automaticamente para locatários secundários, e pode ser substituída em qualquer nível.

Inteligência entre locatários (escopo do domínio): lida automaticamente com os dados, metadados, lógica de negócios e contexto de processamento para locatários que têm acesso a dados de locatários adicionais.

Em geral, os dados definidos em um nível superior na hierarquia de domínio não são visíveis em níveis inferiores na hierarquia.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

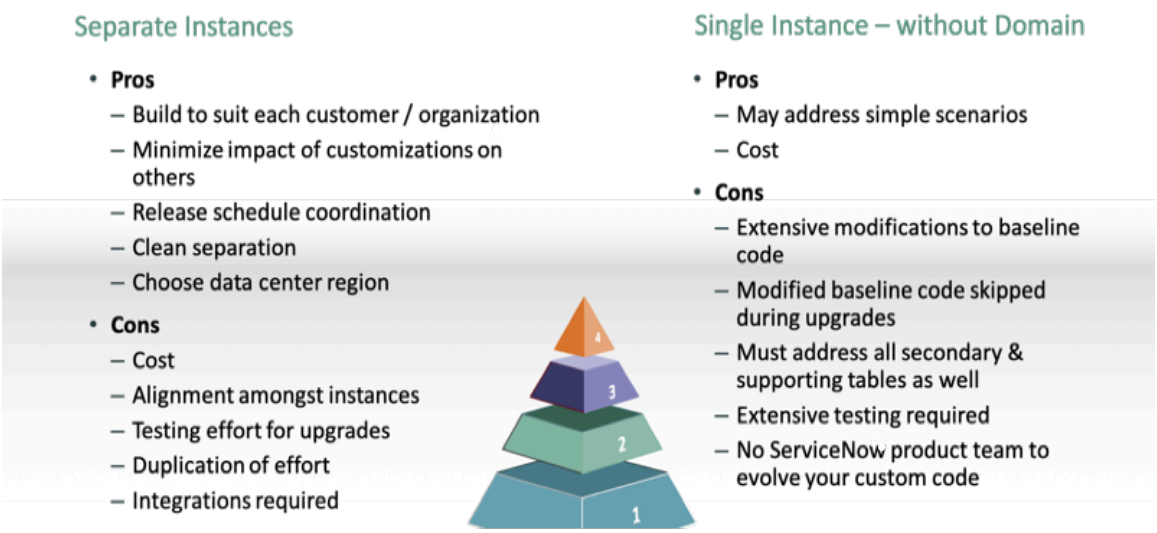


Migração de caminho de domínio

Caminhos do domínio são usados para todos os clientes. A numeração de domínio não é usada. Suporte e atendimento ao cliente pode ajudar no upgrade.

Alternativas ao Domain Separation

Instâncias separadas são uma alternativa comum ao Domain Separation. Isso fornece um alto grau de flexibilidade no atendimento aos requisitos para clientes e partes interessadas com pouco ou nenhum impacto sobre os outros.



⚠ **Aviso:** Antes de ativar o Domain Separation, consulte seu representante para verificar se ela é adequada para o seu ambiente. O Domain Separation adiciona um nível de despesa de administração. Embora possa ser desabilitado, ele não pode ser removido de uma instância.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Informações relacionadas

- Práticas recomendadas do Domain Separation para provedores de serviço
- Plug-in Separação de domínios

Configuração que pode ser delegada a clientes internos ou externos

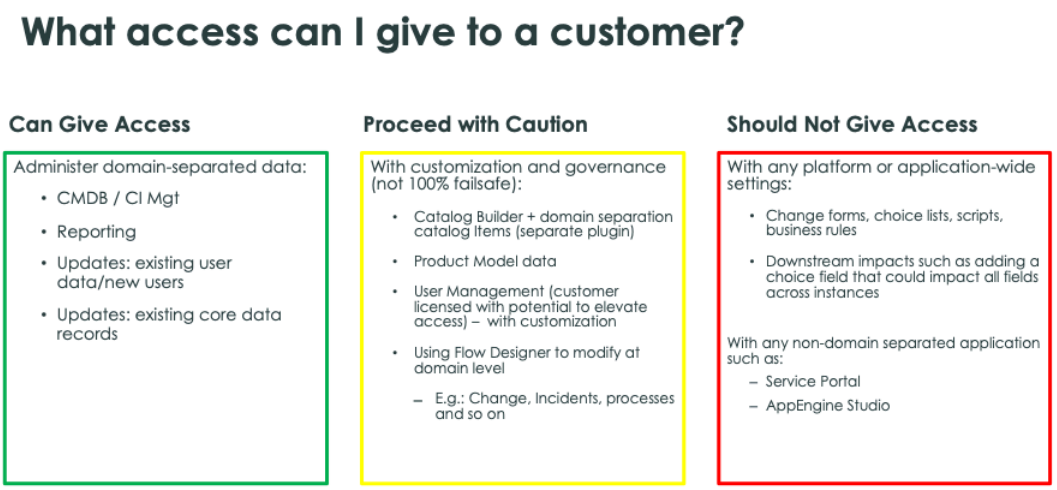
O Domain Separation foi projetado para dar aos provedores de serviço ServiceNow® (SPs) a capacidade de configurar os serviços que oferecem aos clientes. Ele não foi projetado para permitir que seus clientes administrem esses serviços por conta própria, exceto em algumas áreas que este tópico detalha.

Visão geral

É seguro para os clientes do SP, por conta própria, gerenciar os dados contidos em seu domínio que não afetam o licenciamento ou outros clientes. Por exemplo, é seguro para um cliente criar novos relatórios ou gerenciar itens de configuração, mas não é seguro para ele personalizar campos, escolhas, regras de negócios e outros processos em que possam afetar outros clientes na mesma instância.

As ServiceNow funções administrativas do sistema de base e seus controles de acesso na plataforma ServiceNow são projetados para uma única equipe de administradores por instância. Por exemplo, a função domain_admin é concedida a um dos recursos do SP para gerenciar todas as configurações de domínio da instância e para criar novos domínios. Para todas as tarefas de administração específicas do domínio, o SP deve criar novas funções de "administrador do cliente" e controles de acesso conforme necessário para conceder acesso específico aos clientes.

A imagem a seguir é uma visão geral das funções de administrador comuns em várias categorias do que é seguro para um cliente.



Pode conceder acesso

Exemplos:

- Gerenciamento de dados de IC no CMDB
- Criação de relatórios

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Atualizações de dados de usuário existentes ou novos usuários sem funções
- Atualizações nos registros de dados principais existentes, como departamento, grupo, local, centro de custos ou novos grupos sem funções e novos departamentos/centros de custos/local.

Prossiga com cuidado

Exemplos:

- Itens do catálogo: para criar itens do catálogo específicos do cliente que podem ser atualizados pelo cliente, dois recursos podem ser usados juntos: Domain Separation para itens do catálogo (Domain Separation e Catálogo de serviços) habilita o proprietário da instância a criar itens no domínio do cliente. O proprietário da instância pode criar uma função para permitir que os clientes atualizem campos seguros, como preço, descrição e imagens. O Construtor de catálogo (novo na versão Quebec) oferece à equipe de administração do SP a capacidade de criar modelos de item seguros para distribuição aos clientes, a fim de criar novos itens em seu domínio a partir de uma experiência de IU prescritiva.
- Gerenciamento de usuários/grupos: é seguro criar uma função de "administrador do cliente" que pode criar e modificar registros de usuários, mas adicionar e remover funções pode afetar a segurança e o licenciamento. Não há nenhuma maneira no sistema de base de subdividir funções que são seguras para um cliente poder concedê-las. O mesmo se aplica à criação e modificação de grupos. Embora o próprio grupo possa ser modificado, a adição ou subtração de funções deve ser controlada.
- Flow Designer: ServiceNow Flow Designer é a ferramenta de desenvolvimento usada para criar o processo (fluxo de trabalho) das tabelas. A função flow_designer concede aos clientes acesso sem script para criar fluxos. Eles podem ler e clonar todos os fluxos nos domínios acima deles na hierarquia. Eles podem criar e modificar fluxos em seu domínio. Isso não pode acontecer em um silo. Qualquer pessoa que possa afetar o processo deve ser adicionada à equipe de administração global da governança para que os processos não se cancelem ou causem outros conflitos.

Não conceder acesso

Entender como os campos de escolha funcionam é útil para entender por que somente a equipe de administração do SP deve gerenciá-los.

- Estrutura de um campo de opção: os valores do campo de opção são armazenados na tabela sys_choice e agrupados com base em: Tabela, Domínio e Idioma.

  Por exemplo, o campo **Estado** em uma Tarefa está disponível para todas as tabelas que estendem uma Tarefa. Isso significa que cada tabela pode ter seus próprios valores, esses valores podem ser multiplicados por domínio e os valores de domínio podem ser multiplicados por idioma.

  Todos os valores de **Estado** em todas as tabelas, domínios e idiomas são considerados os valores do campo **Estado**.

- Como as mudanças nos campos de opção funcionam: quando um campo de opção é atualizado, uma carga é criada com todos os valores para esse campo (Tabelas, Domínios, Idiomas). Quando você instala esta carga em uma instância, todos os valores existentes para o campo são excluídos e os novos valores são carregados. Isso garante que não haja entradas duplicadas ou valores restantes que não sejam mais válidos.

  Por esse motivo, é impossível dar a um cliente em uma instância separada por domínio a capacidade de atualizar campos de escolha diretamente, pois isso afetaria a instância

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

inteira. Além disso, você não pode atualizar as opções diretamente em uma instância de produção porque quaisquer Conjuntos de atualizações importados que afetem esse campo substituirão as opções existentes. Em alguns casos, os campos de escolha podem orientar os próprios processos, que seriam interrompidos se um cliente alterasse esses campos.

Para saber mais, consulte:

- Explorando a administração de usuários
- Criar uma regra de ACL
- Caminho de aprendizado do provedor de serviço no NowLearning
- Domain Separation para provedores de serviço
- Conceitos sobre provedor de serviço
- Compatibilidade de aplicações com o Domain Separation
- Notas de versão do Domain Separation

Atribuição de domínio

Por padrão, o Domain Separation adiciona um campo de domínio às tabelas e suas extensões.

Você também pode estender o Domain Separation para qualquer nova tabela criada, adicionando um campo **sys_domain** à definição do dicionário da tabela. Por padrão, o sistema separa por domínio as tabelas de plataforma e de aplicação de linha de base quando apropriado.

Aviso: ServiceNow não recomenda separar por domínio tabelas de plataforma (qualquer tabela com o prefixo sys_, como as tabelas de Entrada de Dicionário [sys_dictionary] e de Substituição de Entrada de Dicionário [sys_dictionary_override]) porque isso pode produzir resultados inesperados.

Cada registro é atribuído a um único domínio. Esse domínio é armazenado no campo **sys_domain**. Várias tabelas, por padrão, têm a coluna **sys_domain** e já são separadas por domínio.

O valor do campo **sys_domain** contém o domínio atribuído ao registro por qualquer um dos seguintes:

- Empresa à qual o usuário pertence
- Regra de negócio ao criar o registro
- Módulo usado ao criar o registro
- Modelo de formulário usado ao criar o registro
- Domínio do registro primário
- Domínio atribuído ao registro do Usuário
- Domínio do usuário que o cria

O sistema evita que as seguintes tabelas sejam separadas por domínio:

- Controle de acesso `[sys_security_acl]`
- Inclusão de script `[sys_script_include]`
- Propriedades do sistema `[sys_properties]`

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Entidades da lista de exclusões/inclusões de segurança `[sys_security_restricted_list]`
- Entrada de dicionário `[sys_dictionary]`
- Substituição de entrada de dicionário `[sys_dictionary]`

Atribuição de usuários a empresas

Os administradores podem atribuir rapidamente usuários a um domínio atribuindo-os a uma empresa. Depois que os usuários são atribuídos a um domínio, os registros herdam automaticamente o domínio do usuário.

Por exemplo, atribuir Bow Ruggeri à empresa ACME o atribui automaticamente ao domínio ACME. Atribuir Don Goodliffe à empresa Initech o atribui automaticamente ao domínio Initech. Todos os registros criados por eles são adicionados automaticamente ao domínio apropriado.

Uso de regras de negócios para atribuir domínios

Os administradores podem usar uma regra de negócios para definir automaticamente um valor de domínio ao criar um registro. A regra de negócios deve definir um valor no campo **sys_domain**. Os administradores devem garantir que há uma coluna **sys_domain** disponível para a tabela de registro. Para saber mais, consulte Práticas recomendadas do Domain Separation para provedores de serviço.

Uso de módulos para atribuir domínios

Os administradores podem usar o parâmetro de URL **sysparm_domain** para atribuir automaticamente novos registros a um domínio específico de um módulo. Os administradores devem criar um módulo com um valor de **Argumento** : `sysparm_domain = sys_ID de domínio`.

Uso de modelos de formulário para atribuir domínios

Os administradores podem usar um modelo de formulário para atribuir automaticamente novos registros a um domínio específico. Os administradores devem adicionar o campo **sys_domain** ao formulário e selecionar um valor de domínio. Por exemplo, definir o campo **sys_domain** como domínio **TOP/ACME** atribui automaticamente todos os registros desse modelo ao domínio TOP/ACME.

Herança de domínio em tabelas

Por padrão, os registros relacionados herdam o domínio do registro primário. Por exemplo:

- Um registro de tarefa de mudança herda o domínio do registro de solicitação de mudança primário.
- Um registro de problema herda o domínio do registro de incidente primário.

Atribuição automática de domínio com base nos domínios do usuário

Se nenhuma outra condição de domínio se aplicar, um registro herdará automaticamente o domínio do usuário que a cria.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Domínios de visibilidade e domínios "contém"

Os domínios de visibilidade controlam o que um usuário ou grupo de usuários específico pode ver. Os domínios "contém" controlam o que um domínio inteiro de usuários pode ver.

Domínios de visibilidade

O elemento "Domínios de visibilidade" determina se os usuários de um domínio podem acessar registros de outro domínio. Associe esse elemento aos registros de Usuário [sys_user] e Grupo [sys_user_group] em listas relacionadas nesses registros. Os grupos concedem a seus membros os domínios de visibilidade do grupo. Quando um usuário sai de um grupo, ele perde os domínios de visibilidade do grupo. Conceder aos usuários um domínio de visibilidade concede todos os direitos aos registros nesse domínio com base nas regras de ACL (lista de controle de acesso).

Um domínio de visibilidade:

- É um relacionamento de usuário para domínio e foi concedido explicitamente.
- Não é um domínio secundário.
- Não é controlado pela seleção no seletor de domínio. Os usuários com acesso a um domínio de visibilidade sempre veem os dados desse domínio e de seus domínios secundários.

Nota: Usar domínios de visibilidade excessivamente não é recomendado. Embora a visibilidade seja um método para permitir que os usuários acessem registros, é melhor usar os domínios "contém" para um controle mais robusto.

Domínios "contém"

Normalmente, os relacionamentos primário-secundário definem a hierarquia de domínio. Um domínio "contém" permite que você relacione domínios conforme a necessidade, independentemente de relacionamentos primário-secundário. No entanto, domínios "contém" concedem visibilidade somente aos dados do domínio. Os processos não são afetados por relacionamentos de conteúdo.

Um domínio "contém":

- É um relacionamento muitos para muitos, domínio para domínio.
- Pode ter domínios secundários. Quando um domínio é selecionado, você pode ver os dados desse domínio e seus secundários.
- É controlado pela seleção no seletor de domínio.

Nota: Quando você abre o registro de domínio, o escopo é definido para o domínio desse registro, portanto, você pode ver somente os domínios secundários. Escolha **Alternar escopo do domínio** no menu para preencher a lista relacionada.

Exemplo de domínio "contém"

Quando o domínio inicial de um usuário é A e o domínio A contém os domínios B e C, todos se tornam domínios de mesmo nível. Isso significa que o usuário vê os dados dos domínios A, B e C enquanto está no domínio inicial A. Se os usuários mudarem os domínios com o seletor de domínio para o Domínio B, eles verão somente os dados no Domínio B. Quando os usuários interagirem com um registro do Domínio B ou Domínio C diretamente, eles verão somente os dados desse domínio.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exemplo de domínio de visibilidade

Usando a visibilidade de domínio, se Don Goodliffe estiver no domínio do banco de dados e Bow Ruggeri estiver no domínio Rede e nenhum incidente estiver no domínio global, Don não poderá acessar os incidentes de Bow devido à separação de dados.

Como herdar domínios de visibilidade com base em associação de grupo

Se você definir a tabela de domínio como a tabela Grupo [sys_user_group], os usuários poderão herdar domínios de visibilidade com base em sua associação de grupo.

Informações relacionadas

Consultas "contém" e acesso ao domínio

Práticas recomendadas do Domain Separation para provedores de serviço

Escopo do domínio

O escopo do domínio define o que os usuários podem e não podem acessar.

Cada usuário tem dois escopos de domínio ao estabelecer uma sessão em uma instância separada por domínio.

- *Oescopo da sessão* é definido após o estabelecimento da sessão para o domínio listado no registro de usuário do usuário. Os usuários podem alterar manualmente o escopo do domínio da sessão no seletor de domínio.
- *O escopo do registro* usa o domínio do registro e está ativo ao exibir o formulário de qualquer registro.

Por padrão, o escopo do registro tem precedência sobre o escopo da sessão para que os usuários em domínios de nível superior sigam as restrições de dados e de processo de cada registro. No entanto, esses usuários podem optar por expandir ou recolher o escopo do domínio para mostrar ou ocultar dados de outros domínios. Por exemplo, um usuário no domínio do Provedor de Serviço (SP) também tem visibilidade em domínios secundários, como o domínio ACME. Ao observar um registro de incidente do domínio ACME, o usuário pode optar por expandir o escopo do domínio para mostrar valores do domínio SP ou recolher o escopo do domínio para mostrar somente os valores de registro que correspondem ao domínio ACME do registro.

Nota: Os usuários sempre têm acesso aos dados de domínios que foram concedidos explicitamente a eles pela visibilidade do domínio.

Usuários com a função de usuário domain_expand_scope podem selecionar o escopo do domínio na ação de IU **Alternar escopo do domínio** no formulário. Quando o escopo do registro estiver em vigor, clique na ação de IU para expandir para o escopo da sessão e exibir todos os dados disponíveis com base no domínio do usuário e nos domínios secundários. Quando o escopo da sessão estiver em vigor, clique na ação de IU para recolher para registrar o escopo e exibir somente os dados que correspondem ao domínio do registro atual.

Nota: Um registro não exibe a ação de IU para alternar o escopo do domínio se o registro estiver no domínio global ou se o domínio do usuário corresponder ao domínio do registro.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Seleção de valor de registro de outros domínios

Os usuários que podem ver vários domínios têm a opção de selecionar valores de registro de um domínio diferente do domínio do registro.

Por exemplo, os agentes de central de serviços que trabalham para um provedor de serviços podem atribuir determinados incidentes a si próprios para resolver problemas em nome de seus clientes. Quando eles fazem isso, o campo de incidente **Atribuído a** pode conter um usuário do domínio SP, mesmo que o próprio registro de incidente esteja associado a um domínio secundário, como ACME.

Selecionar um valor de registro de outro domínio não muda o domínio do registro. O registro retém seu domínio original. Quando um usuário exibe um registro com valores de vários domínios, a visibilidade do domínio do usuário determina o que ele vê.

Seleção de valor de registro

Quando estas condições forem atendidas	O usuário tem acesso a esses elementos de IU
O usuário tem acesso ao domínio do registro atual referenciado em um campo.	O usuário pode: • Consulte o valor de exibição do campo de referência. Por exemplo, vê o nome do usuário no campo **Atribuído a**. • Veja o registro relacionado do ícone de referência. Por exemplo, vê o registro de usuário para o usuário no campo **Atribuído a**. • Selecione valores de qualquer domínio visível. Por exemplo, pode selecionar usuários dos domínios SP e ACME.
O usuário não tem acesso ao domínio do registro atual referenciado em um campo.	O usuário pode: • Não consultar os valores de exibição do campo de referência. (Este é o caso se o Domain Separation foi ativado em Madrid ou versões posteriores e o usuário não tem acesso ao domínio desse registro.) • Selecione somente valores do domínio do registro. Por exemplo, pode selecionar apenas usuários do domínio ACME.

Domínios e empresas associadas

Com o Domain Separation, você pode cascatear as mudanças feitas em um registro da empresa para o domínio e outros registros associados à empresa.

Por padrão, o sistema atribui usuários automaticamente ao mesmo domínio da empresa. Por exemplo, todos os usuários da empresa ACME se tornam automaticamente membros do domínio TOP/ACME.

Nota: Usuários com a função de administrador podem mudar seus próprios registros de usuário e, portanto, mudar os domínios. Os Provedores de Serviço podem desabilitar a administração delegada ou configurar um processo de aprovação para verificar se o usuário precisa da função de administrador.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Quando você muda o domínio de uma empresa, a instância muda automaticamente o domínio dos seguintes registros associados para corresponder ao novo domínio da empresa.

- Locais
- Departamentos
- Grupos
- Usuários

Nota: A instância não muda automaticamente o domínio de qualquer registro no qual você tenha marcado a caixa de seleção **Domínio gerenciado**.

Desativação de domínios e empresas associadas

Quando você desativa um domínio, a instância também conclui automaticamente as seguintes ações.

- Desativa todas as empresas no domínio.
- Impede que todos os usuários atribuídos à empresa inativa façam login.

Nota: Quando um usuário de uma empresa inativa tenta fazer login, o usuário vê uma mensagem de erro semelhante a `Empresa inativa - seu acesso a esta instância não está autorizado.`

Por exemplo, se você desativar o domínio ACME dos dados de amostra, a instância também desativará a empresa ACME e os três usuários de amostra serão bloqueados.

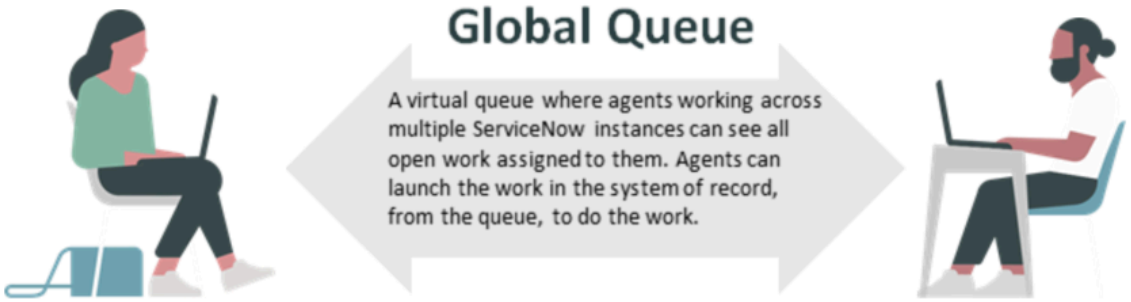
Conceitos para provedores de serviço

Esses conceitos funcionam com os ServiceNow recursos da plataforma existentes para ajudá-lo a resolver casos de uso comuns.

Fila global v.2

O conceito de fila global fornece uma exibição virtual única de tarefas que residem em várias instâncias. O conceito cria uma aplicação personalizada para fornecer a um executante uma exibição do trabalho que reside em várias instâncias sem precisar replicar tarefas ou dados.

Visão geral



Provedores de serviço com agentes trabalhando em tarefas de vários sistemas tendem a integrar os dados de volta a uma instância central, ou uma "cadeira giratória" entre as instâncias. Embora esse método possa ser apropriado em alguns casos, pode ser caro e demorado para criar e manter. Esse método também abre o provedor para possíveis

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

considerações de requisitos de auditoria e de dados, como Regulamento de proteção geral de dados (GDPR) em todas as instâncias em que os dados residem agora.

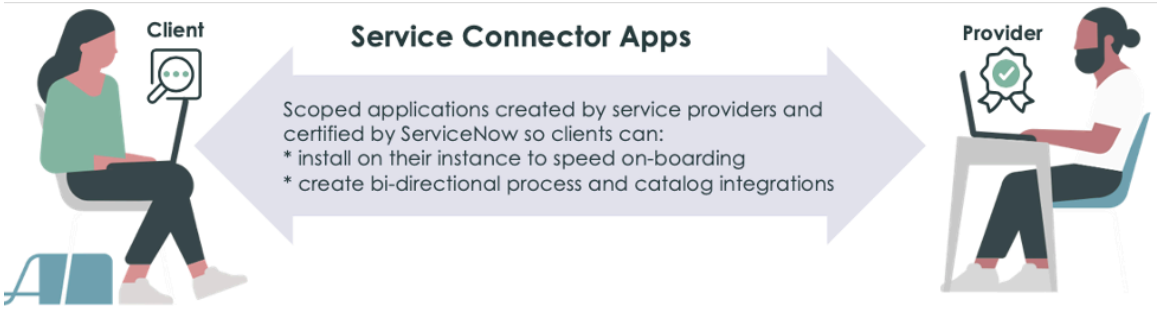
A fila global v.2 é uma alternativa: com esse método, os agentes podem ver os dados atribuídos a eles a partir de uma única instância sem que os dados soberanos persistam na instância em que estão conectados. Por exemplo, nos casos em que os clientes têm requisitos de residência de dados, mas permitem o acesso por agentes de outros países, o provedor pode usar um Help Desk "follow-the-sun" usando a fila global v.2.

Saiba mais sobre a Prova de Conceito da Fila Global v.2 no site do ServiceNow Knowledge.

Nota: Na versão Quebec para frente, a Prova de conceito da fila global foi atualizada para a Fila global v. 2.

Conector do provedor de serviço

A aplicação conectora do provedor de serviços é um design de referência para a criação de ServiceNow uma Aplicação da Store para os clientes usarem na integração com os sistemas. As aplicações do provedor de serviço ajudam a acelerar a integração e a criar integrações padronizadas.

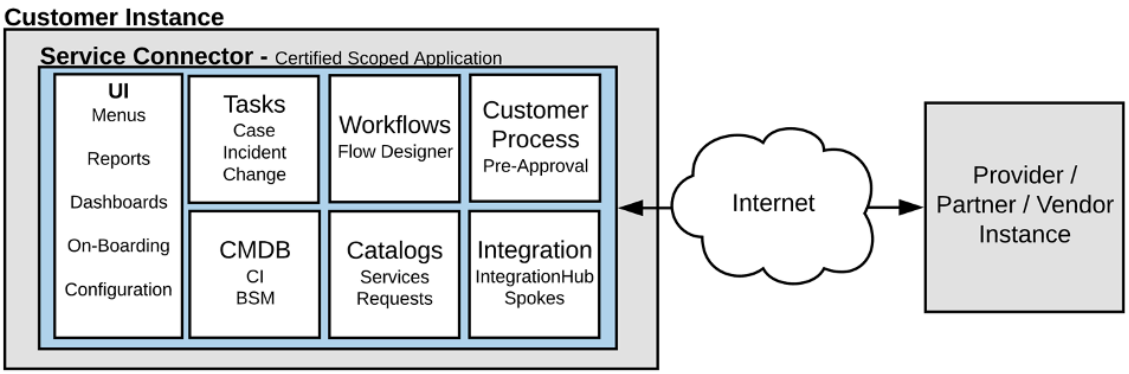


Benefícios dos conectores de serviço

Quando os provedores de serviços (fornecedores, parceiros) publicam conectores, a integração do cliente é mais rápida, o que significa faturamento mais rápido. As instâncias integradas aumentam a produtividade, a visibilidade no ServiceNow ecossistema e os benefícios do programa de parceiros. Os benefícios específicos são:

- Elimina integrações personalizadas, incluindo o custo de serviços necessários para entregá-las e mantê-las.
- Os serviços são definidos pelo provedor em suas ServiceNow instâncias e eliminam a necessidade de complexidade e custo de integrações personalizadas.
- Fluxos de trabalho e solicitações de catálogo podem ser sincronizados com os processos e aprovações do cliente que precedem os processos do provedor, para que os clientes possam seguir seus próprios processos.
- Quaisquer dados criados ou modificados (por exemplo, ICs) para o cliente na instância do provedor podem ser sincronizados de volta para a instância do cliente para sua visibilidade e uso em processos.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Principais recursos

Recurso	Descrição
Interface do usuário	Um conector de serviço deve incluir no mínimo os seguintes componentes de IU: • Relatórios/Painéis - Relatórios e painéis predefinidos por persona ajudam com visibilidade. • Menu e módulos - O cliente deve ser capaz de encontrar a aplicação por meio do menu descritivo do **Provedor de serviços XYZ**. • Funções - Cada conector requer funções de usuário e administrador para garantir que o acesso possa ser controlado pelo cliente. Por exemplo, "x_snc_xyz_user" ou "x_snc_xyz_admin". • Integração - A integração rápida é essencial para uma boa experiência do cliente e deve ser incluída por meio de playbook, Configuração assistida ou item do catálogo de forma que nenhum serviço profissional seja necessário para o cliente entrar em operação. (Há serviços profissionais disponíveis, mas a integração pode ser realizada sem eles). • Configuração - Os pontos de dados devem ser integrados aos processos para considerar a maior parte da configuração de processo normal que um cliente precisa alcançar. Isso elimina serviços profissionais tanto quanto possível. • Documentação - A documentação completa aumenta a satisfação do cliente e a facilidade de uso. • Integração de suporte ou informações de contato - O cliente precisa de uma

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Recurso	Descrição
	maneira fácil de permanecer em contato com o provedor de serviço em caso de problemas, dúvidas ou solicitações.
Tarefas	O uso da aplicação Central de controle de serviços (legado) para tarefas, como incidentes, casos, mudanças, problemas e assim por diante, deve ser predefinido no conector. Essas integrações são criadas usando Flow Designer e Integration Hub para garantir o mais alto nível de resiliência e desempenho.
CMDB	A sincronização de dados principais, como os ICs necessários para os processos ITIL apropriados, deve ser mantida em sincronia entre as instâncias do provedor e do cliente.
Fluxos de trabalho	Todos os fluxos de trabalho devem ser projetados em Flow Designer para garantir resiliência e desempenho.
Catálogos	O catálogo do provedor do qual o cliente solicita deve ser incluído na aplicação como um catálogo de produção de registro. A solicitação gerada pelo item na instância do cliente deve ser realizada no eBonded com as instâncias do provedor. Os fluxos de trabalho do provedor mantêm a solicitação atualizada e sincronizam novamente com a instância do cliente.
Processos do cliente	Quaisquer mecanismos para sincronizar solicitações com a instância do provedor devem permitir que os processos do cliente interajam com as solicitações antes que elas sejam enviadas para a instância do provedor. Durante o processamento do provedor, as aprovações podem ser enviadas para a instância do cliente conforme necessário.
Integração	As integrações devem ser criadas usando Flow Designer e Integration Hub para garantir o mais alto nível de resiliência e desempenho.

Possíveis componentes que você pode incluir em um Conector de serviço

Componente	Descrição
Replicação de dados da instância (IDR)	Quando a replicação é o objetivo: • Pode ser usado para integração de processos, mas pode ser muito rígido, dependendo da lógica de integração de

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Componente	Descrição
	complexidade com base na transição de estado • Para saber mais, consulte Replicação de dados da instância
IntegrationHub	Quando a integração de processos é o objetivo: • Mais fácil de injetar no meio de um processo, como parte de uma etapa complexa ou condicional no meio de um fluxo • Para saber mais, consulte IntegrationHub
Fila de trabalho global (virtual)	Quando a federação de tarefas é o objetivo e o armazenamento de dados externamente não é aceitável: • Usado quando os agentes estão trabalhando em várias instâncias ServiceNow e precisam ver todo o trabalho em aberto atribuído a eles • As linhas retornadas devem ser limitadas a menos de 1000 • Para saber mais, consulte Fila de trabalho global
Tabelas remotas	Quando o uso de dados externos sem armazenamento é o objetivo: • Usado para conectar uma instância a fontes de terceiros, ou a outra instância, para recuperar dados externos e, opcionalmente, armazená-los em cache na memória. Os dados são tratados como uma tabela na instância para fins somente leitura, como agrupar, classificar, agregar e filtrar. • Para saber mais, consulte Recuperar dados externos usando tabelas e scripts remotos
Flow Designer	Quando o design de processo é o objetivo • Usado para automatizar processos em um único ambiente de design. Os proprietários de processo podem usar linguagem natural para automatizar aprovações, tarefas, notificações e operações de registro sem codificação. • Para saber mais, consulte Flow Designer.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Saiba mais sobre a Prova de Conceito do Conector de Serviço no site do ServiceNow Knowledge.

Instalação com Domain Separation

Vários componentes da plataforma são adicionados ou modificados com o Domain Separation.

Funções

Função	Descrição
domain_admin	Pode criar, editar e excluir domínios.

Adições a campos [sys_domain]

O campo sys_domain é adicionado às seguintes tabelas:

Tabelas com o campo sys_domain

Tabelas
sys_attachment
sys_user_has_role
sys_group_has_role
sys_email
sys_user_group
core_company
cmn_location
cmn_department
sys_gauge
sys_report
kb_feedback
sysapproval_approver
sys_user_grmember

Campo para a tabela de tarefas

As extensões MSP adicionam um campo task_for à tabela de tarefas. Esse campo de referência refere-se à tabela do Usuário.

Opções para o Tipo de grupo

As Extensões MSP adicionam várias novas opções-padrão ao campo de tipo da tabela Grupo. Adicione ou atualize esses tipos conforme necessário para oferecer suporte a seus domínios.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabelas
Segurança
Suporte
Visibilidade

Regras de negócio

Nome	Tabela	Descrição
Domínio - Ativar/ Desativar	core_company	Ativa o domínio relacionado se pelo menos uma de suas empresas estiver ativa. Desativa o domínio relacionado se todas as empresas relacionadas estiverem inativas.
Domínio - Empresa em Cascata	core_company	Mantém o domínio da empresa em sincronia com seus usuários, grupos, departamentos e locais.
Domínio - Domínio em cascata - E-mail	sys_email	Mantém o domínio de um e-mail sincronizado com seus anexos.
Domínio - Domínio em cascata - Grupo	sys_user_group	Mantém o domínio de um grupo em sincronia com suas funções herdadas (registros sys_group_has_role).
Domínio - Domínio em cascata - Knowledge	kb_knowledge	mantém o domínio de um artigo de conhecimento em sincronia com o feedback relacionado.
Domínio - domínio em cascata - tarefa	tarefa	Mantém o domínio em sincronia com tarefas relacionadas a wf_context, wf_executing, wf_history, anexos, e-mails, task_sla e seu fluxo de trabalho, sysapproval_approver e seu fluxo de trabalho e sysapproval_group e seu fluxo de trabalho.
Domínio - domínio em cascata - usuário	sys_user	Mantém o domínio de um usuário em sincronia com seus registros de associação de grupo (sys_user_grmember) e função (sys_user_has_role).
Domínio - domínio em cascata - versão	wf_workflow_version	Mantém os domínios em sincronia com as versões de fluxo de trabalho relacionadas para wf_activity e wf_transition.
Domínio - Desativar empresas	domínio	Desativa empresas relacionadas se um domínio for desativado.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome	Tabela	Descrição
Domínio - Padrão - Tarefa	tarefa	Define o domínio da tarefa com base na tarefa do domínio do usuário. Se esse domínio for global, define o domínio como Padrão.
Domínio - Padrão - Usuário	sys_user	Define o domínio de um usuário como Padrão se o domínio for global.
Domínio - Proibir registro de domínio global	domínio	Impede a criação de um domínio com o nome global.
Domínio - Cópia de substituição	sys_app_application	Quando uma aplicação é substituída por um domínio, cria uma cópia de seus módulos para a nova aplicação.
Domínio - Cópia de substituição	sys_data_policy2	Quando uma política de dados é substituída por um domínio, cria uma cópia de suas regras de política de dados para a nova política de dados.
Domínio - Cópia de substituição	sys_gauge	Quando um medidor é substituído por um domínio, cria uma cópia de suas contagens de medidor para o novo medidor.
Domínio - Cópia de substituição	sys_ui_action	Quando uma ação de IU é substituída por um domínio, cria uma cópia de suas visualizações de ação de IU para a nova ação de IU.
Domínio - Cópia de substituição	sys_ui_list_control_embedded	Quando um controle de lista integrada é substituído por um domínio, cria uma cópia de seus scripts de cliente e servidor para o novo controle de lista integrada.
Domínio - Cópia de substituição	sys_ui_policy	Quando uma política de IU é substituída por um domínio, cria uma cópia de suas ações de política IU para a nova política de IU.
Domínio - Definir domínio - Aprovações	sysapproval_approver	Define o domínio com base no registro que está sendo aprovado.
Domínio - Definir domínio - Anexo	sys_attachment	Define o domínio com base no domínio do registro primário.
Domínio - Definir domínio - CMDB_CI	cmdb_ci	Define o domínio de um IC ao de sua empresa.
Domínio - Definir domínio - Departamento	cmn_department	Define o departamento de um IC ao de sua empresa.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome	Tabela	Descrição
Domínio - Definir domínio - Domínio	domínio	Define o domínio de um domínio para si mesmo.
Domínio - Definir domínio - E-mail	sys_email	Define o domínio com base no domínio do registro primário. O registro primário de um e-mail é o registro especificado no campo de instância.
Domínio - Definir domínio - Feedback	kb_feedback	Define o domínio de um feedback de conhecimento ao de seu artigo de conhecimento.
Domínio - Definir domínio - Grupo	sys_user_group	Define o domínio de um grupo ao de sua empresa.
Domínio - Definir domínio - Aprovações de grupo	sysapproval_group	Define o domínio com base no registro que está sendo aprovado.
Domínio - Definir domínio - Função de grupo	sys_group_has_role	Define o domínio de uma função de grupo ao de seu grupo.
Domínio - Definir domínio - Local	cmn_location	Define o domínio de um local ao de sua empresa.
Domínio - Definir domínio - ANS de tarefa	task_sla	Define o domínio do ANS de uma tarefa ao de sua tarefa.
Domínio - Definir domínio - Usuário	sys_user	Define o domínio de um usuário ao de sua empresa.
Domínio - Definir domínio - Função do usuário	sys_user_has_role	Define o domínio de uma função do usuário ao de seu usuário.
Domínio - Definir domínio - Histórico de atividades do WF	wf_history	Define o domínio do histórico de atividades de fluxo de trabalho com base no domínio do contexto de fluxo de trabalho primário.
Domínio - Definir domínio - Contexto do WF	wf_context	Define o domínio de contexto de fluxo de trabalho com base no domínio do registro referenciado, se houver.
Domínio - Definir domínio - Atividade em exec do WF	wf_executing	Define o domínio de atividade em execução do fluxo de trabalho com base no domínio do contexto de fluxo de trabalho primário.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome	Tabela	Descrição
Domínio - Definir tarefa para - Mudança	change-request	Ao converter um tíquete em uma solicitação de mudança, define o campo Solicitado por com o valor Tarefa do tíquete.
Domínio - Definir tarefa para - Incidente	incidente	Ao converter um tíquete em um incidente, define o campo Solicitante com o valor Tarefa do tíquete.
Domínio - Validar Padrão	domínio	Garante que apenas um domínio tenha a caixa de seleção Padrão marcada.
Domínio - Validar Primário	domínio	Garante que apenas um domínio tenha a caixa de seleção Primário marcada.
Regras de negócio Instaladas com o plug-in Domain Support		
Mudar domínio definido	sys_dictionary	Define o domínio definido como o domínio atual.
Propriedades de suporte do domínio	sys_properties	Define as propriedades do sistema para corresponder ao método de consulta de domínio (caminhos de domínio ou numeração de domínio).

Scripts de cliente

Client script	Descrição
Domínio - Definir empresa e local (sys_script)	Monitora o campo do solicitante do incidente quanto a mudanças. Se os campos de empresa e local ainda não tiverem um valor, o script adicionará essas informações do registro do solicitante. Se os campos de empresa e local já tiverem um valor, o script manterá os valores existentes.
Script desativado	
(BP) Definir local como usuário	Monitora o campo de local do incidente e define o campo de local como o local do solicitante.

Informações relacionadas

Práticas recomendadas do Domain Separation para provedores de serviço

Compatibilidade de aplicações com o Domain Separation

Muitas aplicaçõesServiceNow oferecem suporte ao Domain Separation no sistema de base, mas nem todas. Algumas aplicações compatíveis incluem limitações nos dados e configurações administrativas que podem ser separadas por domínio. Essas definições delineiam os níveis de suporte do Domain Separation da perspectiva dos casos de uso reais e das pessoas que os usam.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Níveis de suporte do Domain Separation

ServiceNow aplicações que oferecem suporte ao Domain Separation podem oferecer suporte à separação de dados e roteamento de dados, ter separação de lógica de negócios avançada ou oferecer suporte à administração de nível de locatário (cliente) da aplicação. ServiceNow das aplicações são definidos com os seguintes níveis de suporte incremental.

Basic	Standard	Enhanced
• Data is domain-separated • Logic exists to ensure proper data routing, caching, rollups, and aggregations • Global configuration operational for multiple tenants	• Application properties are domain-aware as needed • Business logic can be domain-separated by the instance owner per tenant	• Data-driven process enables failsafe configuration by tenants through the UI to drive business logic

Sem suporte

- O campo de domínio pode existir em tabelas de dados, mas não há lógica para gerenciar dados.
- Este nível não é considerado separado por domínio.

Básico

- Lógica de negócios: confirme se os dados vão para o domínio adequado para os casos de uso do provedor de serviço (SP) de aplicação.
- Na aplicação, a interface do usuário, as chaves de cache, a emissão de relatórios, acúmulos e agregações usam o domínio em tempo de execução de produção.
- O proprietário da instância deve conseguir configurar a aplicação para funcionar em vários locatários.

Caso de uso de exemplo: quando um SP usa o bate-papo para responder a uma mensagem de locatário-cliente, o cliente deve ser capaz de ver a resposta do SP.

Padrão

- Inclui nível de suporte **Básico**.
- Lógica de negócios: os processos podem ser criados ou modificados por cliente pelo provedor de serviços (SP). Os casos de uso refletem o uso adequado da aplicação por vários clientes de SP em uma única instância.
- O proprietário da instância deve ser capaz de configurar a lógica de negócios do produto mínimo viável (MVP) e os parâmetros de dados por locatário conforme esperado para a aplicação específica.

Exemplo de caso de uso: um administrador deve ser capaz de fazer os comentários obrigatórios quando um registro é encerrado para um locatário, mas não para outro.

Aprimorado

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Inclui os níveis **Básico** e **Padrão**.
- O processo orientado por dados permite que os clientes do provedor de serviços modifiquem a lógica de negócios baseada em casos de uso definidos. Essas configurações são baseadas em IU e à prova de falhas para que as configurações de um cliente não possam afetar outro.
- Os locatários da instância devem ser capazes de configurar por conta própria a lógica de negócios do produto minimamente viável (MVP) e os parâmetros de dados. Essa lógica e os parâmetros seriam esperados para a função normal da aplicação.

Exemplo de caso de uso: os clientes locatários de um ambiente compartilhado devem ser capazes de mudar o impacto, a urgência ou a matriz de prioridade para definir a prioridade em seu domínio.

Nota: Domínio efetivo (*)

Às vezes, um recurso de plataforma ou aplicação pode oferecer suporte a casos de uso de SP, mesmo sem a estrutura de domínio. Em caso afirmativo, os casos de uso devem detalhar seu suporte ao Domain Separation. Um asterisco (*) após o nível de suporte indica este tipo de configuração.

Recurso compatível	Básico	Padrão	Aprimorado
A coluna domínio está presente nas tabelas de aplicação do sistema de base	●	●	●
A configuração específica do domínio é gerenciada pelo proprietário da instância	●	●	●
Os domínios de locatário podem gerenciar os próprios dados de aplicação.		●	●
As propriedades da aplicação reconhecem o domínio quando necessário.		●	●
Lógica de negócios e processos podem ser separados por domínio pelo proprietário da instância.		●	●
A lógica de negócios e os processos podem ser administrados pelo domínio do locatário.			●

Níveis de suporte por aplicação

Pacote de produtos	Aplicação	Nível de suporte
Hiperautomação e low code	App Engine Studio	Sem suporte
	Automation Center	Básico
	Hub Automação de processos robóticos (APR)	Básico
	Construtor de tabelas	Básico
	Central de gestão do App Engine	Sem suporte
	Explorar tabelas de decisão	Padrão

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Pacote de produtos	Aplicação	Nível de suporte
	Integração do Enterprise Resource Planning	Sem suporte
	Mineração personalizada de ERP	Sem suporte
	Construtor de IU Next Experience	Básico
Customer Service Management	Comunidades	Sem suporte
	Customer Service Management	Básico
	Gestão de versões	Básico*
	Gestão de pedidos para Customer Service Management	Básico
	Suporte pós-vendas	Básico
	Separação de domínios em Otimização da força de trabalho para atendimento ao cliente	Básico
DevOps	Domain Separation e Velocidade de mudança para DevOps	Sem suporte
	Domain Separation e Configuração de DevOps	
Gestão de serviços a funcionários	Prestação de serviços de RH	Básico*
	Saúde e segurança	Básico
	Prestação de serviços jurídicos	Básico
	Gestão de serviços de compras (PSM)	Sem suporte
	Pacote de Local de trabalho seguro	Consulte o site de aplicações para obter os níveis de suporte de aplicações individuais
	Conector de pesquisa do SharePoint Online	Básico
	Solicitação universal	Básico
	Tarefa universal	Básico
	Otimização da força de trabalho para RH	Básico
Gestão ambiental, social e de governança (ESG)	Gestão ambiental, social e de governança (ESG)	Básico
Gestão de serviços de campo	Gestão de serviços de campo	Básico

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Pacote de produtos	Aplicação	Nível de suporte
Governança, risco e conformidade	Business Continuity Management	Básico
	Governança, risco e conformidade (GRC)	Básico
	Resiliência operacional	Básico
Produtos do setor		
• Serviços financeiros	Operações com cartão para serviços financeiros	Básico
	Operações de depósito de Serviços financeiros	Básico
	Operações de pagamento de Serviços financeiros	Básico
	Intelligent Servicing for Fraud	
	Manutenção de seguro de propriedade e sinistro	
	Manutenção de seguro de vida	
	Sinistros de seguro	
	Serviços financeiros Know Your Customer	
	Operações de crédito de Serviços financeiros	
	Processador de documentos de serviços financeiros	Básico
• Saúde e ciências da vida	Ajuda para prontuários médicos eletrônicos	Básico
	Gestão de serviços de assistência médica e ciências biológicas Core	Básico
	Pre-Visit Management	Básico
	Patient Support Services	Básico
	Vaccine Administration Management	Básico
• Produção	Manufacturing Process Manager Gerente de processos industriais	Padrão
	Gerenciador de tecnologia operacional	Padrão
	Resposta a vulnerabilidades para tecnologia operacional	Padrão
	Gerenciador de tecnologia operacional	Padrão

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Pacote de produtos	Aplicação	Nível de suporte
IT Asset Management	Insights da nuvem	Sem suporte
	Gestão de ativos de hardware - HAM	Aprimorado
	Software Asset Management	Aprimorado
	Gestão de ativos empresariais	Padrão
Gestão estratégica de portfólios (SPM)	Agile Development	Básico*
	Alignment Planner Workspace	Básico
	Application Portfolio Management	Básico
	Gestão de custos	Sem suporte
	Gestão de demandas	Básico
	Gestão financeira	Sem suporte
	Investment Funding	Básico
	Project Portfolio Management	Básico*
	Gestão de versões	Básico*
	SAFe (Scaled Agile Framework)	Básico*
	Gestão de testes	Básico*
	Estrutura de objetivos	Básico
IT Operations Management	Cloud Provisioning and Governance	Básico
	Agent Client Collector	Básico
	Descoberta	Padrão
	Gestão de eventos	Básico
	Espaço de operações de serviços para ITOM	Básico
	Análise de logs de integridade	Básico
	Inteligência para métricas	Básico
	Mapeamento de serviços	Básico
	Cloud Migration Assessment	Básico
	Biblioteca de Ações	Sem suporte
	Cloud Configuration Governance	Sem suporte
	Governança de marcadores	Básico
	Faturamento dos Insights da nuvem	Sem suporte
	Provisionamento e governança de nuvem: Google Cloud	Básico

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Pacote de produtos	Aplicação	Nível de suporte
	Provisionamento e governança de nuvem: Terraform	Básico
	Espaço de operações na nuvem	Básico
	Descoberta na nuvem	Padrão
IT Service Management	Benchmarks	Sem suporte
	Gestão de mudanças	Básico
	Coaching	Básico
	Gestão de melhorias contínuas	Básico
	Gestão de contratos	Sem suporte
	Linha de gasto	Sem suporte
	Gestão de comunicações de incidentes	Padrão
	Gestão de incidentes	Padrão
	Gestão de serviços de instalações	Padrão
	Gestão de incidentes	Padrão
	Agendamento de plantão	Padrão
	Gestão de ativos	Básico
	Gestão de problemas	Padrão
	Compras	Padrão*
	Catálogo de produtos	Padrão
	Gestão de solicitações	Padrão
	Catálogo de serviços	Padrão
	Gestão de nível de serviço	Básico
	Gestão de portfólio de serviços	Básico*
	Site Reliability Operations	Básico*
	Indisponibilidade de tarefa	Básico
	Separação de domínios e Espaço de gestão de fornecedores	Sem suporte
	Walk-Up Experience	Básico
Configuração e navegação para celular	Móvel	Básico
Now Intelligence	Painéis	Básico

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Pacote de produtos	Aplicação	Nível de suporte
	Performance Analytics	Aprimorado
	Otimização de processos	Básico
	Emissão de relatórios	Básico
	Análise da experiência do usuário	Básico
Now Platform	, Administração, App Engine Studio, Recursos da Now Platform, interface do usuário	
	Domain Separation e Bate-papo do agente	Padrão
	Advanced Work Assignment	Padrão
	Pesquisa com IA	As pesquisas respeitam as restrições de domínio de registros indexados
	App Engine Studio	Sem suporte
	Gestão de aplicações	Sem suporte
	Avaliações	Padrão
	Automated Test Framework	Padrão*
	Serviços de voz da ServiceNow	
	Assinatura de código	Suporte básico
	Pesquisa contextual	Padrão
	Gestão de configuração (CMDB)	Padrão
	Sistema de gestão de conteúdo	Sem suporte
	Credenciais e conexões	Padrão
	Certificação de dados	Básico*
	Classificação de dados	Aprimorado
	Privacidade de dados	Sem suporte
	Gestão de dados	Básico*
	Desenvolvimento delegado	Sem suporte
	Visualizações de dependências	Básico
	Serviços de documentos	Sem suporte
	Tradução dinâmica	Básico
	Edge Encryption	Suporte básico
	Criptografia em nível de coluna	Sem suporte

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Pacote de produtos	Aplicação	Nível de suporte
	Criptografia em nível de coluna para empresas	Sem suporte
	Criptografia da nuvem com gerenciamento de chaves	Suporte básico
	Normalização de Campo	Sem suporte
	Flow Designer	Padrão*
	Configuração assistida	Sem suporte
	Domain Separation e Integration Hub	Padrão*
	Integrações com aplicações e fontes de dados de terceiros	Básico+Padrão
	Gestão de conhecimento	Padrão
	Serviço de envio de mensagens Hermes	Sem suporte
	Documentos gerenciados	Sem suporte
	MetricBase	Básico
	Natural Language Understanding	Básico+Padrão
	Notificações	Padrão
	ODBC Driver	Básico*
	Orquestração	Padrão*
	Redefinição de senha	Padrão
	Segurança da plataforma	Página principal do Domain Separation
	Privacidade de dados	Sem suporte
	Inteligência preditiva	Padrão
	Gatilhos proativos	Básico
	Designer de automação de processos	Básico
	Tabelas remotas	Sem suporte
	Cronogramas	Básico
	Depurador de script	Básico
	Sugestões de pesquisa	Sem suporte
	portal de serviços	Sem suporte
	Domain Separation e Barra lateral	Padrão
	Fluxos de Estado	Sem suporte
	Gestão de assinaturas	Básico*

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Pacote de produtos	Aplicação	Nível de suporte
	Gestão de enquetes	Básico*
	Inteligência para tarefas	Sem suporte
	Separação de domínios e registro de horas	Básico*
	Construtor de IU	Padrão
	Virtual Agent	Básico
	Visual Task Boards	Básico
	Serviços Web	Padrão*
	Fluxo de trabalho	Padrão*
	Espaço	Padrão
Operações de segurança	Conformidade de configuração	Padrão
	Gestão de dados de configuração	Básico
	Ingestão de infração do IBM QRadar	Básico
	Integração de ingestão de alerta da API de segurança do Microsoft Graph	Básico
	Resposta a incidentes de segurança	Padrão
	Inteligência contra ameaças	Padrão
	Resposta a vulnerabilidades	Padrão
Gestão de serviços	Gestão de serviços de instalações	Padrão
	Manutenção planejada	Padrão*
	Gatilhos proativos	Básico
	Editor de código da NOW	Sem suporte
	Otimização da força de trabalho para ITSM	Básico
	Espaço de gestão de fornecedores	Básico

Práticas recomendadas do Domain Separation para provedores de serviço

Você pode criar, implementar e manter o Domain Separation para aplicações e serviços.

Noções básicas de domínio

Com o Domain Separation (também conhecido como ServiceNow Arquitetura de plataforma multilocatária), você pode separar os dados da aplicação, interface do usuário

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

e lógica de negócios em uma única instância de cliente que oferece suporte à modelagem hierárquica com inteligência entre locatários. A lógica de negócios descreve como o Domain Separation está configurado e quais regras estão afetando a configuração.

Antes de iniciar a jornada do Domain Separation, aqui estão algumas práticas recomendadas a serem seguidas. Selecione os tópicos conforme desejado ou siga-os na ordem clicando nos links abaixo da imagem.

Explicação sobre o Domain Separation

Com o Domain Separation, você pode separar dados de aplicação, IU e lógica de negócios, como regras ou fluxos de trabalho, em uma única instância de cliente. A separação desses elementos em domínios definidos logicamente oferece suporte a hierarquias específicas para todos os clientes que usam suas aplicações.

Noções básicas de domínio

O Domain Separation, também conhecido como ServiceNow arquitetura de plataforma multilocatária, adiciona uma despesa considerável ao gerenciamento de uma instância. No entanto, se você usar o Domain Separation corretamente, ele poderá melhorar a eficiência, adicionar mais segurança e aumentar o desempenho das instâncias de seus clientes.

Você não pode separar alguns padrões e propriedades globais, como propriedades do sistema e esquema de tabela, por locatário.

Antes de começar a separar domínios, leia as diretrizes a seguir.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

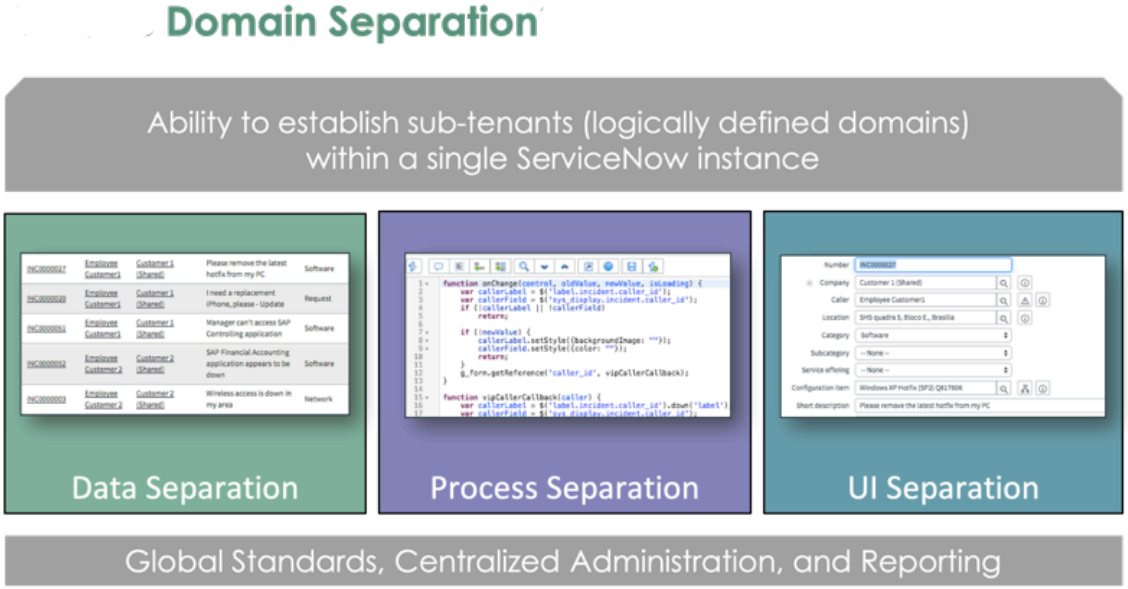
O que você pode fazer com o Domain Separation

- Separação de dados: permite que os locatários do domínio vejam somente os dados que eles têm permissão para ver. Os locatários podem ter acesso a outros dados do locatário, mas não podem consultar os dados do locatário aos quais eles não têm acesso.
  - Quando você atualiza registros de dados, eles não geram registros de Update Sets.
  - Os usuários, incluindo as contas do cliente que são usadas para integrações, veem somente os dados nos domínios que eles têm permissão para acessar.
  - Clientes, agentes e executantes veem dados que pertencem aos clientes e às organizações aos quais eles oferecem suporte.
- Separação de IU: oferece suporte a uma experiência específica de locatário para elementos de IU, como exibições, listas, rótulos e assim por diante.
  - Você pode substituir a interface do usuário baseada no navegador, incluindo menus da aplicação, listas, formulários, e painéis. Você também pode personalizá-los para um domínio específico ou conjunto de domínios enquanto preserva a lógica básica do processo.
  - Os provedores de serviço podem alterar a identidade visual exibida e os elementos de IU para atender às necessidades individuais do cliente.
- Separação de lógica de negócios: cria políticas de sistema específicas de locatário, como notificações por e-mail, regras de negócio, scripts de cliente, política de IU e ações de IU.
- Modelagem hierárquica: aninha seus vários locatários para que os locatários primários possam acessar recursos de locatários secundários. A lógica de negócios para locatários primários é executada automaticamente para locatários secundários, que você pode substituir em qualquer nível.
- Inteligência entre locatários: lida automaticamente com dados, metadados, lógica de negócios e contexto de processamento para locatários com acesso a dados de locatários adicionais.

Resumo do Domain Separation

O gráfico a seguir mostra a divisão de dados, o processo e a separação da IU. Esses conceitos são discutidos em detalhes na seção Práticas recomendadas.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

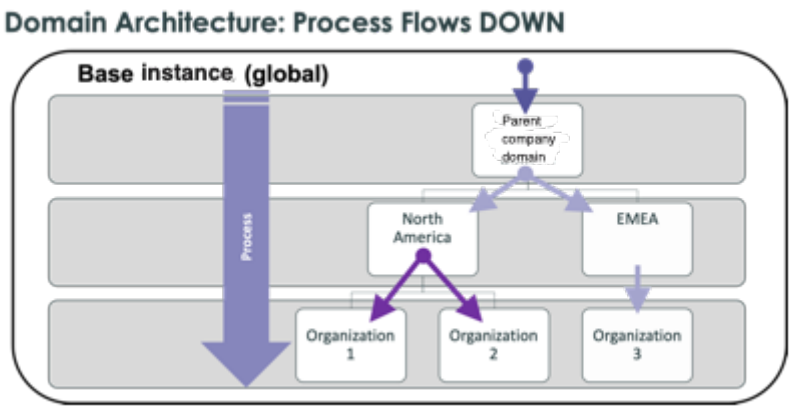


Arquitetura de domínio

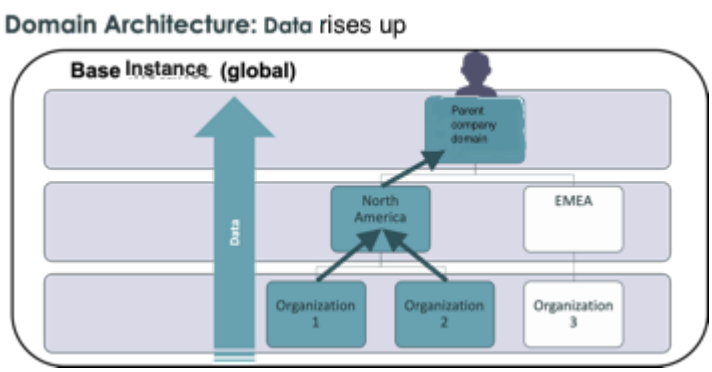
Registros de usuário são atribuídos a um valor de domínio que representa o domínio inicial do usuário. Os usuários não têm acesso a dados em domínios primários, domínios de mesmo nível ou domínios em outras ramificações da hierarquia.

Consulte Consultas "contém" e acesso ao domínio para opções avançadas para conceder visibilidade de domínio adicional.

O diagrama a seguir mostra como o processo de arquitetura flui para os domínios



secundários.



© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Proposta de valor do Domain Separation

Com o Domain Separation, os provedores de serviço podem ter uma arquitetura de instância multilocatária que entrega ofertas com eficiência e segurança aos clientes. Padrões de processo universais fortes, design de processo orientado por dados, governança estrita e administração centralizada ajudam a maximizar esses benefícios.

Benefícios do Domain Separation

Os locatários de um domínio se beneficiam de um rápido retorno do investimento, menor despesa administrativa e aproveitamento dos serviços de negócio fornecidos pelos proprietários da instância.

Aqui está uma exibição rápida desses benefícios.

Proprietário da instância	Locatários do domínio
Produtividade dos funcionários do provedor de serviço	Maior segurança
Somente deltas de processo mantidos	Processos e recursos pré-criados
Eficiências de administração	É necessária uma equipe reduzida
Menos integrações de cliente	Integração mais rápida
Capacidade de atualização e escalabilidade	Aproveitamento das versões mais recentes
Segregação de dados	Serviços fornecidos pelo proprietário da instância
Emissão de relatórios globais	

Definição do Domain Separation

Com o Domain Separation (também conhecido como a ServiceNow® Arquitetura de plataforma multilocatária), você pode separar dados da aplicação, IU e lógica de negócios em uma única instância de cliente que oferece suporte à modelagem hierárquica com inteligência entre locatários (cliente).

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Propriedades do Domain Separation

As aplicações separadas por domínio ServiceNow são definidos com as seguintes propriedades:

Separação de dados

Permite que os clientes vejam somente os dados que eles têm permissão para ver. Os clientes podem ter acesso a outros dados do cliente, mas não podem consultar os dados do cliente se eles não tiverem acesso.

Separação de IU

Oferece suporte a uma experiência específica de locatário para elementos de IU, como exibições, listas, rótulos e assim por diante.

Separação de lógica de negócios

Oferece suporte a políticas de sistema específicas de cliente, como notificações por e-mail, regras de negócio, scripts de cliente, política de IU e ações de IU.

Modelagem hierárquica

Oferece suporte a vários locatários aninhados para que os locatários primários (clientes) possam acessar recursos do cliente secundário. A lógica de negócios para clientes primários é executada automaticamente para clientes secundários e pode ser substituída em qualquer nível.

Inteligência entre clientes (escopo do domínio)

Lida automaticamente com dados, metadados, lógica de negócios e contexto de processamento para locatários que têm acesso a dados de locatários adicionais.

Hierarquias do Domain Separation

Crie uma hierarquia ao definir uma arquitetura de domínio para rastrear seus processos e fluxos de trabalho.

Amostra das hierarquias do Domain Separation

O diagrama a seguir é um bom ponto de partida para definir a arquitetura de domínio. Ele demonstra o relacionamento entre os domínios superiores e inferiores e como o processo, os dados e as regras de negócio afetam os domínios primários e secundários.

- No exemplo a seguir, TOP é um domínio de processo. Ele nunca deve conter usuários. Em vez disso, TOP deve conter os novos processos que os proprietários de instância desenvolvem e as substituições desses processos do domínio global.
- Somente o provedor de serviço (SP) tem acesso ao domínio-padrão. Este domínio nunca contém usuários ativos. Ele contém somente os dados "perdidos" que você precisa reatribuir ao domínio correto.

  Nota: Quando os dados não são atribuídos a um domínio específico, eles são movidos para o domínio-padrão. Eles estão temporariamente "perdidos" e precisam ser atribuídos ao domínio correto.

- Tarefas e usuários sem um domínio são colocados no domínio-padrão automaticamente quando você cria ou atualiza domínios. Você pode substituir essa ação desmarcando a opção **Padrão** neste registro ou selecionando a opção **Padrão** em outro registro de domínio. Se você ainda não definiu um domínio-padrão, as tarefas e os usuários sem domínio serão movidos para o domínio global.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Não mova dados entre domínios enquanto estiver usando a instância.
- Se algum dado terminar no domínio-padrão, isso significa que você tem um problema de configuração ou de procedimento para resolver.

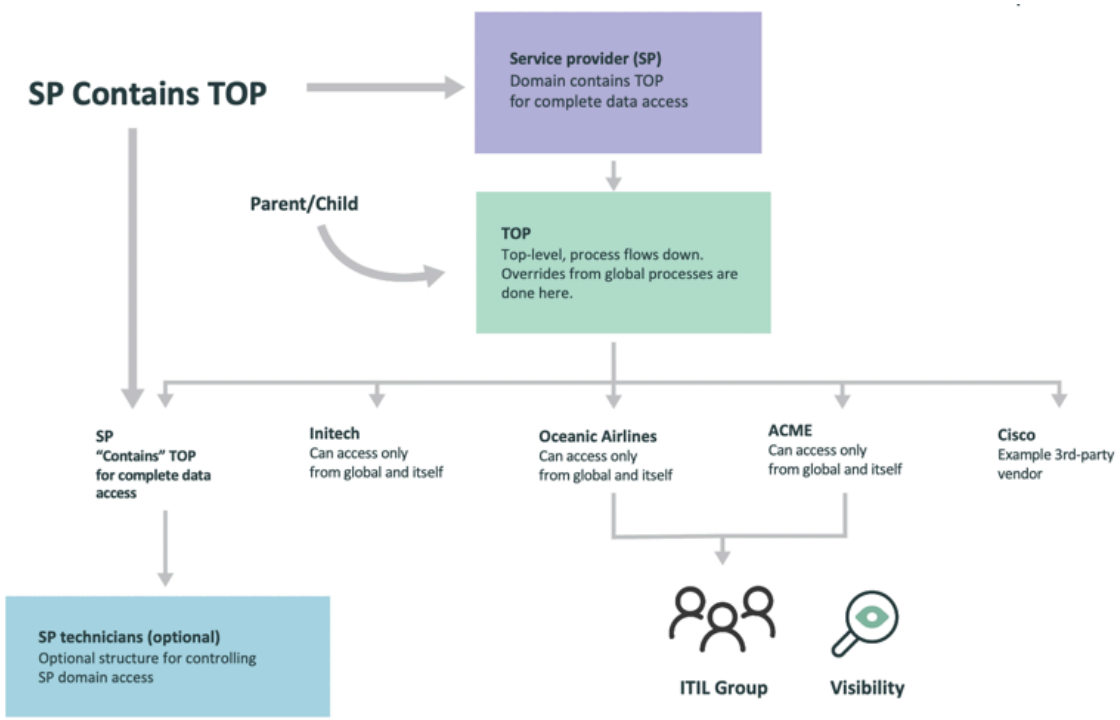
Você não vê a palavra "Global" neste diagrama porque não há domínio global. Lembre-se de que "global" é a ausência de um domínio em um registro.

Por exemplo, uma tabela sem campo de domínio significa que a tabela contém todos os registros globais. Uma tabela que tem um campo de domínio significa que qualquer registro sem um domínio é um domínio global.

A palavra "global" está no campo de domínio. Ela é usada automaticamente quando o registro não tem domínio.

Registros globais estão disponíveis para todos os usuários da instância, a menos que eles estejam restritos por configurações de segurança.

- Use o domínio-padrão para garantir que os registros não terminem no domínio global em tabelas que nunca devem ter registros globais.
- Os proprietários da instância devem fazer a triagem dos registros no domínio-padrão e movê-los para o domínio correto.



Hierarquias do domínio

- Primário/secundário: processo e dados afetados
  - Design baseado em um fluxo do processo.
  - Lembre-se de que os domínios primários podem acessar todos os dados nos domínios secundários.
- Domínio "Contém": somente os dados são afetados. Por exemplo, fazer com que o SP no diagrama contenha TOP não faz com que os processos no SP sejam executados no domínio TOP e para baixo.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Concede direitos de acesso a dados a indivíduos em grupos que exigem acesso dedicado a determinados domínios.
- Contém causas ou condições a serem adicionadas às consultas de banco de dados que podem causar problemas de desempenho com grandes conjuntos de dados e domínio.

- Visibilidade: a hierarquia que está sempre visível para os usuários depois que você fornece acesso. Somente os dados são afetados, não os processos.
  - Concede acesso aos dados de um domínio a outro domínio que não tinha esse acesso quando a hierarquia primária e secundária foi criada.
  - Permite que os usuários vejam todos os dados nos domínios aos quais eles têm acesso de visibilidade, o tempo todo, independentemente do registro em que estão trabalhando.

    Nota: Use com moderação, já que a Visibilidade pode permitir um acesso completo que você não pretende.

Princípios básicos para definir uma hierarquia de domínio

Casos de uso irrestritos e restritos para o Domain Separation.

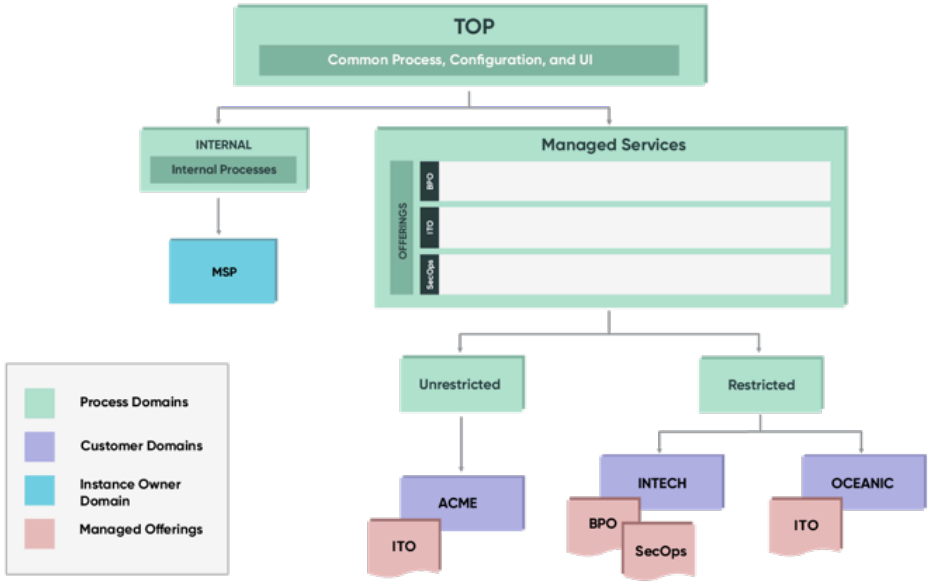
Muitos SPs têm clientes que declaram implicitamente que o acesso a seus domínios deve ser estritamente regulamentado, o que restringe o uso da função "contém" no domínio TOP. O diagrama a seguir explica como atenuar essa regulamentação dividindo os domínios em domínios Restritos e Irrestritos.

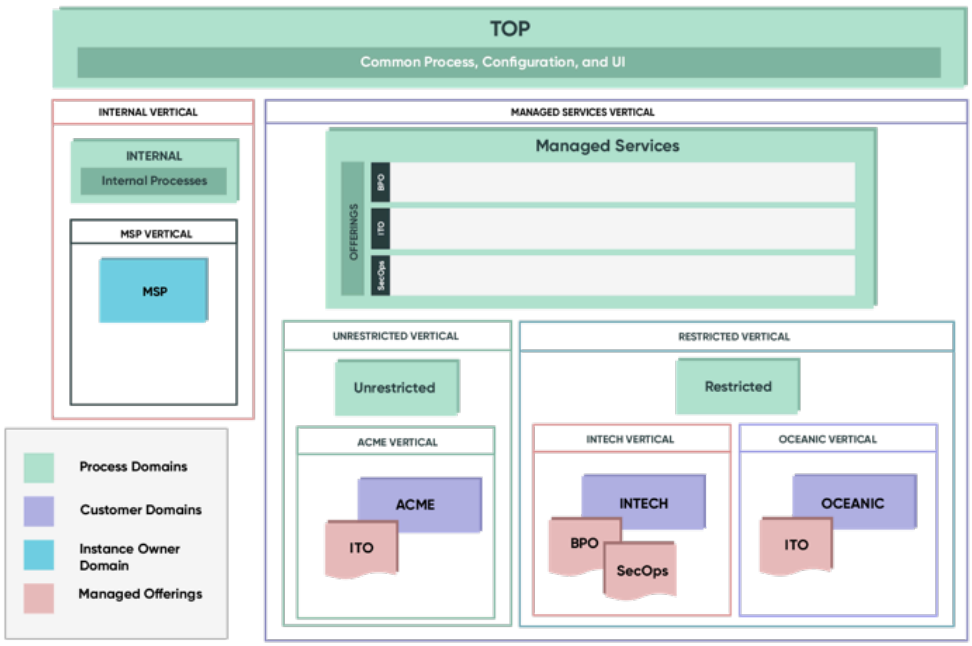
1. Os clientes existem em uma "vertical" específica da hierarquia do Domain Separation. Isso significa que eles consomem somente processos definidos em seu domínio e todos os domínios primários acima deles na hierarquia. Todos os processos definidos em domínios que não estão em sua hierarquia linear primária-secundária não se aplicam.

   Nota: Clientes ou "locatários" são entidades que são separadas umas das outras, não como departamentos ou unidades de negócios que compartilham recursos entre si.

2. Super verticais (restritos, serviços de gerente e assim por diante) são permitidos, desde que os clientes pertençam apenas a um deles.
3. Serviços, produtos ou ofertas que precisam estar disponíveis horizontalmente para todos os clientes não são definidos em hierarquias do domínio separadas.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.





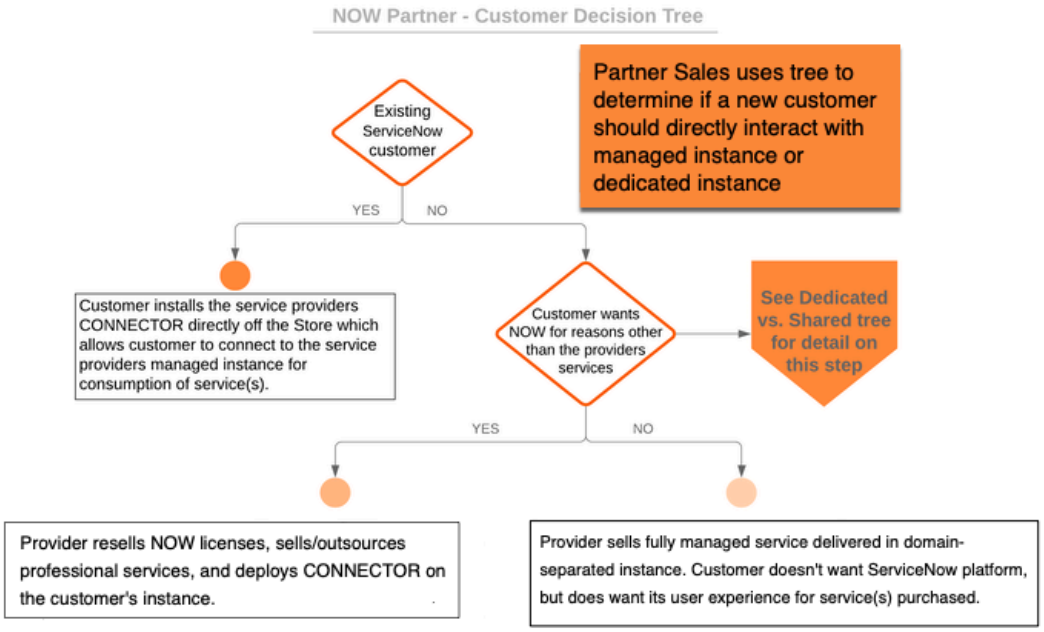
Aqui estão alguns exemplos de casos de uso:

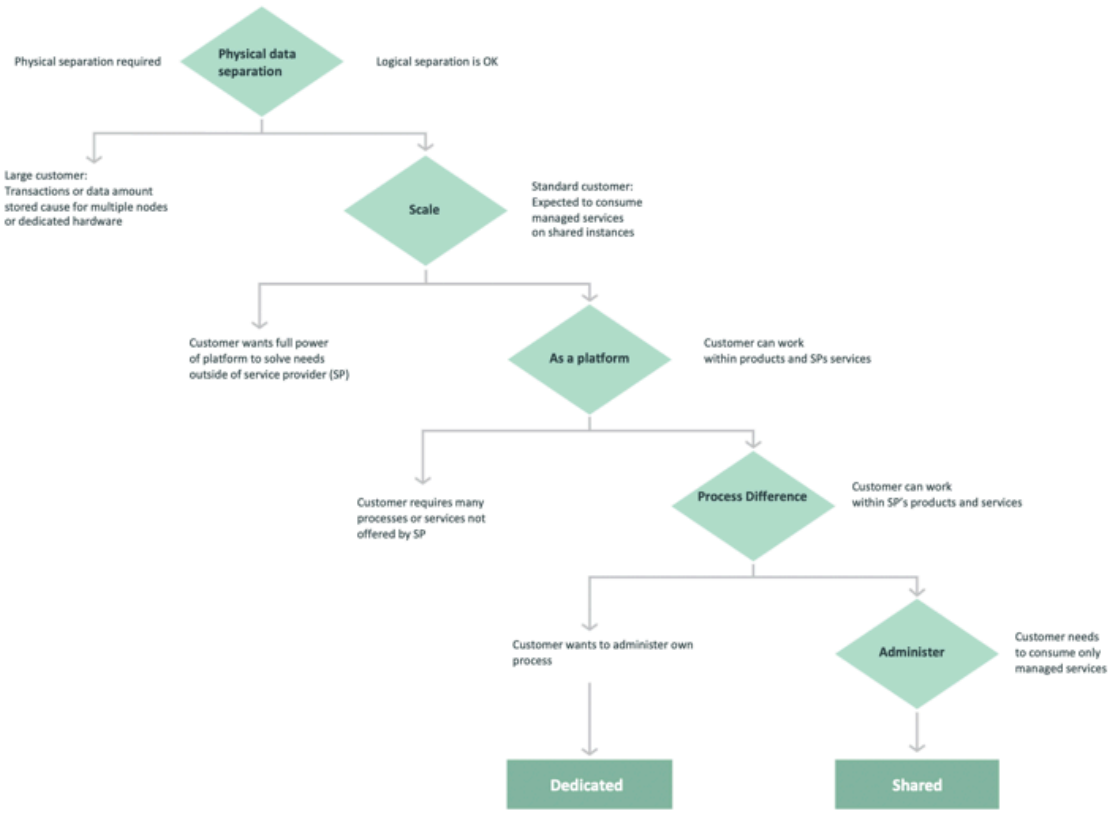
- Em TOP, você pode criar dois domínios, Irrestrito e Restrito.
  - Coloque os clientes e seus domínios que não têm restrições de visibilidade de SP em Irrestrito.
  - Coloque os clientes e seus domínios que têm esse requisito em Restrito.
- Os administradores do sistema podem usar as funções "contém" e "visibilidade" de maneira eficiente e direcionada.
  - Aplique "contém" a Irrestrito, para que um único "contém" possa conceder visibilidade à maioria dos clientes.
  - Aplique a visibilidade do domínio usando "grupos de visibilidade do domínio" a domínios específicos, conforme necessário.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Árvores de Decisão do Cliente

O diagrama a seguir descreve como escolher qual modelo de hierarquia é ideal para você. Você pode escolher hierarquias separadas, híbridas ou compartilhadas, dependendo de quais processos e funcionalidades você deseja nas estruturas de domínio.





Para saber mais sobre a arquitetura de hierarquia, consulte Arquitetura de referência do provedor de serviço.

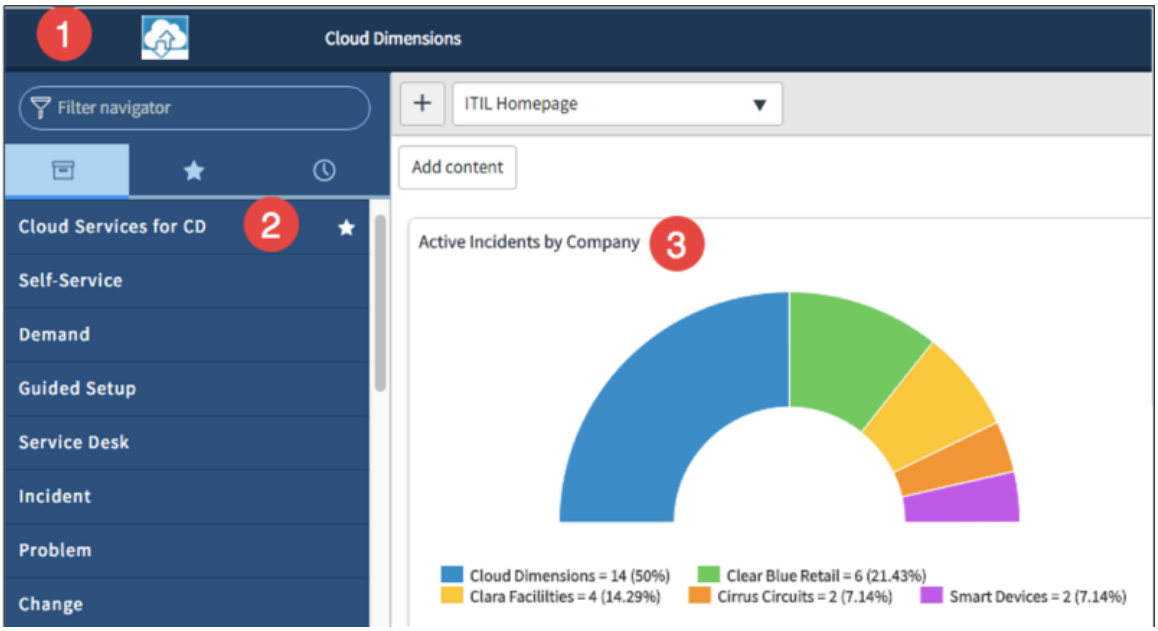
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Contexto e Domain Separation

O contexto da sessão de um usuário determina os processos, os dados e a interface do usuário (IU) conforme o usuário navega pelas exibições de lista, páginas iniciais, relatórios e artigos de conhecimento. O contexto é determinado pelos processos que você cria, as regras de negócio que você define, seus fluxos de trabalho e outros fatores.

Contexto da sessão do usuário

Muitos fatores determinam o contexto de uma sessão de usuário, como perfis de usuário, grupos, critérios da empresa e assim por diante. No diagrama a seguir, você vê que os incidentes que uma empresa criou fazem parte do contexto.



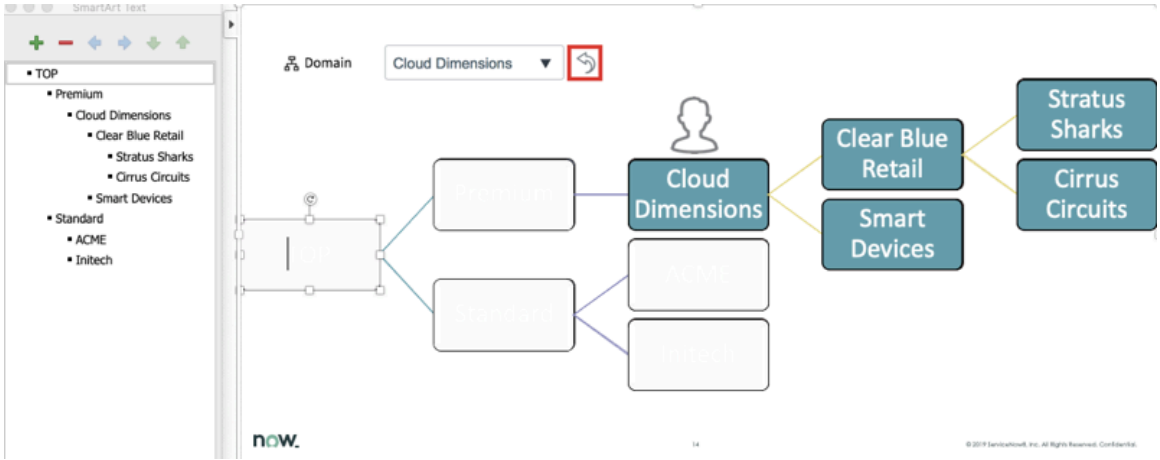
O usuário neste exemplo tem um domínio inicial de Dimensões de nuvem.

1. A identidade visual reflete as configurações no domínio Dimensões de nuvem e no registro da empresa.
2. O navegador de aplicações mostra os itens que são herdados de domínios de nível superior, bem como os módulos que são definidos no domínio Dimensões de nuvem.
3. As páginas iniciais e os dados da lista refletem os dados visíveis para o usuário. Esses dados são baseados no contexto da sessão do usuário. Nesse caso, o usuário no domínio Dimensões de nuvem pode ver os dados em Dimensões de nuvem, domínios secundários e o domínio global.

O contexto da sessão do usuário começa no domínio inicial

No diagrama a seguir, você pode ver os elementos do contexto.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



O administrador do sistema define os domínios iniciais dos usuários em seus registros de usuário. Normalmente, o domínio inicial de um usuário é definido como o mesmo domínio da empresa. Quando o usuário faz registro em log, o seletor de domínio é definido automaticamente como o domínio inicial do usuário. Os usuários podem retornar ao domínio inicial a qualquer momento, clicando no ícone de seta no seletor de domínio.

A lista do seletor de domínio inclui domínios no contexto de sessão do usuário. Os usuários podem limitar ainda mais o contexto da sessão selecionando domínios secundários com o seletor.

O contexto da sessão do usuário inclui o domínio inicial do usuário e todos os domínios secundários. Este conjunto de domínios no contexto da sessão do usuário é anexado automaticamente a cada consulta enviada ao banco de dados. Dessa forma, os resultados são limitados apenas aos dados nesses domínios e aos dados globais. Este processo está incorporado no código compilado que não está acessível.

As contas de serviço usadas para integrações também têm contexto da sessão do usuário. Há contexto de usuário e contexto de registros, cada um com seus próprios dados em seu próprio domínio. Esses contextos afetam as integrações. Consultas de banco de dados (registros) são limitadas da mesma forma que usuários interativos (usuários), o que significa que elas funcionam normalmente, mas são limitadas por quaisquer restrições que o desenvolvedor tenha configurado.

Você pode aprender sobre maneiras adicionais de adicionar domínios ao contexto de sessão de um usuário em Arquitetura de referência do provedor de serviço.

Contexto de registro

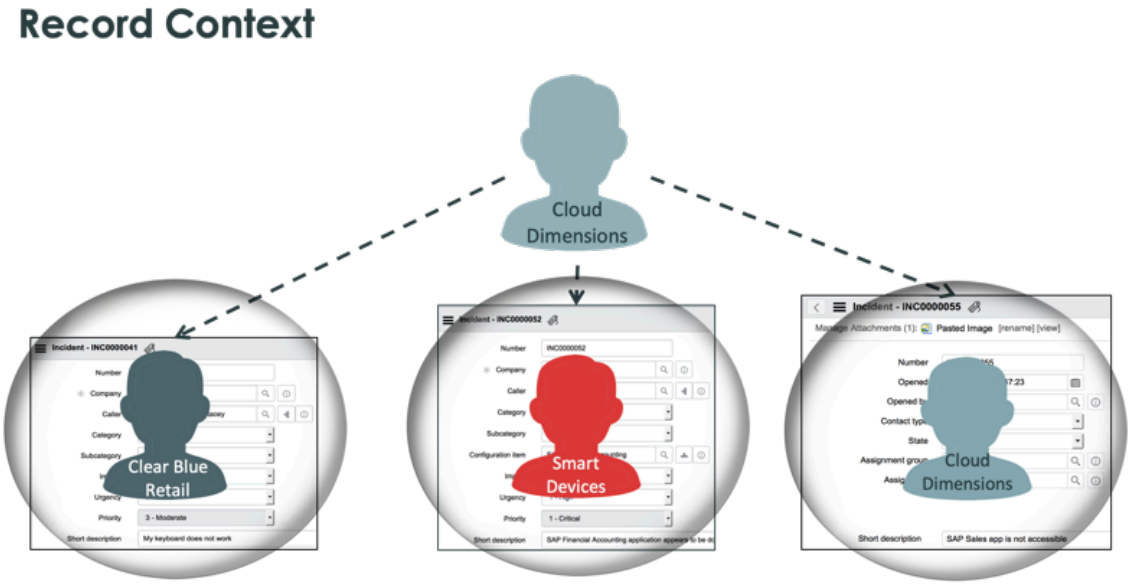
Conforme um usuário detalha registros individuais, o contexto de registro é ativado. O contexto de registro determina os elementos e processos de IU a serem aplicados ao registro.

O domínio de um registro determina o processo, os dados e a disponibilidade de elementos de IU no registro.

Nota:

- O contexto de registro persiste mesmo se o domínio do usuário for alterado.
- Os usuários podem exibir registros simultaneamente em várias guias do navegador, enquanto mantêm seu próprio contexto de registro.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

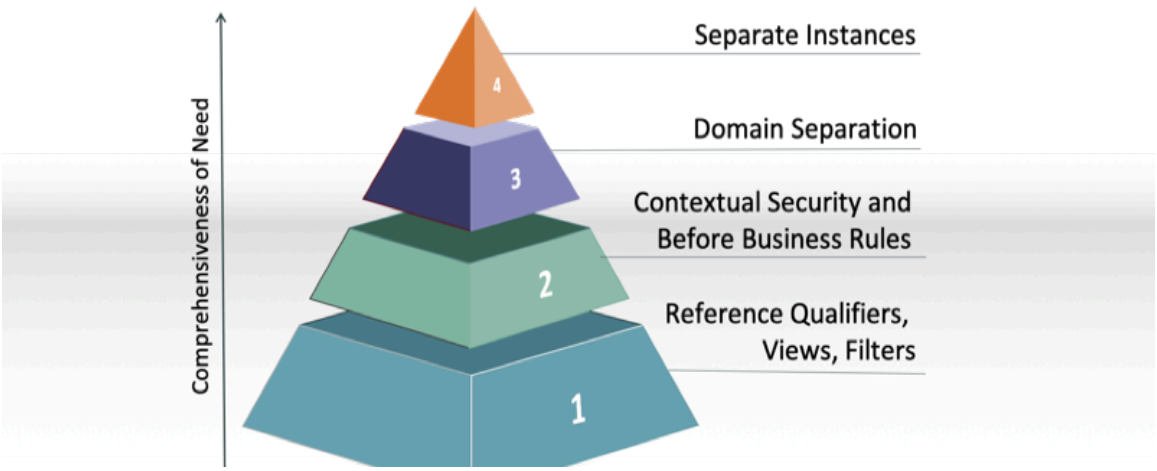


Segregação e proteção de dados com Domain Separation

Você pode segregar e proteger dados na plataforma ServiceNow de várias maneiras, dependendo das necessidades do cliente.

Segregação de dados de várias maneiras

O diagrama a seguir mostra quatro maneiras de segregar dados. Você pode usar instâncias separadas, Domain Separation, segurança contextual e regras de negócio, e a própria arquitetura de referência como formas de segregar dados.



Você pode segregar dados destas quatro maneiras:

1. Personalizar a arquitetura de referência com qualificadores e filtros para que os departamentos e grupos de uma empresa possam se concentrar em seu próprio trabalho. Ao segregar os dados entre esses departamentos ou grupos, um departamento ou grupo não pode ver registros de outro departamento ou grupo.
2. Adicionar segurança contextual e regras de negócio Antes da consulta como camadas adicionais de segurança para proteger contra violações de dados. Consulte Contexto e Domain Separation e Regras de negócio Antes da consulta para saber mais sobre o Domain Separation e as regras de negócio.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Adicionar outro nível de segurança em uma empresa usando o Domain Separation. Os dados de cada consulta ao banco de dados são limitados aos dados visíveis em um domínio antes que a segurança contextual e as regras de negócio sejam executadas.
4. Como usar instâncias separadas para segregar os dados no banco de dados e na camada da aplicação.

Instâncias separadas, Domain Separation, segurança contextual e regras de negócio, e a arquitetura de referência são formas de segregar dados. Essas quatro maneiras estão relacionadas entre si, conforme indicado pela seta Abrangência de necessidade no diagrama. Como cada camada interage com as outras camadas depende de como você definiu a configuração do Domain Separation.

Nem todas as organizações exigem o Domain Separation. Você pode encontrar outras alternativas, como instâncias separadas ou uma única instância sem um domínio. Para saber mais sobre essas alternativas, consulte Avaliação da necessidade do Domain Separation.

Inteligência entre locatários

Uma arquitetura de vários locatários é onde você tem uma única instância que atende a vários locatários. Dados, metadados, lógica de negócios e contexto de processamento para locatários são resolvidos automaticamente com acesso a dados de locatários adicionais.

Um único locatário versus vários locatários

Instância de locatário único

Você é um cliente ServiceNow, comprou as licenças e depende de você decidir quais serviços deseja. Você pode fazer upgrade quando quiser, ver visualizações de todos os novos recursos excelentes e configurar sua instância imediatamente. Ser um único locatário tem estes benefícios e restrições:

- Você tem custos iniciais e despesas administrativas mais altos, mas tem mais liberdade para reformar e expandir.
- Você tem custos mais altos para obter e manter a instância e a equipe de administração de suprimentos. Embora você seja livre para criar o ambiente conforme necessário, você deve estar em conformidade com as ServiceNow práticas e padrões recomendados.

Instância de vários locatários

Outra pessoa é proprietária da instância, possivelmente um provedor de serviço com vários clientes. Eles fazem upgrade quando desejam e colocam novos serviços na instância quando desejam. Se você é cliente de um provedor de serviço, provavelmente está na instância dele porque quer o que ele oferece. Vários locatários têm estes benefícios e restrições:

- Uma equipe centralizada administra configurações, integrações e upgrades.
- O proprietário da instância presta serviços adicionados.
- Os locatários do domínio têm custos iniciais mais baixos para usar a plataforma ServiceNow, têm custos mensais mais baixos porque a compartilham com muitos locatários e não precisam empregar uma equipe para administrar o ambiente.
- Benefícios compartilhados de solicitações ou mudanças que são iniciadas por outros locatários.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Alternativas à separação de domínios

Você pode usar uma instância separada como alternativa à separação de domínios para seus clientes. Uma instância separada permite a flexibilidade para atender aos requisitos de separação de dados nos grupos e departamentos em uma organização com pouco ou nenhum impacto nas outras pessoas.

Instâncias separadas

Prós e contras de instâncias separadas

Instância separada	Instância única - sem domínio
Pontos positivos	**Pontos positivos**
Criada para atender a cada cliente/ organização	Pode tratar de cenários simples
Minimize o impacto da personalização em outras pessoas	Custo
Coordenação de programação de versão	**Pontos negativos**
Limpar separação	Modificações extensas no código de linha de base
Escolha a região DATACENTER	Código do sistema de base modificado ignorado durante os upgrades
Pontos negativos	Deve abordar todas as tabelas secundárias e de suporte também
Custo	Testes extensivos necessários
Alinhamento de instâncias	Nenhuma ServiceNow equipe de produto para evoluir seu código personalizado
Esforço de teste para upgrades	
Duplicação de esforço	
Integrações necessárias	

Você pode cronometrar os upgrades e versões separadamente para cada instância. No entanto, se você optar por usar instâncias separadas, precisará coordenar bastante com outras pessoas que estão administrando as instâncias. Ao configurar uma instância com segurança contextual, visualizações do formulário, qualificadores de referência, filtros e condições robustas, você não precisa usar a Separação de domínios em sua empresa.

Com uma instância separada, você pode lidar com a separação de dados e processos, mas os proprietários da instância devem manter e acompanhar as extensas personalizações necessárias para instâncias separadas.

Informações relacionadas

- Contexto e Domain Separation
- Arquitetura de referência do provedor de serviço

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Avaliação da necessidade do Domain Separation

Você pode descobrir que o Domain Separation nem sempre funciona para as organizações de seus clientes. É melhor que você baseie sua decisão de optar pelo Domain Separation observando as necessidades dos clientes.

Avaliação da necessidade do Domain Separation

Motivos para o Domain Separation

Esses fatores podem ajudá-lo a decidir escolher o Domain Separation para as organizações de seus clientes:

- Seus clientes têm alinhamento moderado de processos e requisitos gerais de plataforma.
- Seus clientes planejam trabalhar em tarefas como executantes em vez de solicitantes.
- Seus clientes têm um acordo contratual que requer que os registros de dados sejam isolados, mas o proprietário da instância determinou que o requisito pode ser tratado em outro lugar na configuração.
- Os proprietários de instância da sua empresa têm entidades inteiras que operam como organizações fisicamente separadas e não compartilham dados, mas a emissão de relatórios completa ainda é necessária. Domínios separados permitem a visibilidade dos dados quando configurados corretamente.

Motivos para não usar o Domain Separation

Esses fatores podem apontar motivos pelos quais as organizações de seus clientes podem não querer configurar o Domain Separation:

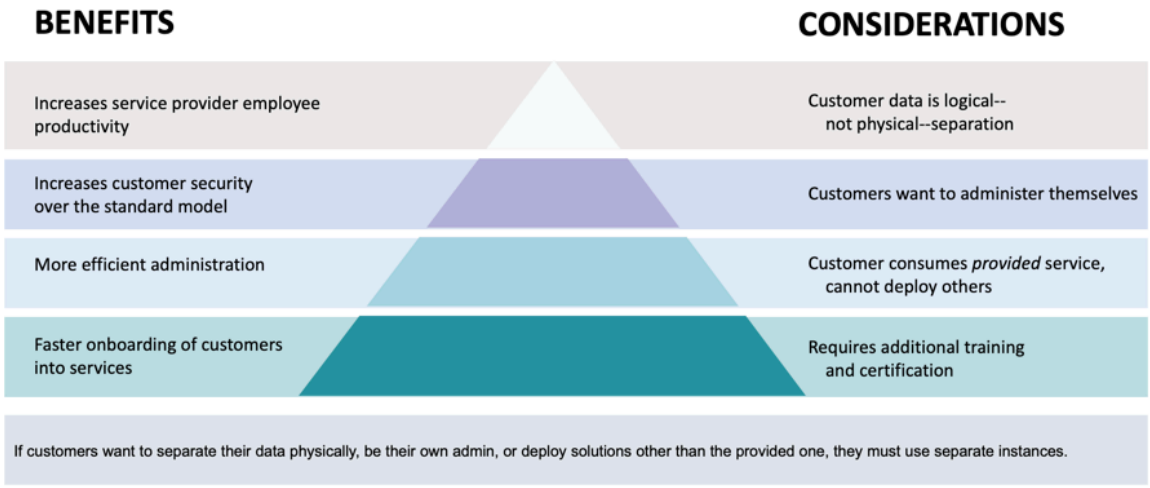
- Seus clientes desejam administrar seu ambiente, ter total propriedade sobre ele e definir o mapa para expansão.
- Seus clientes exigem que os dados e o processo no nível físico ou de banco de dados sejam completamente isolados.

Nota:

As instâncias separadas por domínio contêm um banco de dados compartilhado, portanto, isso prejudica o requisito de isolamento.

- Os departamentos na organização de seus clientes desejam isolar registros. (Controles de acesso podem ser suficientes).
- Todos os seus clientes desejam processos, regras de negócio e fluxos de trabalho próprios.
- A cultura corporativa é de não colaboração entre as organizações de seus clientes.
- Seus clientes interagem com a plataforma somente como usuários finais.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

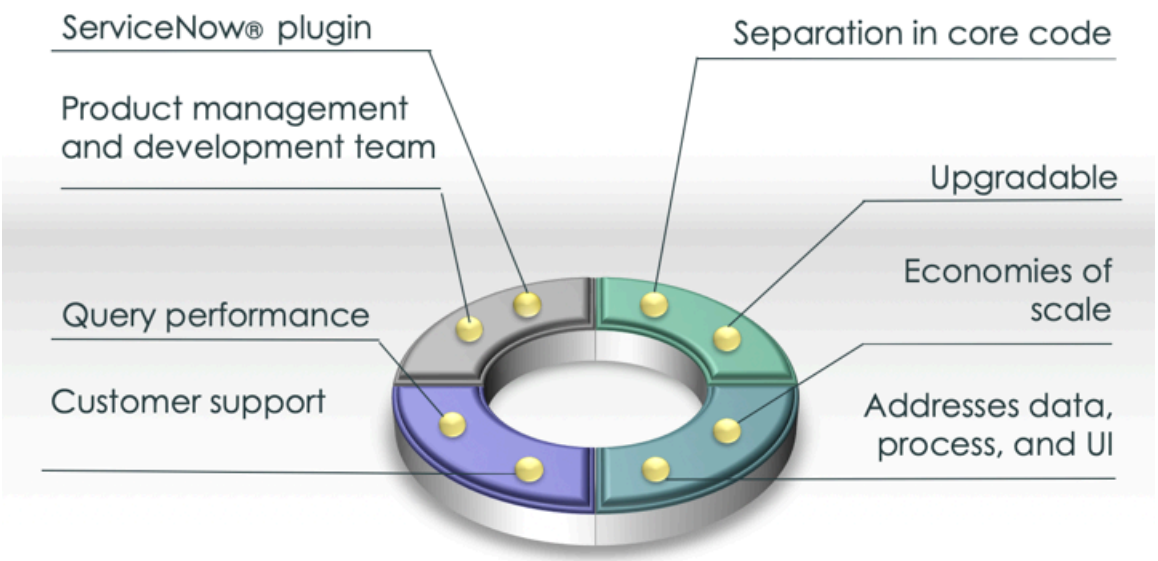


Benefícios do Domain Separation

O Domain Separation pode funcionar melhor para as organizações dos clientes do que qualquer outro método para separar os dados entre grupos e departamentos.

Resumo dos benefícios do Domain Separation

Você pode habilitar o Domain Separation com um plug-in ServiceNow que tenha funcionalidade integrada à plataforma principal. A configuração de domínios separados é gerenciada por um gerente de produto que tem suporte de uma equipe de desenvolvimento. Aprimoramentos e correções para a funcionalidade do Domain Separation estão inclusos nas versões ServiceNow e prontos para serem usados pelos clientes. Para assistência com o Domain Separation, os proprietários da instância podem usar Suporte e atendimento ao cliente recursos, como o Portal de serviços.



Como uma consulta ao banco de dados funciona com o Domain Separation

Usar consultas de banco de dados com Domain Separation nas aplicações dos clientes os ajuda a proteger seus dados. Essas consultas aceleram os processos de configuração e compilação.

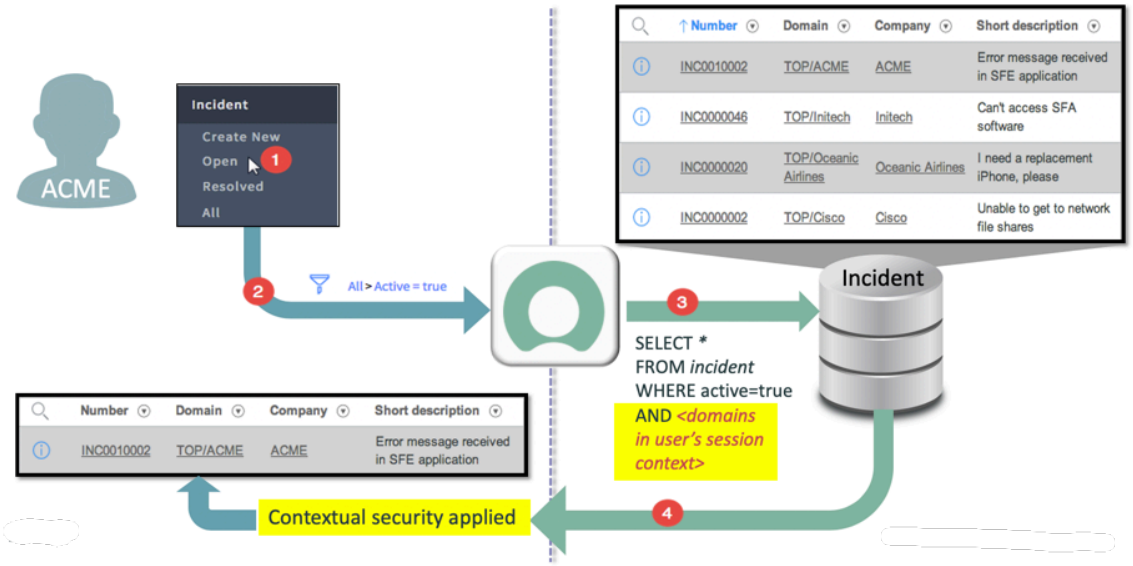
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Como o Domain Separation protege os dados

Na figura a seguir, a tabela Incidente [incidente] tem um campo de domínio que é herdado da tarefa do incidente. Ao ver este campo de domínio, você sabe que os registros na tabela podem ter atribuições de domínio.

Quando os usuários fazem login, seu domínio inicial aparece com o conjunto de domínios que eles podem acessar. Isso é chamada de contexto da sessão do usuário. Para obter mais informações sobre os contextos das sessões, consulte Contexto e Domain Separation.

Consulta ao banco de dados com o Domain Separation



1. Em um navegador, o usuário de uma das empresas, a Acme, seleciona o módulo Incidentes em aberto para exibir todos os incidentes em que ativo = verdadeiro.
2. O filtro active=true é enviado para a aplicação.
3. A aplicação envia uma consulta ao banco de dados anexando uma cláusula WHERE a active=true. A cláusula WHERE limita os registros de incidentes que são retornados aos registros que estão no domínio do usuário ou aos domínios que o usuário pode acessar. Somente os registros nesses domínios são retornados à aplicação para processamento.
4. A segurança contextual é aplicada, limitando ainda mais os dados que são retornados ao usuário. Os registros de incidentes aparecem na lista de Incidentes abertos.

Nota:

Ao aplicar a segurança contextual, você cria limites para os dados que são retornados ao usuário. Esses limites protegem outros conteúdos que você pode não querer que os usuários vejam.

Para saber mais sobre segurança contextual, consulte Contexto e Domain Separation.

Nota: Esta lógica de processamento se aplica a todas as consultas ao banco de dados, incluindo as consultas que são acionadas usando integrações.

Níveis de suporte do Domain Separation

Escolha entre três categorias para separação de domínios de uma aplicação para as organizações dos clientes.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Aplicações que oferecem suporte ao Domain Separation podem oferecer suporte à separação de dados e roteamento de dados, ter separação de lógica de negócios avançada ou oferecer suporte à administração de nível de locatário (cliente) da aplicação. Essas definições delineiam os níveis de suporte da perspectiva dos casos de uso reais e das pessoas que os implementam.

Níveis de suporte ServiceNow incrementais

Nível	Tipo	Resumo
Sem suporte		• O campo de domínio pode existir em tabelas de dados, mas não há lógica de negócios para gerenciar os dados. • Este nível não é considerado separado por domínio.
Básico	Gestão de dados de clientes	• Lógica de negócios: garante que os dados vão para o domínio adequado para os casos de uso do provedor de serviço de aplicação. • Na aplicação, a interface do usuário, as chaves de cache, a emissão de relatórios, os acúmulos, as agregações, e assim por diante, levam em consideração as propriedades do domínio em tempo de execução. • Os proprietários da sua instância devem conseguir configurar a aplicação para funcionar normalmente em vários locatários. Caso de uso: quando um provedor de serviço usa o bate-papo para responder a uma mensagem do cliente, o cliente deve ser capaz de ver a resposta.
Padrão	Gestão de processo dos clientes	• Inclui o nível Básico • Lógica de negócios: os processos podem ser criados ou modificados por cliente pelo provedor de serviço.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nível	Tipo	Resumo
		Os casos de uso refletem como a aplicação é usada por vários clientes de provedor de serviço em uma única instância. • Os proprietários da instância precisam ser capazes de configurar a lógica de negócios do MVP (Minimum Viable Product, produto mínimo viável) e os parâmetros de dados por cliente para a aplicação específica. Caso de uso: um administrador deve ser capaz de fazer os comentários necessários quando um registro é encerrado para um cliente, mas não para outro.
Aprimorado	Configuração autogerenciada pelo cliente	• Inclui os níveis Básico e Padrão • Permite que os clientes do provedor de serviço modifiquem a lógica de negócios baseada em casos de uso definidos. Essas configurações são baseadas em IU e à prova de falhas para que as configurações de um cliente não possam afetar outro cliente. • Os clientes da instância devem ser capazes de configurar a lógica de negócios do MVP e os parâmetros de dados. Caso de uso: o cliente de um ambiente compartilhado deve ser capaz de fazer mudanças de acordo com o impacto, a urgência ou a prioridade em um domínio.
Domínio efetivo*		Em alguns casos, um recurso de plataforma ou aplicação pode oferecer suporte a casos de uso de provedor de serviço, mesmo se a estrutura de domínio não estiver sendo usada. Os casos de uso devem ser detalhados para oferecer suporte ao Domain Separation. Um asterisco (*) após o nível de suporte indica este tipo de configuração. Caso de uso: antes da versão New York, Catálogo de serviços não tinha suporte de domínio, mas os proprietários da instância podiam configurar catálogos e itens separados para cada locatário em uma instância separada por domínio usando critérios do usuário. O resultado foi que

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nível	Tipo	Resumo
		cada locatário pode usar o Catálogo de serviços no nível Padrão.

Para exibir todos as aplicações listadas por seu nível de suporte, consulte Compatibilidade de aplicações com o Domain Separation.

Resumo

O Domain Separation é uma estrutura que você deve usar para tornar as aplicações cientes dos clientes.

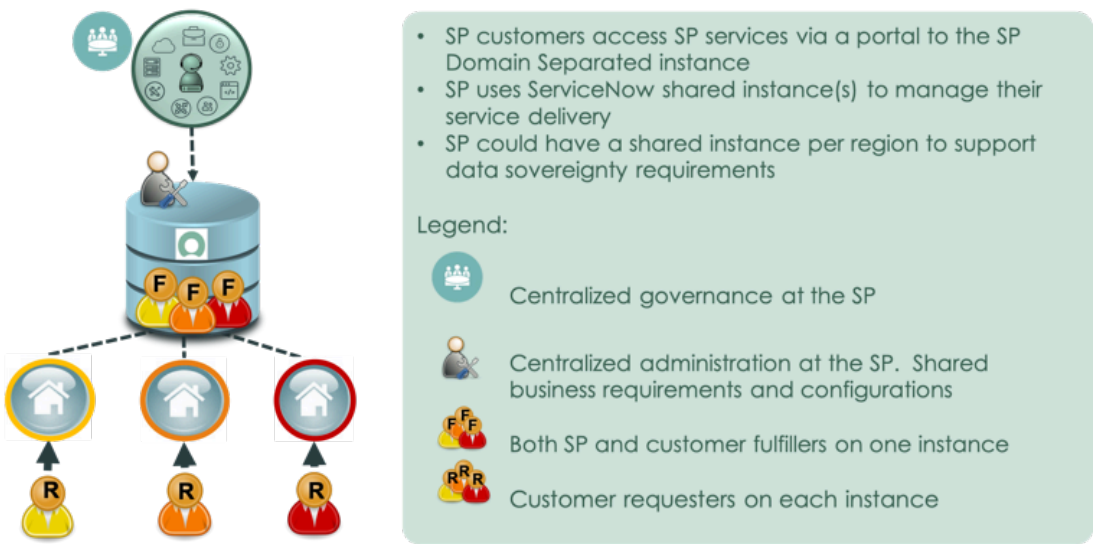
Considere os recursos da estrutura de domínio, os casos de uso de negócios de suas aplicações, quais são as personas e como elas usam a aplicação antes que você possa usar a estrutura para tornar sua aplicação passível de suporte.

Arquitetura de referência do provedor de serviço

Os clientes podem acessar os serviços do provedor de serviço (SP) usando um portal projetado para que eles acessem sua instância separada por domínio.

Atributos básicos da arquitetura de referência do provedor de serviço

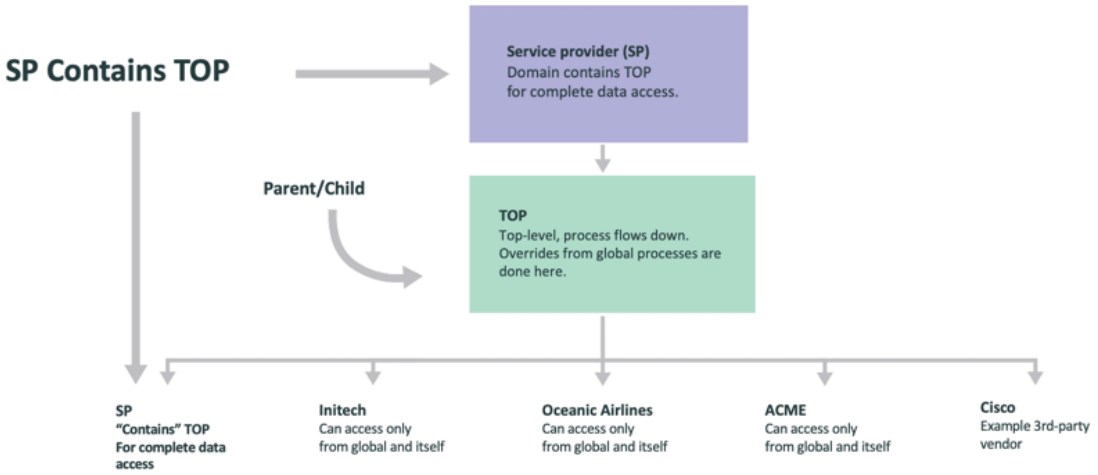
- Você não atribui executantes a um domínio. Em vez disso, você os compartilha entre domínios. Isso torna mais difícil auditar quantos executantes você tem por domínio.
- Você pode compartilhar e aproveitar a administração de domínio. Isso significa que não há sobrecarga e que você pode otimizar licenças.
- O número de usuários na instância pode mudar quando você obtém um novo cliente. Um novo cliente pode resultar em dezenas ou até mesmo centenas de milhares de novos usuários no sistema. O número total de usuários é virtualmente ilimitado em um ambiente compartilhado.



O portal para serviços de SP é dedicado ou compartilhado com a instância compartilhada do SP. Os provedores de serviço usam instâncias compartilhadas de ServiceNow para gerenciar sua entrega de serviço.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Hierarquia de referência para instâncias separadas por domínio



Comparação da arquitetura de referência do SP

Standalone (SA)		Multi-Tenant (MT)		Hybrid (MT+SA)		SIAM (Multi-Vendor)	
Platform as a Service	Enterprise scale	Processes simplified	Cost reduction	Managed Services (MT)	Custom Services (SA)	Service Integration	Multi-supplier governance
Customer wants full power of platform to Solve own needs outside those offered by SP.	Large customer: Transactions or data amount stored cause for multiple nodes or dedicated hardware.	Global governance & admin for business use case & process can be developed & maintained on the instance. Best when used w/ minor-to-moderate process differences among customers or sub-entities.	Lower administration, transaction, & onboarding costs, & ongoing operational costs for resources & licensing. Faster onboarding = more revenue.	Standardized re-usable services. procedures. processes, & resources delivered on a single ServiceNow instance to multiple Customers.	Services for sole use of customer, offerings specific to industry or vertical solutions, government, or regulatory requirements, applications that do not support Domain Separation.	Multiple best in class Service providers for individual services bringing together tooling, reporting, SLAs, strategy, & design for unified customer experience.	Unified governance across all providers to ensure organization requirements are met & that all providers cooperate on behalf of the customer.

Árvores de decisão da arquitetura de referência do provedor de serviço

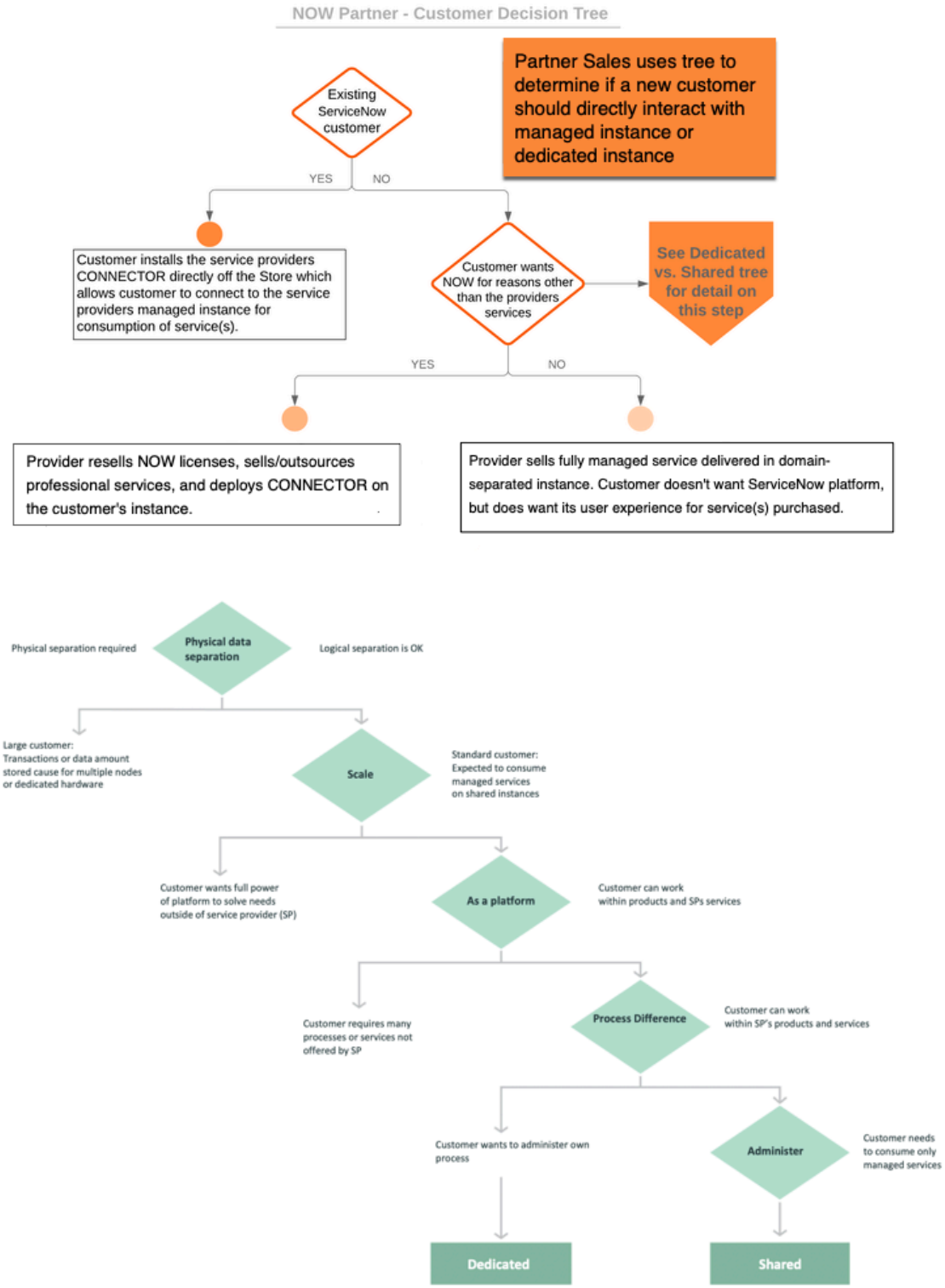
Você pode usar árvores de decisão e um gráfico de comparação para determinar se um novo cliente deve ser adicionado a uma instância compartilhada ou à sua própria instância dedicada.

Árvores de decisão

Use essas árvores de decisão para ajudar seus clientes a decidir se devem usar uma instância gerenciada ou dedicada.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Árvore de decisão do cliente



© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

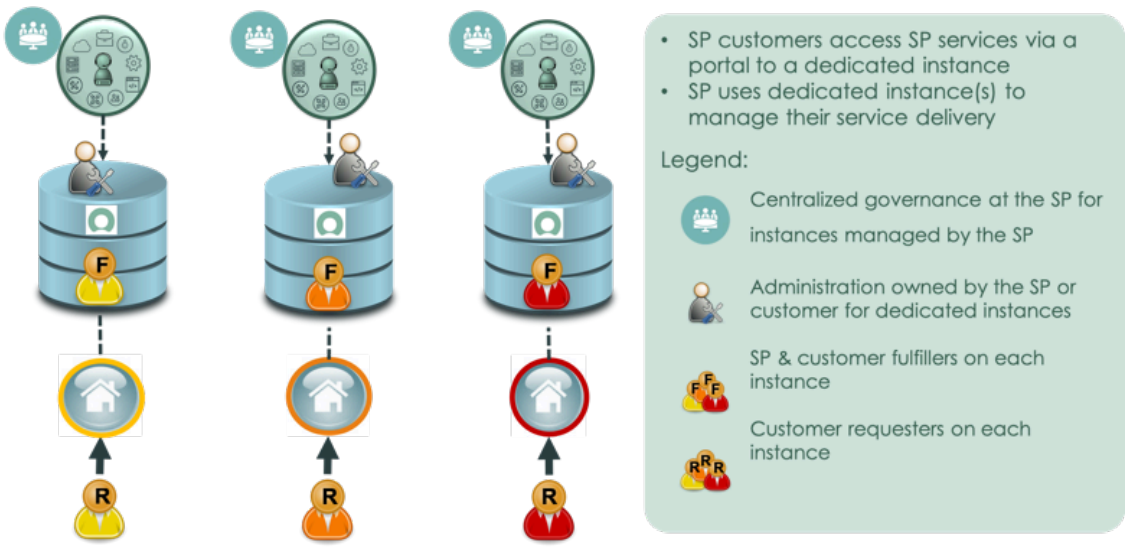
Comparação da arquitetura de referência do SP

Standalone (SA)		Multi-Tenant (MT)		Hybrid (MT+SA)		SIAM (Multi-Vendor)	
Platform as a Service	Enterprise scale	Processes simplified	Cost reduction	Managed Services (MT)	Custom Services (SA)	Service Integration	Multi-supplier governance
Customer wants full power of platform to Solve own needs outside those offered by SP.	Large customer: Transactions or data amount stored cause for multiple nodes or dedicated hardware.	Global governance & admin for business use case & process can be developed & maintained on the instance. Best when used w/ minor-to-moderate process differences among customers or sub-entities.	Lower administration, transaction, & onboarding costs, & ongoing operational costs for resources & licensing. Faster onboarding = more revenue.	Standardized re-usable services. procedures. processes, & resources delivered on a single ServiceNow instance to multiple Customers.	Services for sole use of customer, offerings specific to industry or vertical solutions, government, or regulatory requirements, applications that do not support Domain Separation.	Multiple best in class Service providers for individual services bringing together tooling, reporting, SLAs, strategy, & design for unified customer experience.	Unified governance across all providers to ensure organization requirements are met & that all providers cooperate on behalf of the customer.

Arquitetura de referência do provedor de serviço para instâncias dedicadas

Os clientes do provedor de serviço (SP) podem acessar os serviços de SP usando um portal para uma instância dedicada. Os SPs usam essas instâncias dedicadas para gerenciar sua entrega de serviço.

Instâncias dedicadas



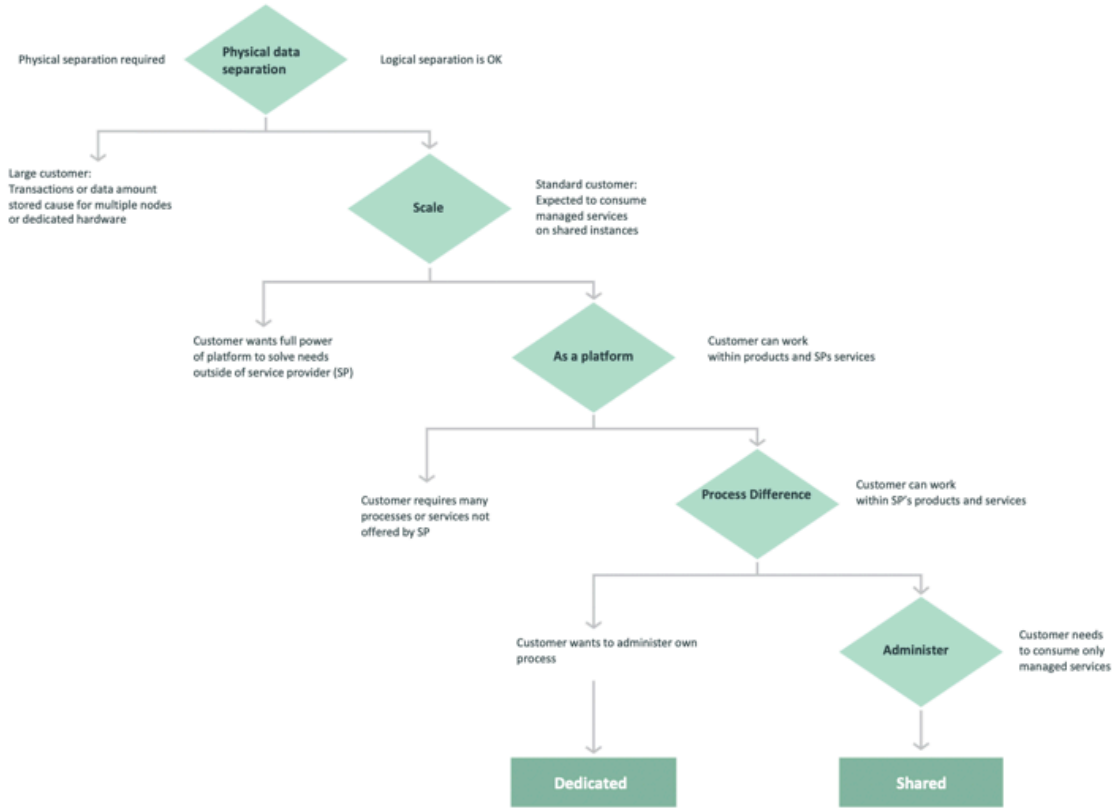
Atributos

- As instâncias dedicadas exigem que você tenha uma administração separada e equipes dedicadas. Você precisa de várias licenças para os administradores e desenvolvedores que fazem login em várias instâncias.
- Cada instância tem um número finito de solicitantes e executantes. Ao obter um novo cliente, você deve adquirir uma instância que se baseie no tamanho e na escala da empresa do cliente.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Instância compartilhada

Instância dedicada versus compartilhada



Comparação da arquitetura de referência do SP

Standalone (SA)		Multi-Tenant (MT)		Hybrid (MT+SA)		SIAM (Multi-Vendor)	
Platform as a Service	Enterprise scale	Processes simplified	Cost reduction	Managed Services (MT)	Custom Services (SA)	Service Integration	Multi-supplier governance
Customer wants full power of platform to Solve own needs outside those offered by SP.	Large customer: Transactions or data amount stored cause for multiple nodes or dedicated hardware.	Global governance & admin for business use case & process can be developed & maintained on the instance. Best when used w/ minor-to-moderate process differences among customers or sub-entities.	Lower administration, transaction, & onboarding costs, & ongoing operational costs for resources & licensing. Faster onboarding = more revenue.	Standardized re-usable services. procedures. processes, & resources delivered on a single ServiceNow instance to multiple Customers.	Services for sole use of customer, offerings specific to industry or vertical solutions, government, or regulatory requirements, applications that do not support Domain Separation.	Multiple best in class Service providers for individual services bringing together tooling, reporting, SLAs, strategy, & design for unified customer experience.	Unified governance across all providers to ensure organization requirements are met & that all providers cooperate on behalf of the customer.

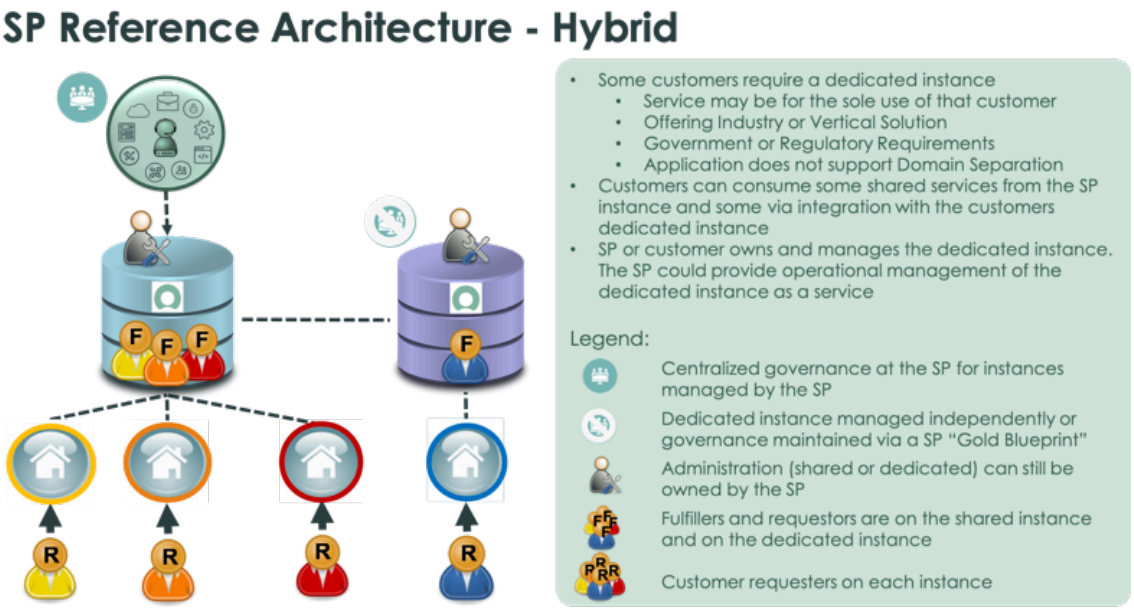
Arquitetura de referência do provedor de serviço para híbrido

Use a arquitetura de referência do provedor de serviço (SP) híbrido para obter uma solução personalizada. Os clientes precisam de uma instância dedicada para um serviço específico. Eles ainda podem usar a instância SP compartilhada para outros serviços, mas isso requer a integração de cada instância.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Arquitetura híbrida

O cliente pode ser responsável por entregar este serviço adicional diretamente. Você precisa criar uma solução híbrida de vários atributos para o cliente oferecer.



Atributos

- Você pode compartilhar e aproveitar a administração da instância. Isso significa que não há despesa e que você pode otimizar licenças.
- Se houver uma nova instância para um ambiente descentralizado, a equipe do programa será responsável e financiada adequadamente como usuários administradores dedicados para essa instância. Em um ambiente centralizado em que todas as instâncias derivam de um plano gráfico, você precisa de licenças de administração duplicadas.
- Você não atribui executantes a um domínio. Em vez disso, você os compartilha entre domínios.
- Se um cliente estiver compartilhando um ambiente compartilhado e um ambiente dedicado, ele precisará de um executante em ambos os ambientes. Isso significa mais trabalho para cada equipe porque os processos de instâncias compartilhadas e dedicadas exigem trabalho diferente para cada instância.
- O número de usuários na instância pode mudar quando você obtém um novo cliente. Um novo cliente pode resultar em dezenas ou até mesmo centenas de milhares de novos usuários no sistema. O número total de usuários é virtualmente ilimitado em um ambiente compartilhado.
- Cada instância tem um número finito de solicitantes e executantes. Ao obter um novo cliente, você deve adquirir uma instância que se baseie no tamanho e na escala da empresa do cliente.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Comparação da arquitetura de referência do SP

Standalone (SA)		Multi-Tenant (MT)		Hybrid (MT+SA)		SIAM (Multi-Vendor)	
Platform as a Service	Enterprise scale	Processes simplified	Cost reduction	Managed Services (MT)	Custom Services (SA)	Service Integration	Multi-supplier governance
Customer wants full power of platform to Solve own needs outside those offered by SP.	Large customer: Transactions or data amount stored cause for multiple nodes or dedicated hardware.	Global governance & admin for business use case & process can be developed & maintained on the instance. Best when used w/ minor-to-moderate process differences among customers or sub-entities.	Lower administration, transaction, & onboarding costs, & ongoing operational costs for resources & licensing. Faster onboarding = more revenue.	Standardized re-usable services. procedures. processes, & resources delivered on a single ServiceNow instance to multiple Customers.	Services for sole use of customer, offerings specific to industry or vertical solutions, government, or regulatory requirements, applications that do not support Domain Separation.	Multiple best in class Service providers for individual services bringing together tooling, reporting, SLAs, strategy, & design for unified customer experience.	Unified governance across all providers to ensure organization requirements are met & that all providers cooperate on behalf of the customer.

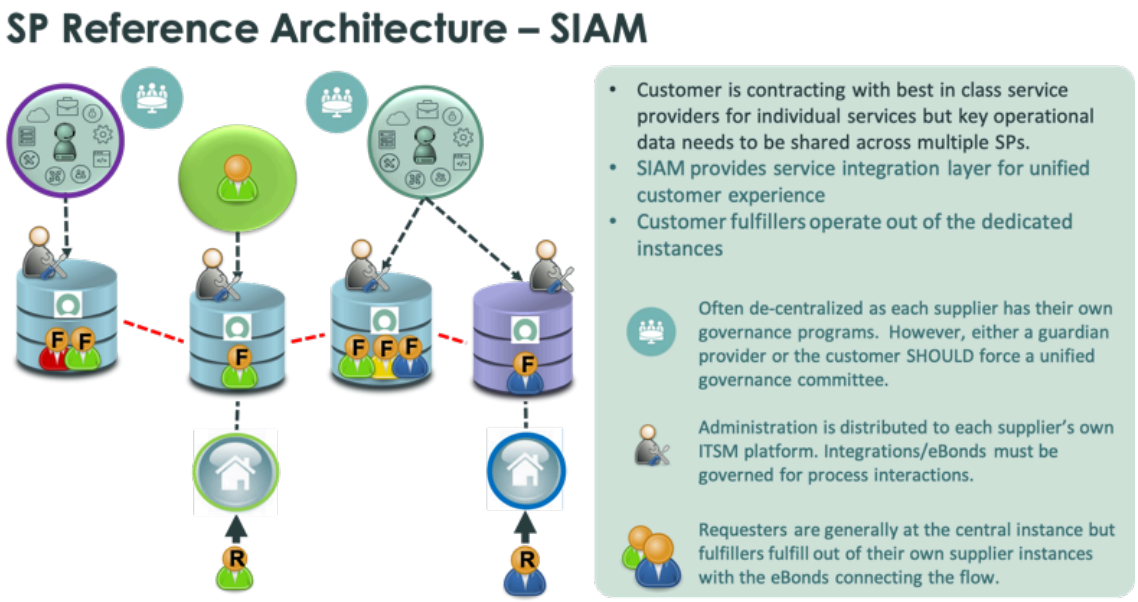
Arquitetura de referência do provedor de serviço para Gestão e integração de serviço (GIS)

A arquitetura Gestão e integração de serviço GIS (Gestão e integração de serviços) para SP (service provider, provedor de serviço) integra serviços para uma experiência unificada do cliente.

Atributos da arquitetura GIS

- Serviços de SP para acesso de clientes em um portal dedicado ou compartilhado com a instância compartilhada do SP.
- Os SPs usam instâncias compartilhadas da ServiceNow para gerenciar sua entrega de serviço.

Resumo da arquitetura GIS



© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Comparação da arquitetura de referência do SP

Standalone (SA)		Multi-Tenant (MT)		Hybrid (MT+SA)		SIAM (Multi-Vendor)	
Platform as a Service	Enterprise scale	Processes simplified	Cost reduction	Managed Services (MT)	Custom Services (SA)	Service Integration	Multi-supplier governance
Customer wants full power of platform to Solve own needs outside those offered by SP.	Large customer: Transactions or data amount stored cause for multiple nodes or dedicated hardware.	Global governance & admin for business use case & process can be developed & maintained on the instance. Best when used w/ minor-to-moderate process differences among customers or sub-entities.	Lower administration, transaction, & onboarding costs, & ongoing operational costs for resources & licensing. Faster onboarding = more revenue.	Standardized re-usable services. procedures. processes, & resources delivered on a single ServiceNow instance to multiple Customers.	Services for sole use of customer, offerings specific to industry or vertical solutions, government, or regulatory requirements, applications that do not support Domain Separation.	Multiple best in class Service providers for individual services bringing together tooling, reporting, SLAs, strategy, & design for unified customer experience.	Unified governance across all providers to ensure organization requirements are met & that all providers cooperate on behalf of the customer.

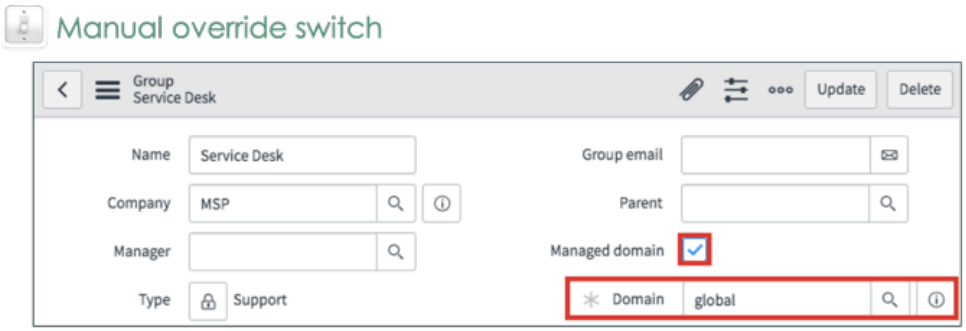
Termos do Domain Separation

Com uma instância ServiceNow, você pode melhorar a eficiência, adicionar mais segurança e aumentar o desempenho das organizações do cliente. É útil entender alguns dos termos mais comuns ao criar as configurações.

Domínio gerenciado

Em um domínio gerenciado, o campo **Domínio gerenciado** permite que os administradores de domínio selecionem manualmente um domínio para o usuário, grupo, departamento, local ou registro de IC, em vez de usar o domínio que é atribuído automaticamente a partir do registro da empresa.

Se você quiser mudar essas propriedades, poderá substituí-las para personalizar ainda mais as funções das aplicações em cada um dos



- Common Use Cases
  - Set admins to 'global'
  - Set support groups to 'global'
- UI Policy shows Domain when Managed domain = true

Tables with managed_domain	
User [sys_user]	Location [cmn_location]
Group [sys_user_group]	Department [cmn_department]
Configuration Item [cmdb_ci]	

domínios.

Tabelas de processo

Em tabelas de processo, se você vir um valor no campo **Substituições [sys_overrides]**, existe um registro de substituição de processo. Isso significa que a administração delegada, que é como os administradores podem definir políticas específicas de domínio, está em vigor. Os

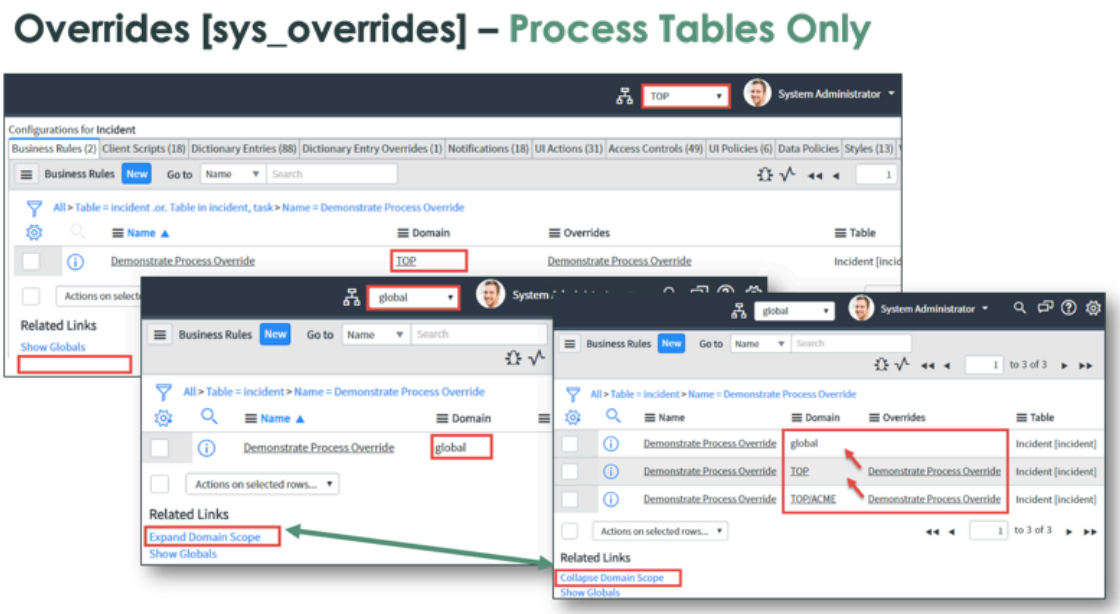
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

administradores no domínio global podem usar o link relacionado **Expandir/recolher escopo do domínio** para ver registros de substituição.

Nota: Os relatórios são separados em domínios e contêm um campo **Substituições**. Para exibir todos os relatórios do domínio global, use o link relacionado **Expandir escopo do domínio**.

Ao exibir tabelas de processo de um domínio, você vê somente os registros de processo relevantes para o domínio selecionado. Quando você exibe uma tabela de processo do domínio global, o link relacionado **Expandir escopo do domínio** é exibido para permitir que você veja todos os registros de processo, incluindo as substituições. Para exibir somente os registros de processo relevantes para global novamente, use o link relacionado **Recolher escopo do domínio**.

O recurso de escopo do domínio é usado somente para tabelas de processo e faz com que a visibilidade dos dados na tabela mude na direção oposta. Por exemplo, um registro no domínio primário pode ser visto no secundário, mas um primário não pode ver um registro secundário. Isso permite que o processo flua para os domínios secundários.



Tipos de domínios

Diferentes tipos de domínios podem ajudar a organizar os processos e dados e como eles funcionam na aplicação ou recurso.

Domínio do cliente

No domínio do cliente está a interface do usuário, bem como o processo que controla como os dados são usados.

O domínio ACME na imagem a seguir é um domínio de cliente.

Domínio do processo

Você cria processos para como os dados são usados e o que eles fazem no domínio. Esses processos devem ter estes atributos:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Processos específicos e configurações de IU para um conjunto de domínios
- Não há dados principais de qualquer tipo (como dados específicos do usuário).
- O domínio TOP na imagem a seguir é um domínio de processo.

Domínio de Dados

O domínio de dados contém dados relevantes para vários clientes. Esses dados podem ser compartilhados sem compartilhar os domínios reais do cliente. Cada cliente tem seu próprio domínio de dados e pode acessá-lo.

Nota:

Este tipo de domínio não é comum e pode causar problemas de desempenho se usado em excesso. Consulte um arquiteto de SP antes do uso.

Exemplo: o domínio pode conter tarefas com as quais a ACME, a Cisco e o SP precisam interagir.

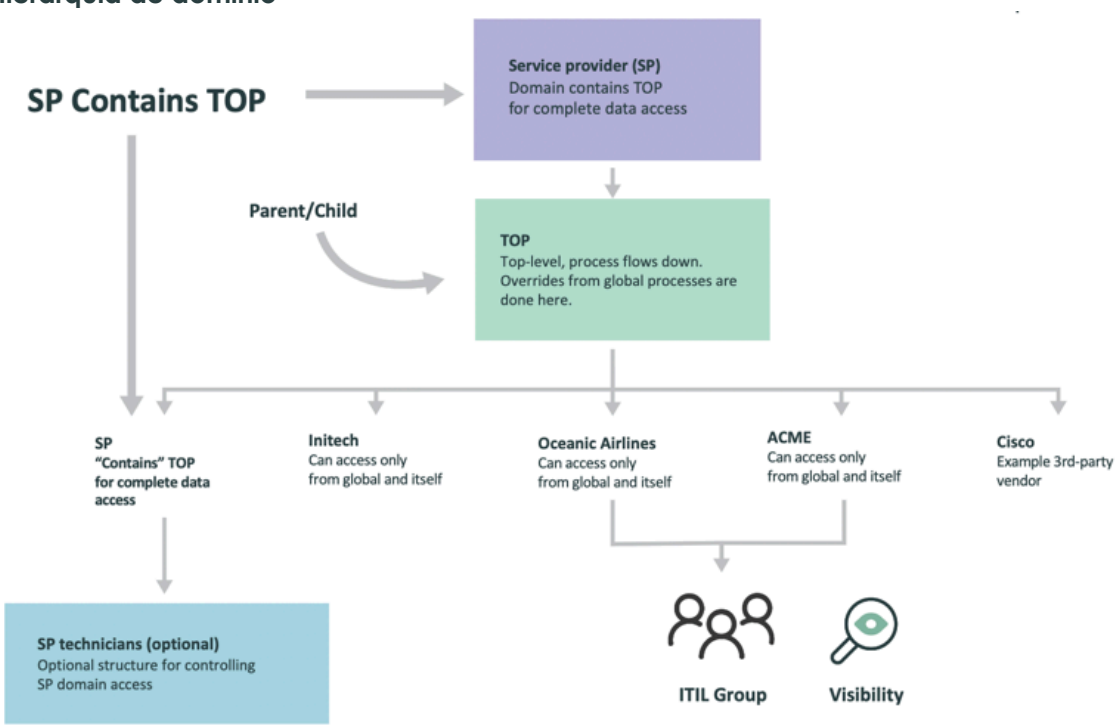
O domínio-padrão na imagem a seguir é um domínio de dados.

Dados do usuário

Os dados de registro do usuário nunca pertencem ao domínio global ou a qualquer um dos domínios de processo. Os usuários são criados principalmente em domínios de cliente e às vezes podem ser criados em domínios de dados.

As contas de administrador são especiais, pois não devem ser usadas como usuários diários da instância e devem estar no domínio global para facilitar as funções administrativas.

Hierarquia de domínio



Listas, administrador, processo global

Listas

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

No domínio global, se você clicar com o botão direito do mouse em qualquer rótulo de campo de opção, selecionar **Configurar opções**e adicionar uma nova opção, a opção será enviada por push automaticamente para todas as listas específicas de domínio desse campo. Se a nova opção estiver marcada como **Selecionada**, ela será adicionada como ativa. Se a nova opção estiver marcada como **Disponível**, ela será adicionada como inativa.

Administração de Instância

Os administradores do proprietário da instância devem lidar com toda a criação, modificação e manutenção de processos normais em uma instância separada por domínio. Os gerentes de domínio individuais podem manter algumas partes de processos orientados por dados. Os tipos de gerenciadores de domínio mantêm a administração do usuário, oferecem suporte a associações de grupo e locais ou gerenciam aplicações projetadas com a administração de locatários em mente.

Processo/parâmetros globais

Você pode criar e manter o processo que afeta o domínio global, bem como definir os parâmetros. Essas propriedades são comuns a todos os usuários de uma instância separada por domínio.

Exemplos: propriedades do sistema, substituições de dicionário, `sys_documentation` (rótulos de campo), o modelo de dados (classes, tipos de IC e assim por diante), tabelas e campos `[sys_dictionary]` (o acesso pode ser restrito), indexação (índices de texto, bem como banco de dados), ACLs, saídas de instalação, ações de entrada, páginas públicas e interceptadores.

Como separar por domínio uma tabela personalizada

Pode ser necessário criar tabelas personalizadas em domínios separados. Este tópico cobre o procedimento e o conceito por trás de uma tabela personalizada de separação de domínio.

1. Criação de um campo sys_domain

Nota: Se uma tabela do sistema ou uma tabela não tiver sido separada por domínio pelo plug-in Separação de domínios, é melhor não a separar por domínio.

Use esses pontos como diretriz para criar um campo sys_domain.

- Crie um novo campo como um tipo *domain_id*.
  - Nome da coluna: sys_domain
  - Outros atributos: definidos automaticamente
- O Sys_domain_path é criado automaticamente.

O nome da coluna **sys_domain** está reservado no Now Platform, o que significa que o sistema o reconhece e aplica automaticamente o tipo de campo e os atributos apropriados para você. Esta configuração automática também cria um campo **sys_domain_path** correspondente.

- Defina o nome da coluna como `sys_domain` em vez de usar o rótulo.
- A Separação de domínios não é apropriado para todas as tabelas. Em geral, se uma tabela fizer parte da instância base e essa tabela não tiver um campo **sys_domain**, você deverá deixá-la assim.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Um campo **sys_domain** é criado automaticamente quando você cria um campo do tipo domain_id com o nome "sys_domain".

2. Como adicionar uma regra de negócio para definir o domínio

Sem regras de negócio

O domínio é definido como o domínio atual do usuário que cria o registro.

Com regras de negócio

O domínio é atribuído usando lógica de script, normalmente com base no campo Empresa.

Além de um `campo sys_domain`, as tabelas personalizadas precisam de uma regra de negócios semelhante a **Domínio - Definir domínio - Tarefa**para definir o valor do campo de domínio. Além disso, você precisará de **Domínio - Padrão - Tarefa**, que move registros sem um domínio para o domínio-padrão se a primeira regra não conseguir atribuir um domínio.

Na tabela de tarefas, revise as regras de negócio do Domínio. Preste atenção especial ao campo Pedido. A prioridade de execução é fornecida pelo campo Pedido de baixo para alto.

A primeira regra executada, **Domínio - Definir domínio - Tarefa**, tentará definir o domínio do registro com base no domínio da empresa do registro.

Se a primeira regra não encontrar um domínio apropriado, a segunda regra, **Domínio - Padrão - Tarefa**, será executada. Esta regra define o domínio do registro como o domínio-padrão.

Por fim, se o domínio de um registro de tarefa mudar, a regra de negócio **Domínio - Domínio em cascata - Tarefa** mudará o domínio em todos os registros relacionados à tarefa, como fluxos de trabalho, métricas, ANSs e anexos.

3. Como adicionar uma regra de negócio se a Etapa 2 falhar

Se a regra de negócios inicial não definir um domínio e o domínio ainda estiver vazio ou global, uma segunda regra de negócio será executada. Esta regra examina o campo `task_for` que se baseia no campo solicitante ou `solicitado`. Esta regra verifica se você pode definir o domínio do registro com base no domínio do usuário. Caso contrário, esta regra define o domínio do registro como o domínio-padrão.

A seguir está um script de exemplo para a regra de negócio:

```
/* essentially
If (task_for is set)
  set the domain to the user's domain
ELSE
  set the domain to the default domain
*/
```

4. Domínio - domínio em cascata - tarefa

As tarefas podem ter muitas tabelas relacionadas que funcionam juntas para objetivos de negócios. Esses registros relacionados incluem fluxo de trabalho, ANS, aprovações, anexos e e-mail. Se o domínio de uma tarefa mudar, o domínio dos registros relacionados também deverá mudar, para que eles permaneçam visíveis para os usuários no novo domínio.

Esta Regra em cascata é normalmente acionada quando você limpa registros do domínio-padrão.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Os registros relacionados a um Domínio em cascata contidos no script são mostrados de forma semelhante ao exemplo:

```
/*
* Keep domains in sync w/related records for:
* workflow context
* workflow history
* approver tables and related workflows
* attachments
* emails
*/
```

Como personalizar propriedades e temas de domínio

Você pode personalizar as propriedades e os temas da empresa de seus clientes nos domínios que configurou. A personalização faz com que as instâncias se encaixem na aparência geral das empresas.

Como personalizar temas e logotipos da empresa

No registro da empresa, você pode personalizar temas de design e logotipos específicos para cada empresa.

Como personalizar o domínio

Por padrão, quando você tem o plug-in do provedor de serviço instalado, as regras de negócio padrão contidas nas tabelas principais fazem com que o domínio do registro seja definido como o domínio da empresa associada ao registro. A empresa pode controlar tabelas como Tarefa, Usuário, Grupo, Local, Departamento e assim por diante.

Com todas essas tabelas, exceto a tabela de Tarefas, você pode substituir o domínio em que um registro é criado. Isso fornece mais opções de personalização.

Como gerenciar o Domain Separation para usos específicos

Você pode configurar domínios separados para notificações por e-mail e personalizar as propriedades de catálogo, tabelas, usuários, grupos e exibições. Isso permite que você forneça um comportamento mais específico em cada domínio, dando aos clientes mais flexibilidade.

E-mails

Você pode usar domínios separados para notificações por e-mail e substituições. Ao usar domínios separados para notificações, você pode fazer uma substituição com base no domínio apenas do registro anexado, não no domínio inteiro do usuário.

Catálogo de serviços

O Catálogo de serviços agora está separado por domínio para que seus clientes possam ver e acessar o catálogo. Os itens são processados como condições OR quando vários itens são usados. Os provedores de serviço devem administrar as categorias e os itens para que eles se encaixem especificamente em seus próprios critérios.

Usuários e grupos

Use somente contas de administrador no domínio global porque os administradores precisam de acesso a todos os domínios. Faça todos os testes de aplicação de um domínio real, não no domínio global. As substituições não são processadas corretamente no domínio

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

global. Os administradores também devem receber contas de usuário na produção, se quiserem usar a aplicação.

Trabalho com campos

Há vários pontos a serem considerados ao trabalhar com campos. Preste muita atenção a esses campos porque eles podem ter muitas variações que afetam as configurações.

Listas

Há listas pessoais, globais e de domínio, bem como várias exibições de cada um.

Formulários

Há listas globais e de domínio, bem como várias exibições de cada um.

Um banco de dados

Todos os campos que você cria existem para todos os usuários, em um banco de dados. Considere o impacto global antes de criar um.

Nota: Os scripts de ACL não podem impedir que um campo seja exibido em uma lista porque eles não são executados. Você pode adicionar uma ACL de LEITURA para ocultar um campo dos usuários se a ACL for baseada somente em função.

Criação de tabelas

Ao criar uma tabela, você deve adicionar um campo `sys_domain` ou `sys_overrides`. Qualquer tabela que contenha dados que os usuários da instância devem acessar precisa do campo `sys_domain`. Tabelas que estendem ou oferecem suporte a processos e que precisam fluir para domínios secundários também precisam do campo `sys_domain`.

Configuração do Domain Separation com o seletor de domínio

Use o seletor de domínio com inteligência e lembre-se da abordagem 80/15/5 para não personalizar muito e afetar o desempenho da instância.

Verificação do domínio antes de fazer mudanças

O seletor de domínio reúne todos os domínios em uma lista para você escolher.

Se a sessão expirar e mesmo se você não for desconectado, a sessão retornará ao domínio no registro do usuário. Você também perde funções elevadas ao mesmo tempo. Nesse caso, o seletor de domínio ainda pode mostrar o último domínio selecionado se o quadro superior da lista não tiver sido recarregado. Por esse motivo, você deve recarregar sua lista completamente se tiver ficado ausente da instância por algum tempo.

Configuração no domínio TOP ou no domínio global

O Domain Separation funciona melhor quando você fornece serviços aos clientes que são na maioria-padrão em sua configuração e definição de usuário e grupo. Quanto mais você personaliza e cria soluções "pontuais", mais uma margem de erro é criada. Quando você cria seus processos e lógica de negócios, todas as variações devem estar em propriedades que funcionam automaticamente para cada cliente. Embora os processos ainda possam ser ajustados conforme necessário, tome muito cuidado ao decidir quando e em que grau criar uma configuração exclusiva para um único cliente.

Você precisa usar uma abordagem “80-15-5” na configuração dos domínios para evitar uma margem muito grande para personalização e, portanto, erros.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Abordagem recomendada para configuração:
  - **Padrão** de **80%** ou mais
  - **Paramétrico** de **15%** ou mais
  - **Configuração** inferior a **5%**
- Determine se uma mudança sugerida deve ser uma propriedade global ou configurável.
- Não exagere, adicionando mais e mais personalizações que precisam ser gerenciadas. Em vez disso, faça o seguinte:
  - Comece com os recursos do sistema de base e verifique as lacunas antes de fazer mudanças.
  - Procure soluções sem código.
  - Use scripts do lado do servidor, crie APIs modulares e crie propriedades separadas por domínio.
  - Se você precisar usar Client scripts, use somente APIs ServiceNow. Limite as chamadas "síncronas" (aquelas que vão e voltam do cliente para o servidor, também chamadas de AJAX).
  - Grave todos os scripts de forma lógica para mantê-los simples e eficazes. Imponha revisões de pares de mudanças de código e certifique-se de que todos estejam seguindo o Práticas recomendadas do Domain Separation para provedores de serviço nesta seção.

Considerações de desempenho do Domain Separation

Ao configurar o Domain Separation na aplicação e serviços, certifique-se de considerar o número e as propriedades dos domínios que você cria. Muitos domínios com muitas propriedades podem afetar o desempenho da instância.

Limitação de domínios com muitas propriedades

Você pode criar quantos domínios forem necessários, mas certifique-se de não criar domínios desnecessários na instância. Colocar muitos domínios na instância com muitas propriedades pode afetar o desempenho da instância.

O número de domínios não é o que afeta o desempenho, mas o que há neles. Muitas propriedades podem tornar o seletor de domíniomais lento, o que torna mais lenta a experiência geral do usuário dos clientes. Se você estiver carregando o seletor de domínio e já tiver um grande número de domínios com muitas propriedades, o seletor de domínio precisará carregar todos os domínios antes de fornecer o controle na sessão. Esse processo pode levar a uma indisponibilidade na qual você não pode acessar nada na instância até que o seletor de domínio seja concluído. Antes de criar novos domínios, navegue até a hierarquia de domínio em **Administrador do domínio** > **Mapa de domínio** e certifique se você realmente precisa criar um novo domínio ou se uma hierarquia de domínio existente pode funcionar.

Uso do seletor de domínio IU principal

O seletor de referência de domínio está disponível em IU principal. Com o seletor de referência, você não carrega todos os domínios de uma vez, mas o domínio é pesquisado conforme você começa a inserir o nome do seu domínio no seletor de domínio.

Habilite o seletor de referência de domínio em IU principal seguindo estas etapas:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

1. No navegador de aplicações, insira `sys_properties.list`.
2. Defina a propriedade *`glide.ui.domain_reference_picker.enabled`* como verdadeira.
3. Atualize o navegador.

Nota: Não carregue um grande número de domínios (mais de 30) por meio de integração ou Conjuntos para importação sem fazer alguns testes antes ou você pode desativar a instância.

Configuração de hierarquias do domínio

Você pode evitar lentidões e impactos no desempenho na instância, sabendo como as hierarquias do domínio funcionam e configurando-as corretamente.

Com base na hierarquia de domínio, os usuários têm acesso aos dados em seu domínio inicial e a todos os domínios secundários. O processo flui para baixo para os domínios secundários e os dados sobem.

Faça mudanças na hierarquia de domínio existente somente quando necessário. Quando você atualiza o primário de um domínio, o sistema restabelece o domínio primário com todos os seus domínios secundários que mudam a hierarquia do domínio. Quando a hierarquia de domínio é atualizada, o sistema aciona uma atualização em cascata em todas as tabelas relacionadas a domínios para os registros criados nesse domínio. Como resultado, um grande número de tabelas de suporte também precisa ser atualizado.

Pelas mesmas razões, mesmo que você precise mudar a hierarquia de domínio, nunca faça uma atualização em massa. Imagine o número de consultas que o sistema precisa executar para mudar a hierarquia do domínio. Sempre faça uma atualização em pequenos lotes. Antes de iniciar o próximo lote de atualizações, verifique se os registros de Solicitação de trabalho de domínio (DWR - Domain Work Request) foram processados. As DWRs são relatórios que exibem se há erros após a mudança da hierarquia de domínio.

Rastreamento de registros DWR

Na tabela syslog_domain, procure uma entrada de informações na coluna Mensagem da **execução DWR concluída.** para confirmar que a DWR foi concluída.

Como verificar se há erros e avisos nos logs do domínio

Verifique os logs de domínio para encontrar erros ou avisos nos processos de caminho de domínio e configurações de hierarquia.

Você pode encontrar os logs de domínio na tabela Logs de domínio [syslog_domain]. Quando a hierarquia do domínio é atualizada, o sistema aciona um trabalho agendado para recalcular os caminhos do domínio. A tabela logs de domínio captura os resultados.

Procure erros e avisos nessa tabela. Depois de revisar essa tabela, você precisa resolver esses erros e executar o validador de caminho de domínio novamente.

Neste exemplo de log, o sistema detectou dez registros órfãos na tabela sys_ui_list. Os erros nesses registros devem ser corrigidos para que o caminho de domínio seja executado com êxito.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Error	10 records detected in 'sys_ui_list' that are not in any existing domain and Domain Paths. Fix the domain value in these records & run validator again.	com.glide.domain.validator
Error	10 records detected in 'sys_ui_list' that are not in any existing domain and Domain Paths. Fix the domain value in these records & run validator again. Entries causing the error are as follows:sys_id:1d13ae40470002007f47563dbb9a7170, sys_domain:11722b01473231007f47563dbb9a7154 sys_id:22e34b23470002007f47563dbb9a718c, sys_domain:11722b01473231007f47563dbb9a7154 sys_id:4c85fa809f233100fc6cd4b4232e706b, sys_domain:11722b01473231007f47563dbb9a7154 sys_id:94648b23470002007f47563dbb9a711b, sys_domain:11722b01473231007f47563dbb9a7154 sys_id:a0844b23470002007f47563dbb9a71ef, sys_domain:11722b01473231007f47563dbb9a7154 sys_id:a95ff2c09f233100fc6cd4b4232e7096, sys_domain:11722b01473231007f47563dbb9a7154 sys_id:bd25f4719f233100fc6cd4b4232e70da, sys_domain:11722b01473231007f47563dbb9a7154 sys_id:c1263e809f233100fc6cd4b4232e70f6, sys_domain:11722b01473231007f47563dbb9a7154 sys_id:d8a72c45475002007f47563dbb9a71bb, sys_domain:11722b01473231007f47563dbb9a7154 sys_id:e4c3ce39eb10020045e1a5115206fea0, sys_domain:60e014f69f013100fbf01f80a57fcf00	com.glide.domain.validator

Para saber mais sobre erros de Domain Separation, consulte Solução de problemas de erros da separação de domínios.

Importância do domínio-padrão

Organizar seus domínios é uma parte crucial do processo do Domain Separation. Se você não definir um domínio-padrão, novas tarefas e registros de usuário serão enviados para o domínio global. Qualquer um pode ver os registros no domínio global, o que significa que os dados podem ser vistos quando não deveriam.

Quando você define o domínio-padrão, seus registros não ficam visíveis para nenhum usuário que não seja um administrador.

Nota: O acesso-padrão pode ser alterado concedendo aos usuários visibilidade para o domínio-padrão ou o domínio primário.

Você sempre deve definir um domínio-padrão para os registros de domínio na instância. O domínio-padrão é onde o sistema atribui automaticamente a tarefa e os registros de usuário que ainda não foram atribuídos a um domínio.

Ao criar um domínio-padrão na tela Administração de domínio, adicione o nome Padrão no campo **Nome** para diferenciá-lo de outros domínios. Marque a caixa de seleção **Padrão** do registro.

Mantenha regularmente os registros criados no domínio-padrão e mova-os para os domínios corretos. Se os registros aparecem com frequência no domínio-padrão, talvez seja necessário investigar o motivo. O ideal é que você verifique se todos os registros foram criados nos domínios apropriados (não nos domínios globais ou padrão).

Consultas "contém" e acesso ao domínio

Use uma consulta "contém" somente em casos especiais, como quando os usuários ou grupos precisam ver dados de um domínio ao qual eles não têm acesso, mas você não deve mover esses usuários para um domínio. Criar domínio "contém" e acesso de usuário ou grupo para um domínio deve ser uma exceção, somente quando absolutamente necessário.

"Contém" é um relacionamento de domínio para domínio que é muitos para muitos e não tem efeito no fluxo do processo. Se você criar um grande número de relacionamentos de domínio "contém" ou fornecer acesso amplo, gerará consultas com muitas condições OR. As condições OR são lentas e afetam o desempenho da instância. Em vez de usar muitos relacionamentos "contém", configure a hierarquia de domínio da seguinte forma:

Consulta de amostra

```
SELECT ... FROM task task0 ignore index(number) WHERE task0.`sys_class_name`
= 'incident' AND (task0.`sys_domain_path` = '/' OR task0.`sys_domain_path` LI
KE '!!$/!!(/%' OR task0.`sys_domain_path` LIKE '!!$/!!$/!!&/%') ORDER BY task
0.`number` DESC limit 0,20
```

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de mover usuários para um domínio, verifique se eles realmente devem ter acesso a esse domínio. Considere os benefícios e as limitações. A consulta acima é apenas para um relacionamento contém. Se você tiver um domínio que contém outro domínio e esse domínio for o primário de vários outros domínios, terá muito mais condições OR. Tenha cuidado ao criar um mapa de domínio para não afetar o desempenho da instância.

Método de consulta de caminhos do domínio

Você pode criar consultas eficazes com caminhos do domínio.

Use caminhos do domínio em vez do spool de domínio (`sys_domain`) ou da numeração de domínio. As consultas que usam caminhos do domínio são muito mais rápidas do que o spool ou a numeração.

Caminhos do domínio é o método de consulta padrão para instâncias que têm o Domain Separation habilitado.

Se você quiser verificar o método de consulta na instância, procure as seguintes propriedades do sistema no painel do administrador:

- *`If domain path is enabled`*: Na tabela Propriedades do sistema, você vê `glide.sys.domain.provider = domain_paths` e `glide.sys.domain.paths.installed = true`.
- *`If domain path is not enabled`*: Na tabela Propriedades do sistema, você vê `glide.sys.domain.provider != domain_paths,glide.sys.domain.paths.installed=false`

Depuração de consultas lentas e SQL

A depuração de SQL e consultas lentas pode ajudar a resolver problemas de lentidão em uma instância.

Ao depurar uma instância, você pode habilitar a depuração SQL para procurar consultas lentas ou procurar consultas lentas verificando a tabela Consultas lentas [sys_query_pattern] navegando até **Diagnóstico do sistema > Estatísticas > Consultas lentas**. Esta tabela armazena todas as consultas lentas na instância.

Ao pesquisar a tabela, procure consultas que contenham `domain_path` para determinar se as consultas lentas são devido ao caminho do domínio em sua instância.

Se você encontrar consultas lentas, tente analisar por que elas são lentas.

Motivos comuns para consultas lentas

- Uma consulta tem muitas condições OR (para obter mais informações, consulte Consultas "contém" e acesso ao domínio). Na hierarquia de domínio, coloque o usuário ou um domínio em um nível de hierarquia em que contém ou a visibilidade não são necessários.
- O método de consulta não é o método de consulta de caminho de domínio (para obter mais informações, consulte Método de consulta de caminhos do domínio): se você não estiver usando o método de consulta de caminho de domínio, entre em contato com Suporte e atendimento ao cliente.
- Uma consulta precisa de um banco de dados para ser indexado para que você possa ver o que há no banco de dados rapidamente. Se você puder identificar a consulta lenta, execute o "plano de explicação" para ver se há opções de indexação disponíveis. O "plano de explicação" é uma função do SQL que mostra a consulta e o que está acontecendo com ela.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Regras de negócio Antes da consulta

Você pode usar uma regra de negócio Antes da consulta para ajudar a oferecer suporte à segregação de dados em uma instância. Aplicações ServiceNow que oferecem suporte à Separação de domínios podem oferecer suporte à separação de dados e roteamento de dados, ter separação de lógica de negócios avançada ou oferecer suporte à administração de nível de locatário (cliente) da aplicação.

Uma regra de negócio Antes da consulta é um código suplementar usado para oferecer suporte à segregação de dados em ambientes separados por domínio.

Aviso: Não use a regra de negócio Antes da consulta no lugar do plug-in Separação de domínios. Esta regra de negócio não impede o vazamento de dados com a mesma segurança que o plug-in.

Uso da regra de negócio Antes da consulta para segregação de dados

Você pode usar a regra de negócio Antes da consulta com a segregação de dados nas seguintes situações:

- Quando a Separação de domínios não é compatível com uma aplicação ServiceNow e você deve conceder ou restringir o acesso à tabela ou linha a um ou mais clientes não internos fora da organização do provedor de serviço.

  Nota: Antes de começar a desenvolver, entre em contato com o ServiceNow Suporte ao cliente sobre o roadmap da aplicação para esse produto; melhorias no suporte ao domínio podem ser planejadas para as próximas versões.

- Quando uma tabela é separada por domínio, mas o acesso a suas linhas deve ser concedido ou restrito com base em determinadas condições que se aplicam somente a um conjunto de domínios no sistema.

  Nota: Por exemplo, um cliente no domínio X tem vários fornecedores que oferecem suporte a esse domínio e esses fornecedores têm acesso para ver somente os registros atribuídos a eles.

Pontos a serem considerados antes de criar regras de negócio Antes da consulta

Você pode criar um script de regras de negócio Antes da consulta para impedir o acesso à tabela primária e secundária com base em uma combinação de informações do usuário, associações de grupo, empresas, funções ou condições de campo específicas do registro. As regras de negócio Antes da consulta são colocadas em domínios separados e criadas para serem aplicadas globalmente a uma ramificação específica de uma hierarquia de domínio.

- Onde for possível, crie regras de negócio Antes da consulta na parte mais baixa possível da hierarquia de domínio para que a regra seja executada somente para os usuários aos quais se aplica.
- Saiba que há cenários no sistema em que as regras de negócio podem não ser executadas ou em que uma interação acionada pelo usuário pode não acionar uma regra de negócio para ser executada. Por exemplo, uma regra de negócio não será executada quando você tiver mapas de transformação com regras de negócio Executar desativadas ou tiver scripts com o fluxo de trabalho desabilitado.
- Sempre preencha o campo de condição para especificar quando a regra será executada. Por exemplo, você pode especificar se a regra de negócio se aplica somente a determinados fornecedores em um domínio.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

> ⚠ **Aviso:** Ao projetar e codificar regras de negócio (especialmente regras de negócio de Consulta), limite as cláusulas OR e as pesquisas em campos não indexados. Muitas cláusulas OR e pesquisas em campos não indexados podem tornar as consultas lentas ou afetar o desempenho da instância.

- Use as regras de negócio Antes da consulta somente quando necessário. Muitas regras Antes da consulta podem afetar o desempenho da instância.

As regras de negócio Antes da consulta são executadas antes das listas de controle de acesso (ACLs) e têm um desempenho melhor em geral. Isso é verdadeiro especialmente quando você limita os resultados retornados aos usuários em ambientes de provedor de serviço (SP) que têm acesso a vários domínios no sistema.

> ℹ **Nota:** A filtragem de dados é transparente (ao contrário das ACLs) para os usuários que não veem a mensagem `de restrição de Segurança de dados….` ao interagir com dados.

Quando não usar as regras de negócio Antes da consulta e ACLs

Tenha cuidado ao usar regras de negócio Antes da consulta e ACLs para separar dados do cliente. Ao usar regras de negócio e ACLs, você cria personalizações que devem ser mantidas. As personalizações podem causar problemas de desempenho. As equipes de desenvolvimento devem criar processos para garantir que não violem o sistema.

A Separação de domínios fornece escalabilidade e governança com o método de consulta de caminho de domínio atual (v3), que é uma estrutura amplamente compatível. As equipes da Plataforma e do App ServiceNow são responsáveis pela manutenção da estrutura, aliviando o cliente.

Para empresas com muitos clientes em várias instâncias, o uso excessivo de consultas Antes e ACLs pode fazer com que as consultas de banco de dados não funcionem bem.

Como a Separação de domínios é habilitada

Você pode habilitar a Separação de domínios com um plug-in ServiceNow. Um gerente de produto, com o suporte de uma equipe de desenvolvimento, gerencia a funcionalidade. Aprimoramentos e correções para a funcionalidade da Separação de domínios estão incluídos nas versões ServiceNow. Os proprietários de instância podem consultar Suporte e atendimento ao cliente recursos, como Portal de serviços, em https://support.servicenow.com para obter assistência com a Separação de domínios.

Como evitar um caminho de domínio em scripts

Caminhos do domínio podem fazer com que os valores do script sejam alterados ou até mesmo interrompidos, portanto, não os use em scripts.

O script não deve depender do caminho de domínio porque se você mudar a hierarquia do domínio, o caminho de domínio será recalculado e seu valor será alterado. Quando isso acontece, os scripts são inúteis ou podem gerar erros ou ficarem inválidos. A melhor estratégia é não escrever seus scripts com base em caminhos do domínio.

Use o campo **sys_domain** nos scripts em vez de depender do caminho de domínio. Se você alterar a hierarquia de domínio, o caminho de domínio será recalculado e seu valor será alterado, o que pode fazer com que o scripts sejam inúteis, gerem erros ou fiquem inválidos. Procure regras de negócio do sistema de base, que usam o campo **sys_domain**, para obter algumas ideias antes de criar seus próprios scripts.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A plataforma ServiceNow não captura os valores de sys_domain_path em um conjunto de atualizações para evitar problemas com diferenças na hierarquia de domínio de cada instância. Portanto, você deve validar a hierarquia de domínio depois de importar um conjunto de atualizações para garantir que os valores de caminho de domínio para seus registros estejam corretos.

Para saber mais sobre o caminho de domínio, consulte Solicitação de separação de domínios e Central de Separação de domínios.

Atribuições de domínio

O modo como você atribui um domínio afeta o valor do campo sys_domain. As atribuições contêm designs e propriedades de negócios que afetam o funcionamento da aplicação em cada domínio.

Valor do campo sys_domain

O valor do campo **sys_domain** contém o domínio atribuído ao registro por qualquer um dos seguintes:

- Empresa à qual o usuário pertence
- Regra de negócio usada ao criar o registro
- Módulo usado ao criar o registro
- Modelo de formulário usado ao criar o registro
- Domínio do registro primário
- Domínio atribuído ao registro do usuário
- Domínio do usuário que o cria

Certifique-se de que as estratégias e designs de atribuição de domínio estejam bem documentadas e testadas para que você crie registros conforme essas estratégias e os designs sejam inseridos no domínio correto. Assim, você poderá ver as propriedades de cada domínio caso precise duplicá-las ou modificá-las.

Domain Separation e o plug-in Customer Service Management (CSM)

Para obter o melhor resultado, saiba como as propriedades no plug-in CSM funcionam. Quando o plug-in está habilitado, você pode ver o status dos registros nos domínios.

Os proprietários da instância devem entrar em contato com Suporte e atendimento ao cliente para habilitar a propriedade *csm_auto_account_domain_generation*.

Nota: Esta propriedade de sistema base está localizada na tabela de propriedades do sistema e está disponível depois que os plug-ins CSM são habilitados.

O que a propriedade faz

Sempre que uma nova conta na aplicação Atendimento ao cliente é criada, um domínio é criado e colocado sob o domínio TOP. Se o campo primário no formulário de conta estiver preenchido e um novo registro for inserido, ele criará essa conta como um subdomínio do primário.

O que acontece se esta propriedade não for verdadeira e o domínio estiver habilitado

Novos registros de conta em um ambiente separado por domínio são colocados automaticamente no domínio padrão.

Na barra de cabeçalho, você pode ver o status dos registros com o plug-in habilitado.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Suporte para Separação de domínios

Assistência adicional para a Separação de domínios

Visão geral de vídeo da Separação de domínios

Exploração, Aprendizado, Desenvolvimento

Práticas recomendadas

Dicas e truques para criar e desenvolver sua estrutura de domínio com inteligência

Conceitos para provedores de serviço

Conceitos que funcionam com a plataforma ServiceNow para ajudá-lo a resolver casos de uso comuns

Níveis de suporte por aplicação

Sua aplicação é compatível com a Separação de domínios? Consulte os níveis de suporte e os casos de uso.

Classes

- Para desenvolvedores: ServiceNow Separação de domínios do site do desenvolvedor
- Para provedores de serviço: Separação de domínios para provedores de serviço (login Now Learning necessário)

Pacote de Local de trabalho seguro e separação de domínio

ServiceNow As aplicações Local de trabalho seguro ajudam você a reabrir seus locais de trabalho e oferecem suporte à saúde e à segurança de seus funcionários após emergências e pandemias como a COVID-19. O pacote tem muitas aplicações para ajudar sua organização a mobilizar, recuperar e recriar.

Configuração e administração

- Upgrades
- Solicitação de separação de domínios
- Criação de um domínio

Solução de problemas

- Pesquise artigos de erros conhecidos no Portal de erros conhecidos
- ContatoSuporte e atendimento ao cliente
- Pergunte ou responda questões na comunidade

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

• Configuração que pode ser delegada a clientes internos ou externos		

Configuração e administração do Domain Separation

Configurar o Domain Separation envolve solicitar a ativação de um plug-in, definir opções e atribuir usuários e registros a domínios.

Faça o seguinte para configurar o Domain Separation:

1. Solicitação de separação de domínios
2. Criação de um domínio
3. Como adicionar um campo de domínio a uma tabela

Você também pode executar estas tarefas administrativas básicas em domínios:

- Como habilitar ou desabilitar um domínio
- Exibição de relacionamentos do domínio
- Expansão do escopo do domínio
- Criação de uma lista de seleção específica de domínio

Consulte Administração avançada do domain separation para obter uma lista de tarefas a serem executadas depois de configurar o Domain Separation e executar a administração básica.

Solicitação de separação de domínios

Todos os recursos de suporte de domínio são ativados com um plug-in chamado **Domain Support - Domain Extensions Installer**. Os administradores podem solicitar a ativação desse plug-in.

Antes de Iniciar

Para adquirir uma assinatura, entre em contato com o seu gerente de contas ServiceNow. O gerente de contas pode providenciar para que o *com.glide.domain.msp_extensions.installer* plug-in seja ativado nas instâncias de produção e desenvolvimento da sua organização, geralmente dentro de alguns dias.

Se você não tem um gerente de conta, se decidiu atrasar a ativação após a compra ou se quer avaliar o produto em fase de desenvolvimento sem custos, siga estas etapas.

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

Se o plug-in Domain Support - Domain Extensions Installer já estiver ativo, o conteúdo do plug-in Domain Support - Domain Extensions Installer não será instalado para evitar um possível conflito com uma implementação existente.

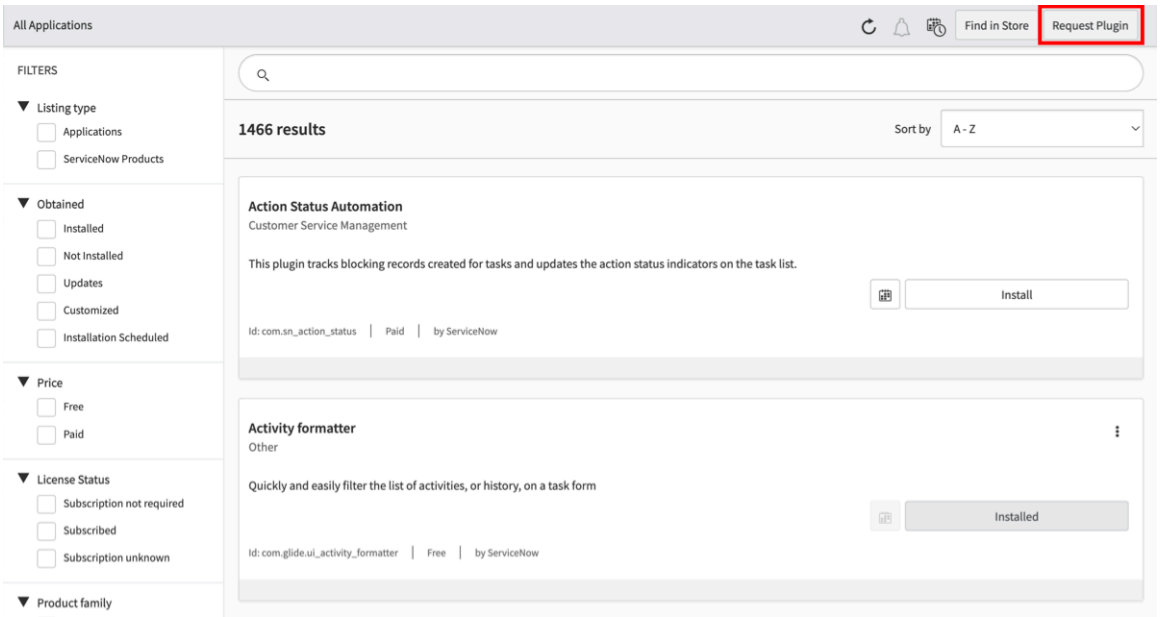
O Domain Separation substitui a Separação de empresa. A partir da versão Helsinki, o plug-in Company Separation não pode mais ser ativado. No entanto, se a separação de empresa já estiver ativa quando você ativar o Domain Separation, os dois plug-ins estarão ativos ao mesmo tempo. Você pode controlar o status de ativação de separação da empresa com a propriedade *glide.db.separation.field*.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

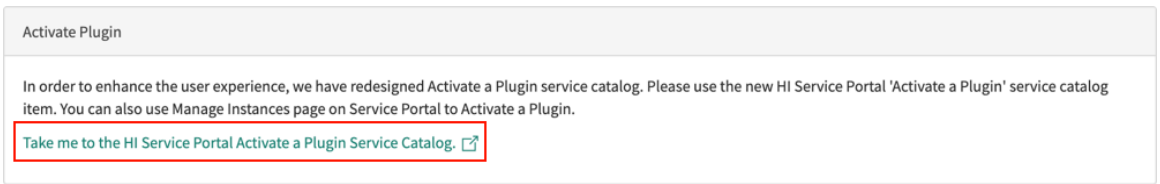
Nota: Caminhos de domínio são usados para todos os clientes na versão Helsinki em diante. A numeração de domínio não é mais usada. Suporte e atendimento ao cliente pode ajudar no upgrade.

Procedimento

1. Navegue até **Todas** > **Aplicações do sistema** > **Todas os aplicações disponíveis** > **Todas**.
2. Na página Todas as Aplicações, selecione **Solicitar plug-in** para abrir o formulário **Ativar plug-in** em Now Support.



3. No Now Support, selecione o link para acessar o Now Support Portal de serviços Catálogo de serviços.



4. Selecione sua instância.
5. Selecione **Ações > Ativar plug-in**.
6. No formulário **Ativar plug-in**, forneça as seguintes informações.

Formulário Ativar plug-in

Campo	Descrição
Qual é a sua instância de destino	Instância na qual o plug-in será ativado.
Qual plug-in você deseja ativar	Nome do plug-in a ser ativado.

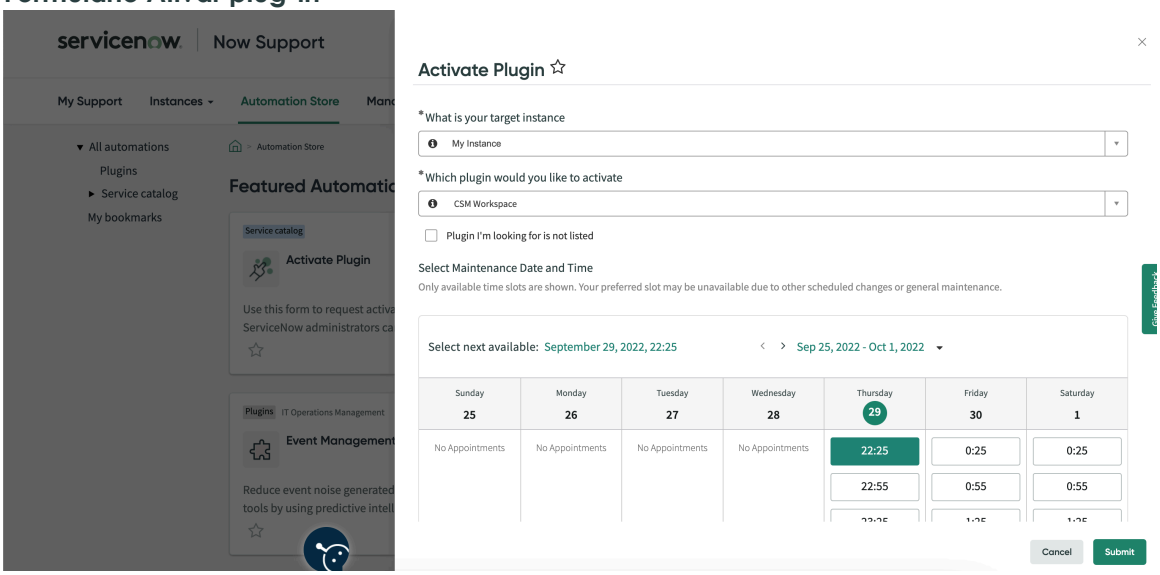
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: Se o sistema não listar o plug-in desejado ou se você estiver ativando o plug-in em uma instância do OEM ou no local, marque a caixa de seleção O **plug-in que estou procurando não está listado** e insira o nome do plug-in.
Selecionar data e hora de manutenção	A data e a hora para ativar o plug-in. **Nota:** Os plug-ins são ativados em dois lotes, uma pela manhã e outra à noite, em todos os dias úteis no fuso horário do Pacífico dos EUA. Se o plug-in deve ser ativado em um momento específico, insira a solicitação no campo **Motivo/ Comentários**.

Example

Por exemplo, consulte o formulário a seguir para ativar o plug-in Espaço de trabalho CSM em uma instância chamada Minha instância.

Formulário Ativar plug-in



7. Selecione **Enviar**.
   Para obter detalhes adicionais sobre como solicitar um plug-in, consulte Solicitar um plug-in no artigo do Catálogo de serviços [KB0751715] em Now Support Base de conhecimento.

Resultados

Ativar o plug-in Domain Extension Installer habilita estes recursos:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- O Domain Separation é baseado na tabela Domínio `[sys_domain]`.
- A administração delegada permite que cada domínio tenha uma política separada.
- Todos os registros fazem parte do domínio global.
- O domínio do usuário atual determina o domínio a ser usado ao exibir ou operar em um registro em um domínio diferente.

Informações relacionadas

Plug-in Domain Separation

Plug-in Separação de domínios

O plug-in Domain Support - Domain Extensions Installer ativa vários recursos e propriedades da Separação de domínios de uma só vez. Esse plug-in é normalmente conhecido como plug-in Separação de domínios.

Prática recomendada para ativar o plug-in Separação de domínios

Como parte do desenvolvimento da Separação de domínios, os administradores devem solicitar a ativação desse plug-in. Para obter melhores resultados, ative o plug-in Separação de domínios no início do processo de desenvolvimento, de preferência antes de qualquer outro plug-in ser habilitado.

Importante: Solicite a ativação do plug-in Domain Extensions Installer (com.glide.domain.msp_extensions.installer) antes de ativar a Separação de domínios (plugin com.snc.pa.domain_support).

Se você habilitar a Separação de domínios no final da ServiceNow implementação ou depois que uma instância for ativada, sua aplicação estará em risco no desempenho e no processo. Em instâncias estabelecidas, dependendo de como as coisas foram estruturadas no desenvolvimento, o risco para a plataforma e sua usabilidade podem ser altos. Para saber mais sobre o processo da Domain Separation, consulte Explorando o Domain Separation.

Por exemplo, quando o plug-in Separação de domínios está habilitado, a coluna **Domínio** (sys_domain) é adicionada à tabela de tarefas e todos os registros existentes são colocados automaticamente em **global**. Para usar um script para atribuir todos os registros nos domínios corretos, é necessária uma hierarquia primário/secundário estabelecida. Esses tipos de ações de script podem ser corrompidos ou perdidos, além de um possível tempo de inatividade da produção, conforme grandes quantidades de dados são movidas. Muito do código da plataforma também é colocado em **global**, como regras de negócio, scripts de cliente, exibições de formulário e fluxos de trabalho.

Se um cliente criar ou modificar o código ServiceNow, haverá risco para o desempenho e a usabilidade da plataforma. Os proprietários de instância podem atrasar severamente sua implementação ou passar por longos períodos de inatividade com esse tipo de abordagem.

Recursos do plug-in Separação de domínios

Estes recursos são habilitados quando você ativa o plug-in:

- A Separação de domínios é baseado na tabela Domínio `[sys_domain]`.
- A administração delegada permite que cada domínio tenha uma política separada.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Todos os registros fazem parte do domínio global.
- O domínio do usuário atual determina o domínio a ser usado ao exibir ou operar em um registro em um domínio diferente.

Informações relacionadas

Práticas recomendadas do Domain Separation para provedores de serviço

Propriedades do sistema do domínio e preferências do usuário

Os administradores têm acesso às propriedades e preferências do usuário que controlam o escopo do domínio.

Propriedades

Novas ativações do Domain Separation restringem automaticamente o escopo do domínio ao domínio do registro para todos os dados ou processos relacionados. Quando o usuário exibe um registro em um formulário, os dados relacionados do registro (como o selecionador de referência e os dados da lista relacionada) e os processos aplicados (como as regras de negócio e os scripts de cliente) são restritos ao escopo do domínio do registro. Se houver registros em várias guias, cada guia terá seu próprio escopo do domínio com base no registro aberto nessa guia. As propriedades a seguir restringem o escopo do domínio ao domínio do registro e ao domínio da sessão atual do usuário.

Propriedades do sistema do domínio

Propriedade	Detalhes
glide.sys.domain.use_record_domain_for_processes	Restringe o escopo do domínio ao domínio do registro para todos os processos. Esta propriedade não se aplica a regras de negócio. As regras de negócio são sempre processadas a partir do registro de domínio. • *Tipo*: verdadeiro | falso • *Valor padrão*: verdadeiro • *Local*: Tabela propriedades do sistemna [sys_properties]
glide.sys.domain.use_record_domain_for_data	Restringe o escopo do domínio ao domínio do registro para todos os dados. • *Tipo*: verdadeiro | falso • *Valor padrão*: verdadeiro em novas ativações de domínio da Fuji em diante (upgrades de instâncias mais antigas que a Fuji não têm esta propriedade na tabela) • *Local*: Tabela propriedades do sistemna [sys_properties]

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Quando a propriedade *glide.sys.domain.use_record_domain_for_processes* ou *glide.sys.domain.use_record_domain_for_data* é definida como **verdadeira**, as seguintes propriedades não são usadas, independentemente de sua configuração:

- *glide.sys.domain.use_record_domain*
- *glide.sys.domain.use_record_domain_for_client_scripts*
- *glide.sys.domain.domain_change_notify*
- *glide.sys.domain.no_change_roles*

Para obter uma lista completa de propriedades, consulte Propriedades do sistema disponíveis.

Nota:

Em novas ativações do Domain Separation começando com a versão Jakarta, o domínio da sessão determina as regras de negócio executadas na tabela de domínio. Nas versões anteriores, as regras de negócio executadas na tabela de domínio eram definidas com base na hierarquia de domínio recém-criado. Esse comportamento é modificado pela propriedade *glide.sys.domain.skip_domain_insert_businessrules*. Definir esta propriedade como verdadeira melhora significativamente o desempenho de inserção de domínio.

Propriedades de escopo do domínio para regras de negócio executadas na tabela de domínio

Propriedade	Detalhes
glide.sys.domain.skip_domain_insert_businessrules	Especifica o escopo do domínio para regras de negócio executadas na tabela de domínio. Em novas ativações do Domain Separation, o padrão da propriedade é verdadeiro e as regras de negócio são determinadas pelo domínio da sessão. Em implementações existentes, o padrão da propriedade é falso e as regras de negócio são determinadas pela hierarquia de domínio recém-criado. • *Tipo*: verdadeiro | falso • *Valor padrão*: Verdadeiro em novas ativações de domínio começando com Jakarta. Falso em implementações existentes.
glide.sys.domain.skip_non_global_businessrule_if_nodomain	Garante que apenas bus.rules do domínio global sejam executadas ao usar queryNoDomain () ou quando a tabela não estiver separada

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Propriedades de escopo do domínio para regras de negócio executadas na tabela de domínio

Propriedade	Detalhes
	por domínio, para que você possa ignorar quaisquer outras regras de negócio • *Tipo*: verdadeiro | falso • Definir a propriedade como falso restaura o comportamento antigo e não se alinha com as ServiceNow® práticas recomendadas. • Recomendado: separe as tabelas por domínio; sempre tente usar o domínio do registro em vez do domínio da sessão.

Preferências do usuário

Além disso, os administradores de usuário podem definir as seguintes preferências do usuário globalmente ou por usuário:

Preferências do usuário do escopo de domínio

Preferência	Categoria	Atualizada Por	Detalhes
glide.domain.session_scope	Domínio	Somente administradores	Quando verdadeiro, define o escopo-padrão para o domínio da sessão do usuário em vez do domínio do registro. Quando falso, o escopo-padrão é o domínio do registro. Usuários com a função do usuário domain_expand_scope ainda podem mudar o escopo do domínio conforme necessário. • **Tipo**: verdadeiro | falso • **Valor padrão**: falso
glide.domain.session_scope_notification	Domínio	Somente administradores	Quando verdadeiro, exibe uma dica visual de que os valores de registro incluem um escopo do domínio

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Preferências do usuário do escopo de domínio

Preferência	Categoria	Atualizada Por	Detalhes
			expandido. Quando falso, a notificação fica oculta. • **Tipo**: verdadeiro | falso • **Valor padrão**: verdadeiro

Informações relacionadas

Propriedades da aplicação Separação de domínios

Criação de um domínio

É possível criar um domínio criando um registro na tabela [domain].

Antes de Iniciar

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

Ao criar um novo domínio, tenha em mente o seguinte:

- Somente um domínio pode ser o domínio-padrão.
- Somente um domínio pode ser o domínio primário.

Procedimento

1. Navegue até **Todos os** > **Domínios do Administrador** > **de Domínio**.
2. Clique em **Novo**.
3. Preencha os campos necessários (consultar tabela).
4. Clique em **Enviar**.

Campos de formulário de domínio

Campo	Descrição
Nome	Insira um nome exclusivo para o domínio.
Tipo	Selecione um tipo de domínio que descreva o domínio. Por padrão, os tipos de domínio são *Fornecedor*, *Clientee MSP*. Você também pode adicionar suas próprias escolhas.
Primário	Marque a caixa de seleção se este domínio for o domínio de nível superior na hierarquia. O domínio de nível superior tem apenas domínios secundários e nenhum domínio primário.
Padrão	Selecione se este domínio deve ser o domínio-padrão para sua hierarquia.
Primário	Selecione o nome do domínio superior na hierarquia que contém este domínio. Este campo deve ter um valor para o domínio aparecer no mapa de domínios.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Ativo	Marque a caixa de seleção para disponibilizar o domínio para uso. Você deve selecionar esta opção para que este domínio apareça no mapa de domínios.
Descrição	Insira uma descrição para o domínio.

Cada registro de domínio também pode ter vários registros relacionados:

- Empresas
- Domínios "contém"
- Incluído em

O que Fazer Depois

Para alterar a hierarquia de domínio, vá para a lista relacionada Domínios Contains e selecione o registro de domínio secundário (contido) do relacionamento "contém".

Como tornar um domínio o padrão

Torne um domínio o domínio padrão ao qual o sistema atribui automaticamente a tarefa e os registros de usuário que ainda não foram atribuídos a um domínio.

Antes de Iniciar

Função necessária: admin

Por Que e Quando Desempenhar Esta Tarefa

Nota: Se você não definir um domínio-padrão, novas tarefas e registros de usuário serão colocados no domínio global.

Procedimento

1. Navegue até **Todos os** > **Domínios do Administrador** > **de Domínio**.
2. Abra o domínio que você deseja que seja o domínio padrão, por exemplo, Principal.
3. Configure o layout do formulário para adicionar o campo **Padrão**.
4. Marque a caixa de seleção **Padrão**.
5. Clique em **Atualizar**.

Como gerenciar manualmente o domínio para registros específicos

Por padrão, o sistema atribui usuários automaticamente a um domínio baseado no registro da empresa do usuário. Em alguns casos, no entanto, os administradores de domínio desejam gerenciar manualmente o domínio ao qual um registro específico pertence.

Antes de Iniciar

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

O campo **Domínio gerenciado** permite que os administradores de domínio selecionem manualmente um domínio para o usuário, grupo, departamento, local ou registro de IC, em vez de usar o domínio é atribuído automaticamente a partir do registro da empresa. O campo **Domínio gerenciado** está disponível nesses tipos de registro.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Registros de usuário
- Registro de grupo
- Registros do departamento
- Registros do local
- Registros de IC

Procedimento

1. Navegue até o registro que você deseja gerenciar manualmente.
2. Marque a caixa de seleção Domínio **gerenciado**.
3. No campo **Domínio**, selecione o domínio do registro.
4. Clique em **Atualizar**.

   Desmarcar a caixa de seleção **Domínio gerenciado** oculta o campo **Domínio** e o registro usa o valor de domínio da empresa do registro.

Informações relacionadas

Práticas recomendadas do Domain Separation para provedores de serviço

Tabelas separadas por domínio

Você pode ver rapidamente quais tabelas são separadas por domínio na instância com o recurso Tabelas separadas por domínio.

Visão geral

Use o recurso Tabelas separadas por domínio para ver quais tabelas são separadas por domínio. Comece a digitar "domínio" no filtro **Todos** para acessar **Tabelas separadas por domínio** no painel de navegação esquerdo.

Você pode filtrar esta exibição para exibir ou remover nomes de coluna para procurar determinadas propriedades ou atributos que estão incluídos em suas tabelas. Existem dois tipos de tabela que são exibidos na lista:

- Tabelas que têm uma coluna *sys_domain* explícita, em que o nome da **coluna** exibe o valor *sys_domain* na lista.
- Tabelas que usam o atributo *domain_master* para derivar o Domain Separation de um registro referenciado, em que a coluna **Atributos** inclui o valor *domain_master=ref-field-value*.

Ao usar as seleções Mostrar correspondência ou Filtrar no menu Nome da coluna, você pode exibir esses dois tipos de tabelas.

Visualizador de substituição de domínio

Com o Visualizador de substituição de domínio, você pode ver e gerenciar todas as substituições de processo de uma só vez em toda a instância.

Visão geral

Em vez de criar uma pesquisa elaborada de substituições em seus scripts, você pode usar o Visualizador de substituição de domínio para localizá-los rapidamente. Comece a digitar "domínio" no filtro **Todos** para acessar **Visualizador de substituição de domínio** no painel de navegação esquerdo.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O seletor de tabela no Visualizador de substituição de domínio exibe uma lista somente das tabelas que contêm substituições de registro, junto com uma contagem de substituições nessa tabela. Depois de selecionar uma tabela, uma lista de todos os registros primários com substituições é retornada. Você pode exibir rapidamente todos os **registros primários**, o **domínio** do registro primário e uma **contagem** de substituições para cada registro.

Selecionar **Substituições de exibição** carrega uma nova guia em que todas as substituições, incluindo o registro primário, são exibidas na exibição de lista padrão. Selecione uma tabela na lista suspensa para exibir todos os registros e substituições. Selecione **Exibir substituições** em um registro para exibir todas as substituições específicas de registro.

Nota: Somente tabelas com substituições são listadas.

Para saber mais, consulte Criar substituições de propriedade separada por domínio.

Como habilitar ou desabilitar um domínio

Quando você ativa ou desativa um domínio, o status de ativação é propagado para as empresas no domínio.

Antes de Iniciar

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

Quando você ativa um registro de empresa, o Domain Separation ativa automaticamente o domínio associado da empresa. Por exemplo, se você ativar a empresa ACME, também ativará o domínio TOP/ACME.

Procedimento

1. Navegue até o registro do domínio.
2. Desmarque ou marque a caixa de seleção **Ativo**.
3. Clique em **Atualizar**.

Aviso: Não exclua domínios. Desative os domínios de que você não precisa mais em vez de excluí-los.

Como adicionar um campo de domínio a uma tabela

Como um administrador, separe por domínio uma tabela personalizada adicionando um campo sys_domain a ela.

Antes de Iniciar

Função necessária: admin

Por Que e Quando Desempenhar Esta Tarefa

Nota:

Não adicione domínios às tabelas do sistema de base.

Procedimento

1. Navegue até a exibição de lista da tabela.
   Por exemplo, digite <table name>`.list` no filtro de navegação.
2. Clique com o botão direito do mouse no cabeçalho da lista e selecione **Configurar** > **Layout da Lista**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Na seção **Criar novo campo**, insira `sys_domain` como **Nome** e `ID de domínio` como **Tipo**.
4. Clique em **Adicionar**.
5. Clique em **Salvar**.

Nota:

Qualquer outro meio de criar um campo adiciona um prefixo **u_** ao nome da coluna. Mas com o campo de domínio, o sistema cria automaticamente o campo sem o prefixo **u_**. Você pode usar a seguinte funcionalidade como um atalho: Sempre que você criar um campo **sys_domain**, nomeie-o como **sys_domain** e deixe o tipo de campo como está. O sistema define automaticamente o tipo de campo como **ID de domínio** e o rótulo do campo como **Domínio**, economizando alguns cliques.

Adicionar domínios às tabelas do sistema base requer testes, atualizações e adição de nova lógica proibitivamente completos. Além disso, em muitos casos, o código-fonte não está acessível para o cliente.

Exibição de relacionamentos do domínio

O mapa de domínio oferece aos administradores de domínio uma representação somente leitura dos domínios ativos na instância e como eles se relacionam entre si.

Antes de Iniciar
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa
Todos os mapas de domínio devem ter um domínio definido como o domínio primário. Além disso, cada domínio no mapa de domínios deve atender a estes critérios:

- O campo **Primário** deve ser preenchido (o domínio primário é a única exceção).
- A caixa de seleção **Ativo** deve ser marcada.

O mapa de domínio não desenha relacionamentos de domínio para domínios que não atendem aos critérios de mapeamento.

Procedimento

1. Navegue até **Todos os** > **Mapas de Domínios** > **do Administrador de Domínio**.
2. Clique nos ícones de mais (**+**) ou menos (**-**) nos cabeçalhos do domínio para mostrar ou ocultar subdomínios.

Seleção de um domínio primário

O domínio primário indica o domínio de nível superior no mapa de domínio.

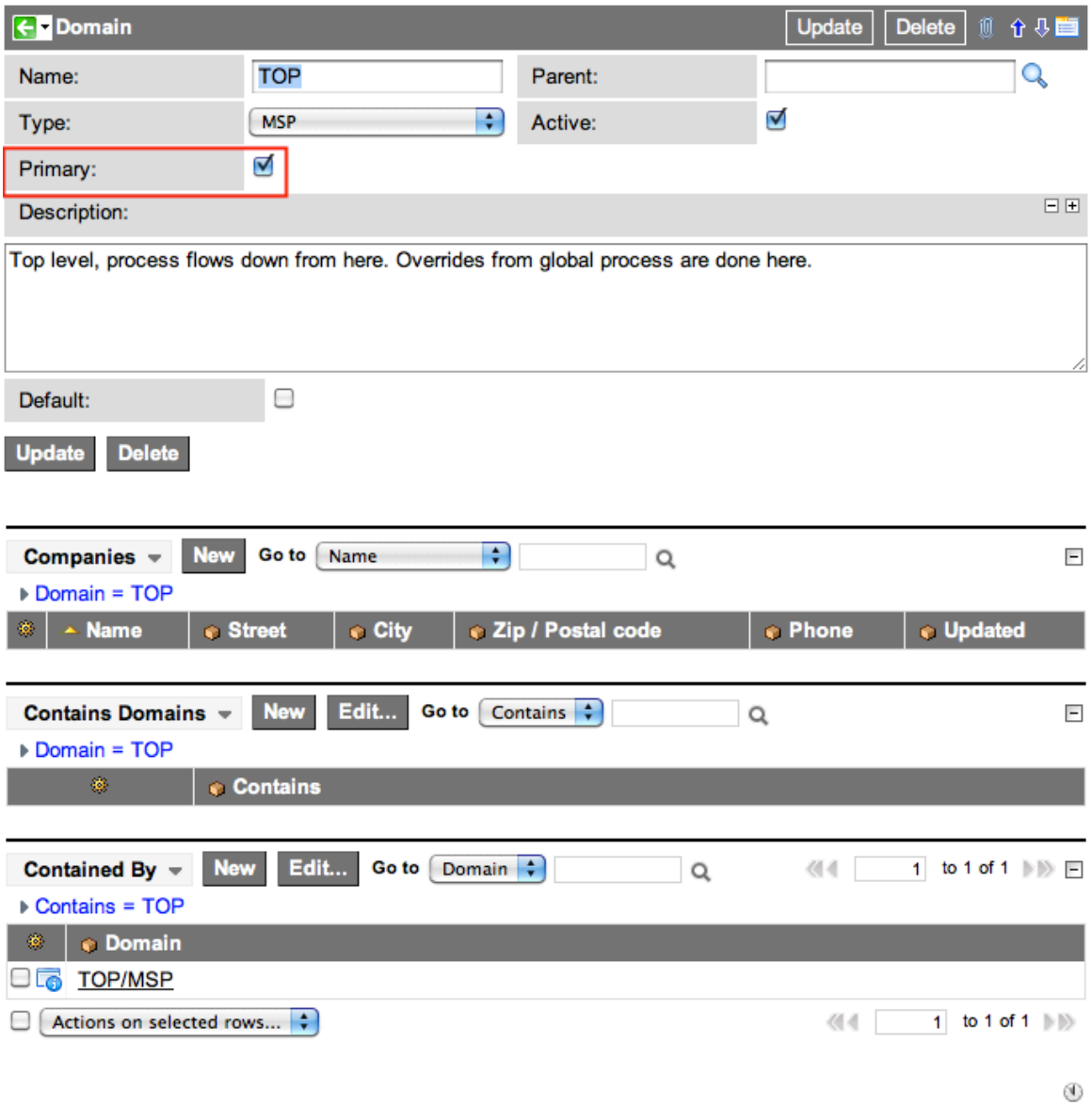
Antes de Iniciar
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa
O domínio primário não pode ter um domínio primário e deve ter pelo menos um domínio secundário. Só pode haver um domínio primário de cada vez. Se você selecionar outro domínio como o domínio primário, ele substituirá o domínio primário anterior.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegue até **Todos os** > **Domínios do Administrador** > **de Domínio**.
2. Selecione o domínio que você deseja que seja o domínio primário, por exemplo, TOP.
3. Marque caixa de seleção **Primário**.
4. Clique em **Atualizar**.



Criação de relacionamentos "contém" entre domínios

Crie um relacionamento “contém” entre domínios para mudar a hierarquia de domínio.

Antes de Iniciar

Função necessária: administrador

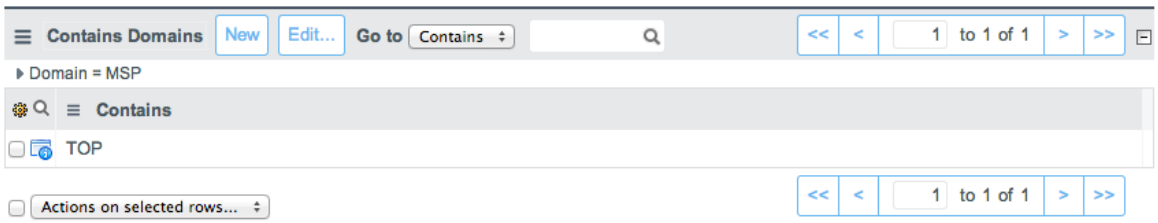
Por Que e Quando Desempenhar Esta Tarefa

Os domínios em um relacionamento "contém" herdam as configurações do domínio que o contém. O domínio contido permite que os usuários vejam os dados no domínio contido, bem como qualquer um de seus secundários. Os processos não são afetados por um relacionamento "contém".

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegue até a tabela do domínio.
2. Selecione o registro de domínio que é o domínio secundário (contêiner) do novo relacionamento "contém".
3. Alterne o escopo do domínio para alternar entre o escopo da sessão e o escopo do registro, se necessário.
4. Na lista relacionada Domínios "contém", clique em **Editar**.
5. Selecione o registro de domínio que é o domínio secundário (contido) do relacionamento "contém".
   Somente domínios secundários aparecem por padrão quando o seletor de domínio é definido como Global. Alterne o escopo do domínio para ver todos os domínios.
6. Clique em **Salvar**e em **Atualizar**.



Informações relacionadas

Práticas recomendadas do Domain Separation para provedores de serviço

Expansão do escopo do domínio

Por padrão, quando um usuário no domínio global exibe uma tabela que contém uma coluna **sys_overrides**, o usuário vê apenas os registros do domínio global. Quando um administrador no domínio global exibe uma tabela de processo, esse administrador vê somente os registros que estão nessa tabela de processo.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Mude a *glide.sys.restrict_global_domain_processes* propriedade para **verdadeira**.
2. Para exibir registros de todos os domínios, clique em **Expandir Escopo do domínio** em Links relacionados.
3. Para retornar à exibição de registros somente do domínio global, clique em **Recolher Escopo do Domínio**.

Como adicionar domínios a uma lista de domínios de visibilidade

Adicionar um domínio de visibilidade permite que um usuário ou grupo veja e potencialmente edite registros de outro domínio, independentemente da associação de domínio normal do usuário ou grupo.

Antes de Iniciar

Função necessária: administrador

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

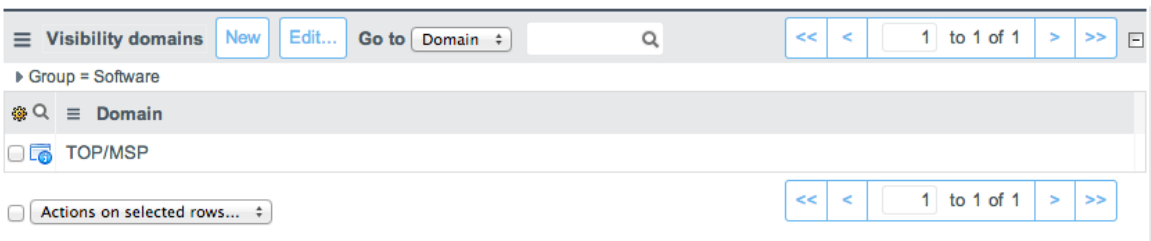
Por Que e Quando Desempenhar Esta Tarefa

Atribuir domínios de visibilidade a todos os membros de um grupo é preferencial em vez de concedê-los a usuários individuais.

Nota: Adicionar um domínio de visibilidade não muda uma tabela ou os requisitos de regra de controle de acesso de um registro.

Procedimento

1. Navegue até a tabela do grupo.
2. Selecione o grupo para o qual você deseja fornecer domínios de visibilidade.
3. Adicione a lista relacionada a **Domínios de visibilidade** ao formulário.
4. Na lista relacionada **Domínios de visibilidade**, clique em **Editar**.
5. Selecione os registros de domínio que você deseja que o grupo ou domínio veja.
6. Clique em **Salvar**e em **Atualizar**.



Como conceder domínios de visibilidade a um usuário individual

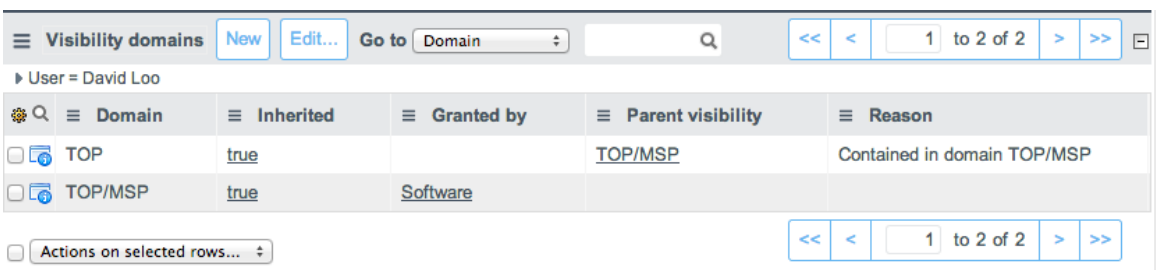
Embora seja possível adicionar domínios de visibilidade para usuários específicos no formulário do usuário, é melhor adicioná-los somente por meio de grupos. Controla as permissões e o acesso caso os indivíduos mudem de departamento ou saiam da empresa.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Navegue até **Todos** > **Administração de usuários** > **Usuário**.
2. Selecione o usuário para o qual você deseja fornecer domínios de visibilidade.
3. Adicione a lista relacionada a **Domínios de visibilidade** ao formulário.
4. Na lista relacionada Domínios de visibilidade, clique em **Editar**.
5. Selecione os registros de domínio que você deseja que o usuário veja.
6. Clique em **Salvar**e em **Atualizar**.



A lista integrada do Domínio de visibilidade contém os seguintes campos.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Domínio	Domínio que está visível para o grupo ou usuário.
Herdados	O domínio é herdado da visibilidade do domínio ou de um domínio primário.
Concedido por	Nome do grupo que concedeu visibilidade ao domínio.
Visibilidade primária	Nome do domínio primário e usado para agrupar registros. Se o registro primário for excluído, todos os registros com o mesmo primário também serão excluídos.

Criação de uma lista de seleção específica de domínio

Os administradores podem configurar listas de seleção para conter entradas específicas para um domínio específico.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Selecione o domínio no seletor de domínio ao qual a opção deve ser adicionada.
2. Clique com o botão direito do mouse no campo de opção que você deseja personalizar e selecione **Configurar opções**.
3. Atualize ou adicione opções.
4. Envie mudanças por meio do processo de mudança normal, como conjuntos de atualizações.

   Nota: Os administradores devem garantir que as opções sejam exclusivas entre os domínios para evitar confusão administrativa no domínio global.

   Se um administrador adicionar uma nova opção do domínio global, os usuários de domínios inferiores na hierarquia verão a nova opção no final de suas listas de seleção atuais. Se a nova opção não estiver ativa no nível global, ela estará disponível para os usuários do domínio por meio de **Configurar opções**, mas não será exibida como uma opção ativa.

Administração avançada do domain separation

Os administradores podem exibir informações sobre o domain separation, identificar possíveis problemas e alterar as definições de configuração.

Você pode executar estas tarefas administrativas avançadas em domínios:

- Uso de menus de seleção de domínio
- Exibição de relacionamentos do domínio

Uso de menus de seleção de domínio

A instância oferece seleção de domínio por meio de dois formatos de menu.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Seletor de domínio: fornece uma lista suspensa simples de domínios disponíveis.
- Seletor de referência de domínio: ativa um campo de referência que oferece filtragem e um recurso de entrada de preenchimento automático. Use este formato para listas mais longas.

O posicionamento desses seletores e o procedimento para mostrá-los ou ocultá-los diferem dependendo da versão da interface do usuário.

Como habilitar menus de seleção de domínio em IU principal

Exibir o seletor de domínio em IU principal habilita o seletor de domínio por padrão. Depois de habilitar o seletor de domínio, você pode adicionar uma propriedade do sistema para habilitar o seletor de referência de domínio.

Antes de Iniciar

Nota: O domain separation (plug-in com.snc.pa.domain_support) é necessário para habilitar o seletor de referência de domínio.

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

Procedimento

1. Clique no ícone de engrenagem no cabeçalho.
2. Na guia Geral, clique no comutador **Mostrar seletor de domínio no cabeçalho**.
   O seletor de domínio aparece no cabeçalho IU principal.
3. Opcional: Habilite o seletor de referência de domínio.

   Nota: Habilitar o seletor de referência de domínio remove a opção global da lista. Para retornar ao seu domínio inicial, clique na seta de retorno ao lado do campo de referência. Os usuários administradores podem clicar na seta de retorno para retornar ao domínio global.

   a. Digite `sys_properties.list` no navegador de aplicações.
   b. Se ainda não estiver presente, adicione a propriedade `glide.ui.domain_reference_picker.enabled` e defina o valor como **verdadeiro**.
   c. Atualize o navegador.
   O seletor de referência de domínio aparece no IU principal cabeçalho.

Restrição do acesso ao seletor de domínio

Use uma propriedade do sistema para restringir o acesso ao seletor de domínio em IU principal e Next Experience.

Antes de Iniciar

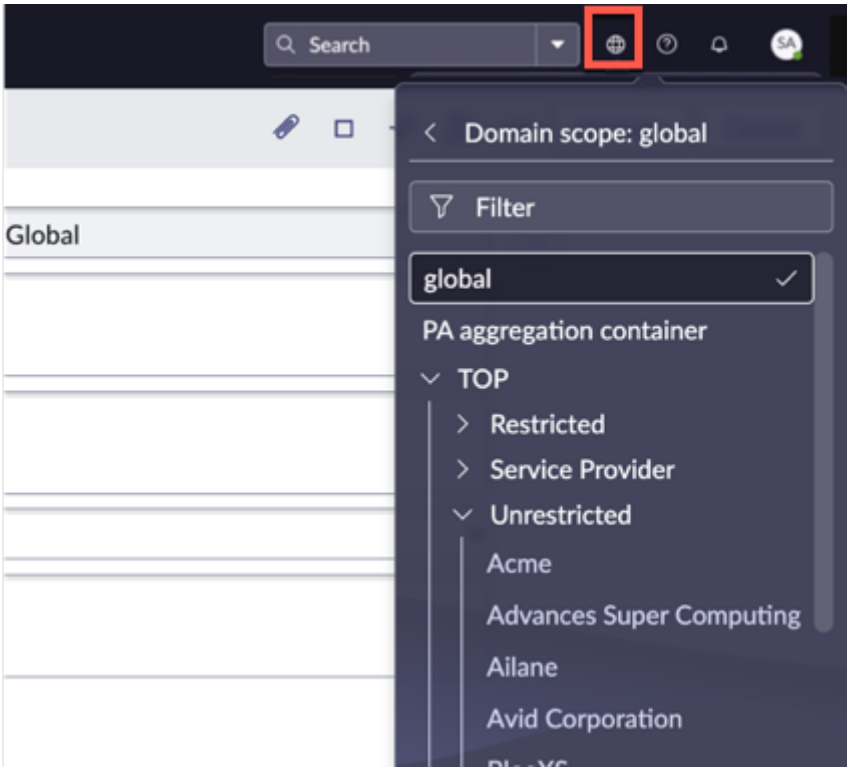
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

Por padrão, os usuários com a função ITIL e as funções que incluem a função ITIL (como o administrador) podem acessar o seletor de domínio em Next Experience. Você pode conceder acesso a outras funções adicionando-as à propriedade ou restringir as funções removendo-as. É recomendável restringir a função apenas a administradores.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Os administradores podem conceder acesso a usuários criando uma propriedade do sistema na tabela sys_properties.



Procedimento

1. Abra a tabela Propriedades do sistema [sys_properties].
2. Adicione esta propriedade: `glide.ui.polaris.domain_picker.role`
3. Configure o valor da propriedade como uma lista de funções separada por vírgulas: **admin, itil**.
   Para saber mais, consulte Configurar seletores do Next Experience

Propriedades da aplicação Separação de domínios

O plug-in Separação de domínios tem duas novas tabelas para dar aos provedores de serviço mais flexibilidade na personalização de suas aplicações que usam a Separação de domínios. Essas tabelas são a tabela de Propriedade de aplicação do sistema [sys_application_property] e a tabela de Valor de propriedade de aplicação do sistema [sys_application_property_value].

Como ass novas tabelas oferecem mais opções

Com as aplicações de provedor de serviço (SP), determinadas ações podem variar dependendo no domínio. No entanto, a tabela Propriedades do sistema [sys_properties] ServiceNow® do sistema de base não é separada por domínio, portanto, não atende aos requisitos para aplicações que usam a Separação de domínios.

Cada cliente de SP pode querer personalizar suas aplicações de forma diferente. Anteriormente, os recursos que podiam ser personalizados eram definidos como apenas um valor global. Os desenvolvedores de aplicações precisam de uma tabela mais flexível. Agora você pode modificar sua aplicação sem precisar criar código sempre que quiser adicionar ou alterar a funcionalidade.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Como as substituições funcionam nas novas tabelas

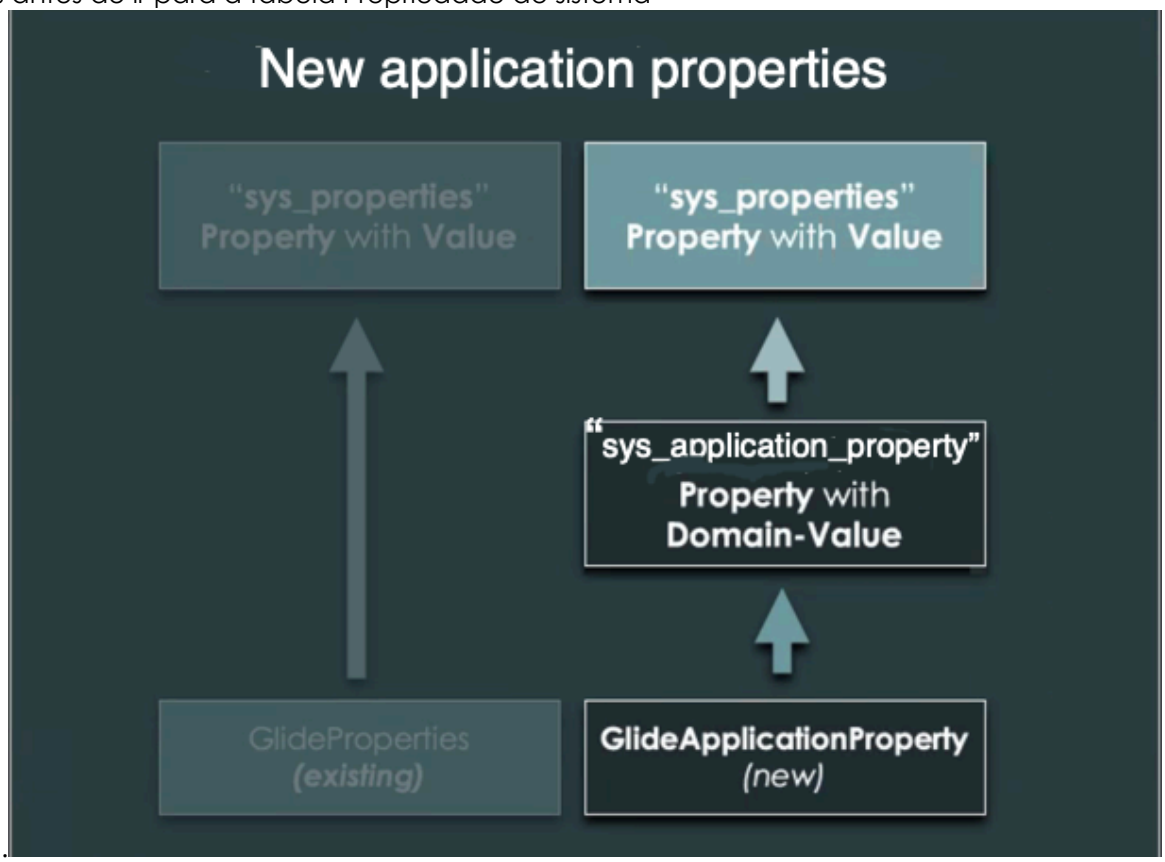
Os desenvolvedores geralmente usam a tabela ServiceNow Propriedade do sistema [sys_properties] para criar várias funções em aplicações. Se você quiser desenvolver uma aplicação para se comportar de forma diferente em domínios diferentes, será necessário personalizá-la.

Na versão Paris, a nova tabela de Propriedade da aplicação [sys_application_property] simplifica essa personalização. Em vez de ir diretamente para a tabela de Propriedade do sistema para obter um valor, a tabela de propriedades da aplicação vai para a tabela de Aplicação do sistema primeiro. Esta nova tabela agora armazena a lógica necessária para configurar sua aplicação. Se encontrar uma propriedade na nova tabela, ele usará esse conteúdo. Se não houver informações nessa tabela, ele muda para a tabela de propriedades do sistema de base.

Ao configurar o suporte para a Separação de domínios, você pode adicionar lógica de domínio a esta nova tabela de Propriedades da aplicação. Esta tabela pode conter propriedades que não existem na tabela Propriedades do sistema. Ou você pode adicionar propriedades à tabela de configuração que podem substituir qualquer propriedade selecionada na tabela Propriedades do sistema.

Por exemplo, digamos que você queira configurar uma aplicação com o recurso Primeiro dia da semana. Às vezes, você pode querer que o primeiro dia da semana seja o domingo. Em outros casos, você pode querer que o primeiro dia da semana seja a segunda-feira. Na tabela do sistema de base, pode haver apenas uma opção de Dia 1, que é o domingo. Com a nova tabela, você pode armazenar outra propriedade, tornando o Dia 1, domingo, e um domínio secundário, segunda-feira.

Esta figura mostra como o sistema extrai propriedades da tabela Propriedade das aplicações antes de ir para a tabela Propriedade do sistema [sys_properties].

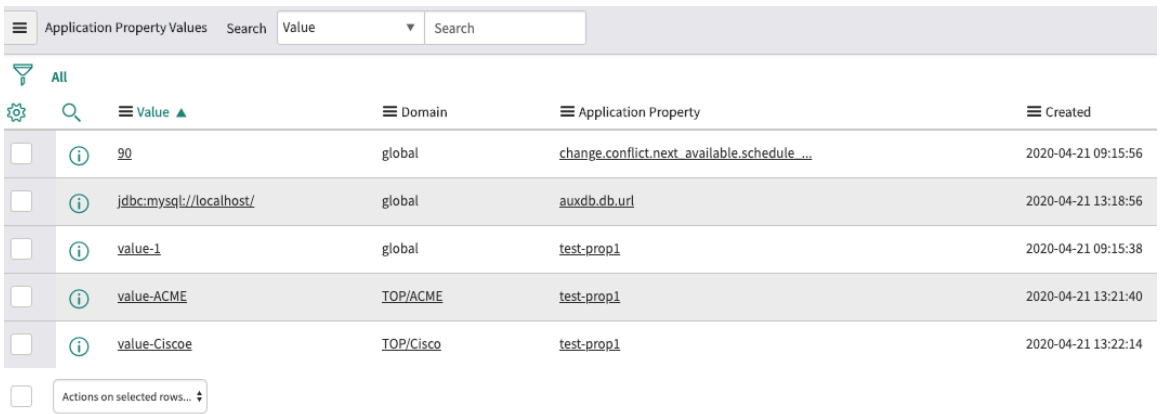


© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Como os aplicativos com escopo funcionam na nova tabela

A nova tabela de Propriedades da aplicação é compatível com aplicações com escopo. O nome da propriedade da aplicação, semelhante ao nome da propriedade do sistema, é exclusivo, o que significa que ele é prefixado com o nome do escopo se não for global. O escopo de uma aplicação afeta sua configuração. O escopo pode determinar qual Dia 1 é definido como domingo e qual como segunda-feira. Você pode usar a mesma propriedade, mas personalizá-la para que o Dia 1, domingo, seja o domínio primário e o Dia 1, segunda-feira, seja o domínio secundário. Na nova tabela, há uma coluna de domínio e uma coluna de escopo, portanto, você pode definir essas propriedades para cada uma.

Você pode usar a exibição Expandir escopo de domínio na tabela sys_application_property_value para mostrar todas as substituições, conforme mostrado na imagem a seguir.



Nota:

Se essas tabelas não estiverem disponíveis, certifique-se de ter ativado o plug-in Domain Extension Installer (com.glide.domain.msp_extensions.installer).

Novas tabelas de propriedades da aplicação

A nova tabela de Propriedade da aplicação do sistema [sys_application_property] contém estes campos:

- nome
- descrição
- tipo (escolha de cadeia de caracteres, verdadeiro | falso, inteiro, fuso horário, cor e assim por diante)
- default_value
- propriedade (referência a sys_properties)
- usage_notes
- read_roles
- write_roles
- chave exclusiva: (nome)

A nova tabela de Valor de propriedade da aplicação do sistema [sys_application_property_value] contém estes campos:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- sys_application_property (ref para sys_application_property)
- sys_domain
- sys_overrides
- valor
- chave exclusiva: (sys_application_property, sys_domain)

Novas APIs

As novas APIs também são compatíveis com aplicativos com escopo. As propriedades da aplicação separadas por domínio têm APIs distintas. A API GlideApplicationProperty tem dois novos métodos programáveis, disponíveis em aplicações globais e com escopo. Consulte GlideApplicationProperty - com escopo, gGlobal para saber mais sobre essas novas APIs.

Informações relacionadas

Práticas recomendadas do Domain Separation para provedores de serviço

Ferramenta de migração de domínio

Use a Ferramenta de migração de domínio para mover um cliente de um ambiente separado por domínio para sua própria instância dedicada.

Plug-in da Ferramenta de migração de domínio

O plug-in da Ferramenta de migração de domínio (com.glide.domain.migration_tool) simplifica a tarefa de mover um cliente de um ambiente separado por domínio para uma instância dedicada mais flexível. Os clientes podem migrar para uma instância separada para aproveitar melhor os recursosNow Platform. Embora o plug-in Separação de domínios esteja instalado, as propriedades de separação de dados e processos estão desativadas.

Nota: Você deve solicitar uma instância clonada e solicitar a ativação do plug-in Domain Migration Tool antes de usá-la.

A Ferramenta de migração de domínio será executada somente se a separação de dados e de processo estiver habilitada na instância separada por domínio:

- A propriedade de dados *glide.sys.domain.partitioning* deve ser definida como **verdadeira**.
- A propriedade de processos *glide.sys.domain.delegated_administration* deve ser definida como **verdadeira**.

O que a ferramenta de migração faz

- Automatiza grande parte do processo de migração, especialmente a limpeza de dados.
- Migra a instância separada por domínio para uma nova instância dedicada.
- Exclui dados da instância dedicada.

  Nota: A ferramenta não exclui dados globais, no domínio de destino ou em domínios de dados adicionais (se especificado).

- Recolhe os dados do processo ou, se não for possível recolher, exclui os dados do processo
- Mantém registros de processo que são visíveis para o domínio de destino

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Atualiza as tabelas especiais sys_choice, sys_ui_list e sys_ui_related_list
- Limpa os registros adicionados por plug-ins Separação de domínios:
  - Regras de negócio
  - Ações de IU
  - Trabalhos agendados
  - Saídas de instalação
  - Módulos de navegação
- Desabilita o Separação de domínios e remove domínios da instância clonada:
  - Define estas propriedades como **falsas** na instância clonada:
    - *glide.sys.domain.partitioning*
    - *glide.sys.domain.delegated_administration*
    - *glide.sys.domain.enabled*
  - Exclui todos os domínios, exceto o domínio de destino e todos os domínios de dados adicionais especificados.
- Atualiza o campo **Status** na tabela domain_migration_tool_status.

Status individual das tabelas

Status	Descrição
Pendente	Status-padrão de tabelas separadas por domínio durante a migração. As tabelas estão programadas para serem migradas, mas ainda não iniciaram a migração.
Falha	Falha no nível da tabela. Se o processo de migração for concluído com erros, este status indica quais tabelas têm erros.
Em execução	O status da tabela que está sendo migrada no momento. Somente uma tabela pode ter este status e migrar no momento.
Bem-sucedido	O status das tabelas que foram migradas com sucesso.
Concluído com êxito	O processo de migração foi concluído sem erros.
Concluído com erros	O processo de migração foi concluído com erros.

- Registra em log o andamento e o status em syslog_domain

  A origem é **MigrationTool** para todas as entradas de log associadas à migração.

  - Registra em log cada tabela de dados e quantas tabelas de dados permanecem
  - Registra em log cada tabela de processo e quais registros de domínio estão sendo desativados ou excluídos

O que a ferramenta de migração não faz

- Clonar a instância
- Criar outra instância separada por domínio

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Migrar registros (dados ou processo) se as propriedades de separação de dados ou de processo forem desabilitadas antes de executar a ferramenta
- Alterar quaisquer dados na instância de origem
- Excluir dados globais, no domínio de destino ou em domínios de dados adicionais (se especificado)

O que você deve fazer após executar a ferramenta

A Ferramenta de migração de domínio automatiza a remoção de dados fora dos domínios desejados (o domínio de destino, quaisquer domínios de dados adicionais e o domínio global). Você deve avaliar todas as configurações restantes para garantir que elas sejam apropriadas e funcionem para a instância dedicada. Por exemplo, se você tivesse uma regra de negócio que definisse o campo de domínio em registros, convém desabilitar essa regra de negócios, já que ela não atende mais a uma finalidade.

Migração da instância separada por domínio para uma nova instância dedicada.

Mova um cliente de um ambiente separado por domínio para seu próprio ambiente de instância dedicada.

Antes de Iniciar

Função necessária: security_admin e administrador

Procedimento

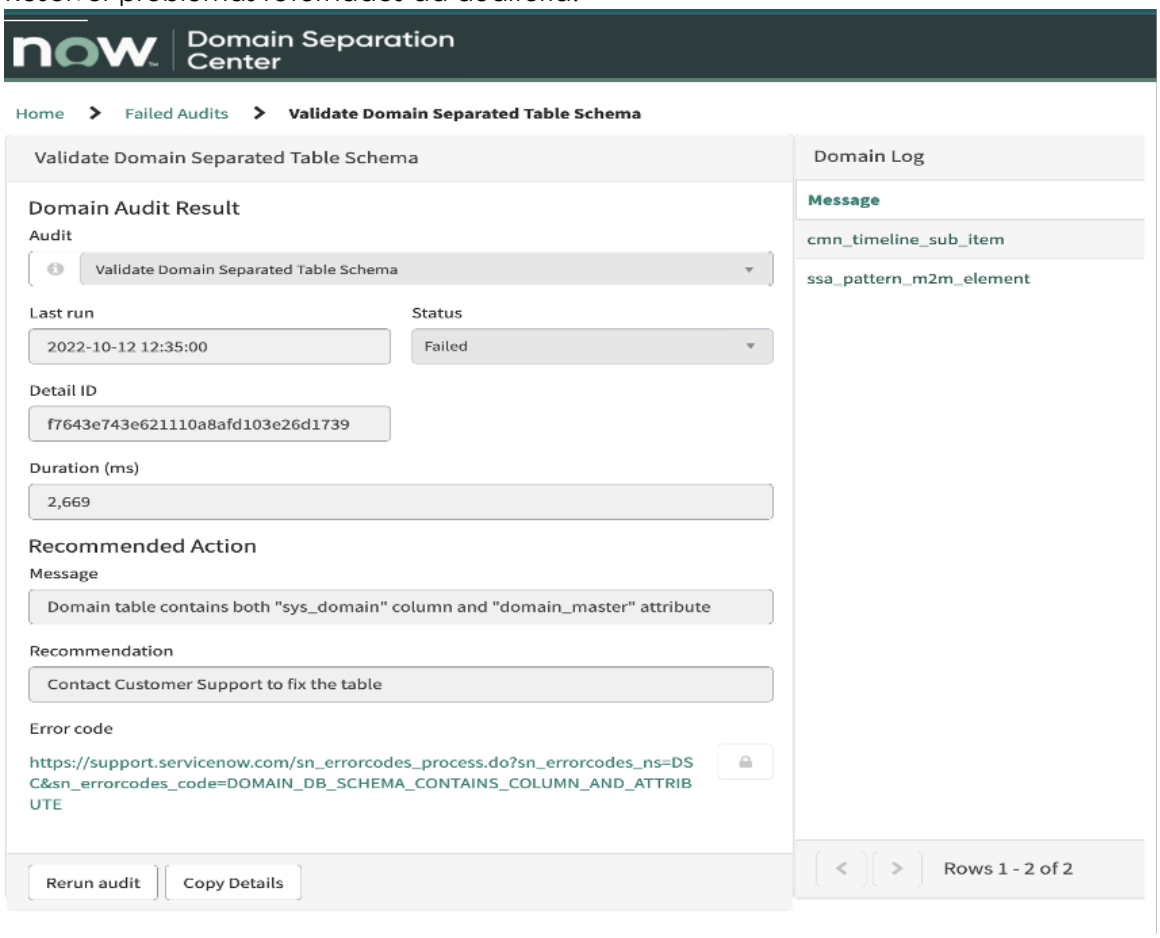
1. Eleve para a função security_admin.
   Consulte Elevação para uma função privilegiada para obter detalhes.
2. Navegue até **Todos** > **Administrador de domínio** > **Ferramenta de migração de domínio**.
   Acesse também com **domain_migration_tool_status.list**.
3. Clique em **Novo**.
4. Preencha o formulário.

Campo	Descrição
Domínio de destino	Especifique o domínio usado para o processo e os dados que você deseja migrar. Somente o domínio de destino é retido, não qualquer um de seus secundários, a menos que especificado no campo **Domínios de dados adicionais**.
Domínios de dados adicionais	Opcionalmente, especifique os domínios de dados adicionais que você deseja migrar. Se você quiser migrar o domínio de destino e todos os seus secundários, deverá especificar todos os secundários.

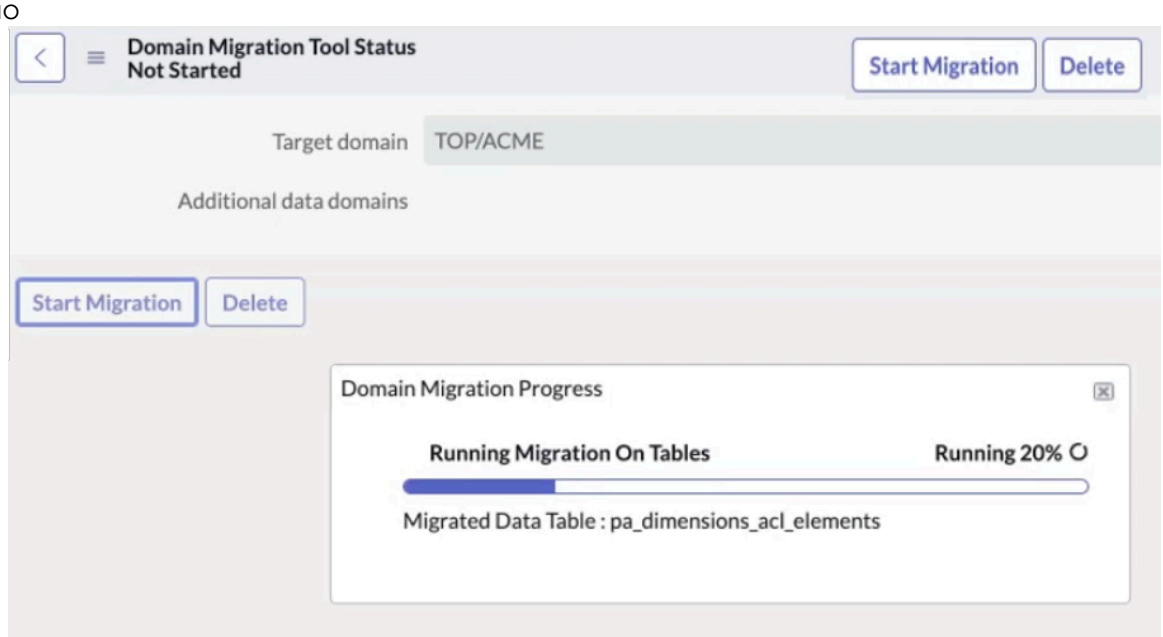
5. Selecione **Enviar**.
6. Abra o formulário que você acabou de enviar.
7. Navegue até **Todas** > **Centro de Separação de domínios** > **Configurar auditorias** .
   Consulte Central de Separação de domínios para obter informações adicionais.
8. Defina a auditoria **Validar esquema de tabela separada por domínio** como **Ativa** e atribua uma programação.
   Esta é uma auditoria de domínio de precaução para verificar previamente o esquema quanto à integridade de tabelas separadas por domínio. Isso permite que você corrija erros antes de executar a migração.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

9. Execute a **Programação de auditoria** que inclui o esquema.
   Consulte Execução de auditorias imediatamente para obter detalhes.
10. Resolver problemas retornados da auditoria.



11. Selecione **Iniciar migração**.
    - A barra de andamento do rastreador de execução e a ferramenta de migração de domínio são acionadas.



    - A tabela de migração atual em andamento é exibida junto com a porcentagem total de tabelas migradas com êxito.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- A tabela em que todas as tabelas separadas por domínio são registradas com o status da migração, o número total de registros em cada tabela e o número de registros migrados.
- A contagem de tabelas em que a migração falhou também é registrada.
- O **Status** é atualizado conforme a ferramenta executa suas funções.
- A migração de domínio ainda estará em execução em segundo plano se você fechar a barra de andamento. Acesse a tabela `sys_execution_tracker` e procure por **Migração em Execução nas Tabelas** para verificar o processo de migração em execução em segundo plano.

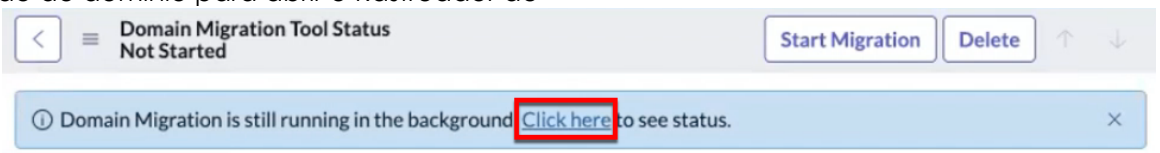
O Status da Ferramenta de migração de domínio exibe os seguintes campos:

Campos de Status da ferramenta de migração de domínio

Campo	Descrição
Status	Exibe o status da migração. - **Migrando tabelas de dados...**: status em andamento. - **Migração bem-sucedida**: o status atualizado após uma migração bem-sucedida. - **Erro de configuração observado em uma das tabelas separadas por domínio**: indica uma falha na migração de dados. Foi encontrado um erro de esquema, a migração não será iniciada. Execute a auditoria **Validar esquema de tabela separada por domínio**. A auditoria falhará e mostrará as tabelas que não seguem o padrão de esquema. - **Concluído com erros nas tabelas de revisão**: o número de tabelas para lidar com a migração de esquema é listado. Localize as falhas em Rever contagem de tabelas e resolva os problemas de esquema. - **Falha na migração de domínio para tabelas...**: registros que não sejam de destino devem ser excluídos manualmente das tabelas com falha. - **Concluído com êxito**: quando todas as tabelas forem migradas.
Domínio de destino	O domínio de destino selecionado para migração.
Domínios de dados adicionais	Preenche se vários domínios de migração foram selecionados.
Rever contagem de tabelas	Este campo será preenchido somente se houver falha na migração de uma tabela. Se não houver falhas, essa contagem será zero. Nesse caso, as tabelas serão revisadas para tentar novamente a migração. Se não houver falhas, não será necessário revisitar as tabelas ou tentar novamente a migração.
Tabela em andamento atual	Exibe o nome da tabela que está sendo migrada. Após a migração bem-sucedida, este campo ficará vazio.

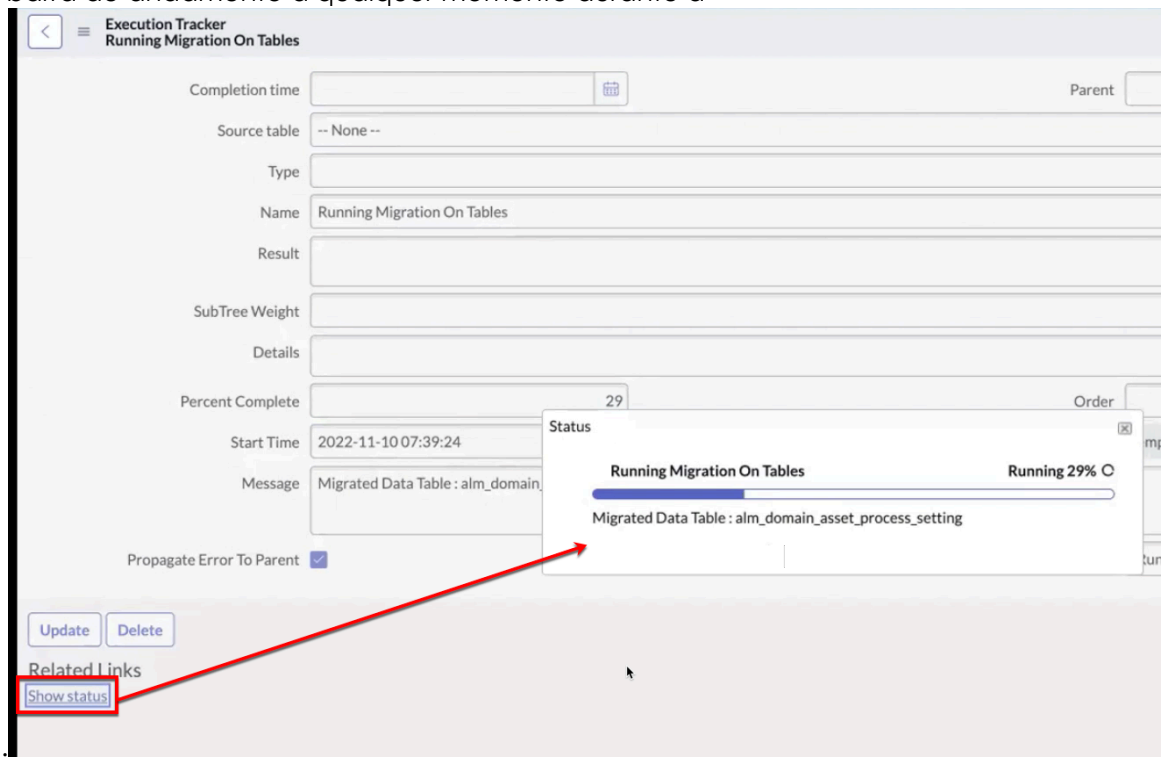
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

12. Selecione o link **Clique aqui** na página Status da ferramenta de migração de domínio para abrir o Rastreador de execução.



Também é possível acessar a tabela *sys_execution_tracker* e procurar por **Migração em execução nas tabelas** para verificar o processo de migração em execução em segundo plano.

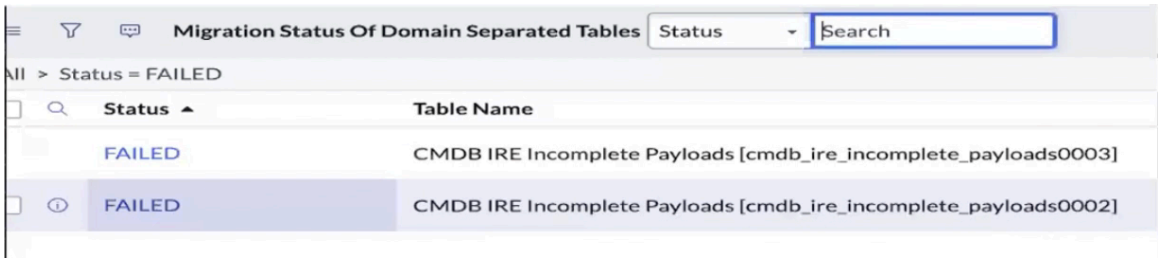
13. Selecione **Mostrar status** na seção Links relacionados para acessar a barra de andamento a qualquer momento durante a migração.



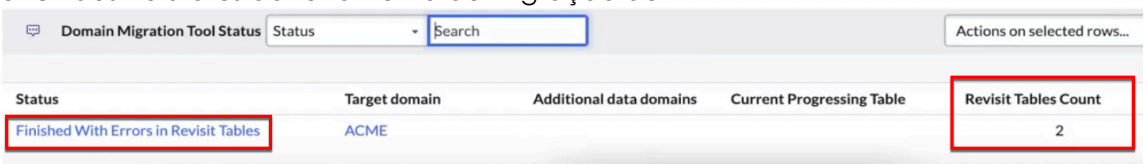
Caso uma tabela falhe na verificação de esquema, o status geral do Status da migração de tabelas separadas por domínio será **Falha**.

Haverá entradas com **Falha** para cada tabela correspondente.

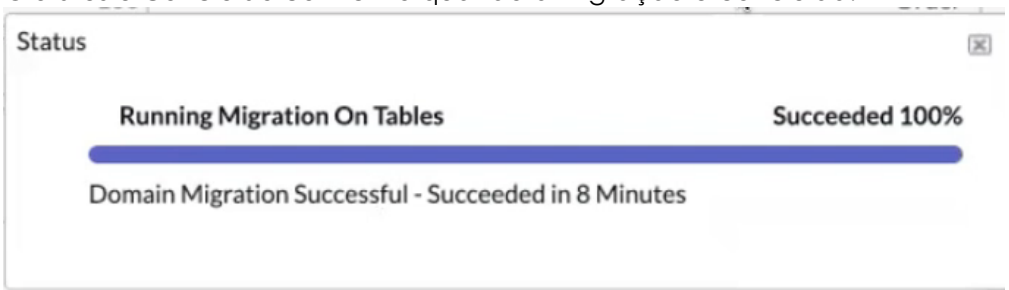
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



O restante da migração continuará e um resumo de todas as tabelas com falha e o número total de **Rever contagem de tabelas** serão preenchidos no Status da ferramenta de migração de domínio.



O **Status** é **Concluído com êxito** quando a migração é concluída.



Administração de processos

A administração de processos permite que os administradores definam políticas específicas de domínio.

As políticas definidas na parte inferior da hierarquia de domínio substituem as políticas definidas na parte superior da hierarquia de domínio. Enquanto em um domínio, os administradores podem definir versões específicas do domínio dessas políticas e configurações globais:

- Scripts de cliente
- Políticas do sistema
- Nomes de aplicações e módulos
- Funções da aplicação
- Filtros de módulo

Aviso: Todos os usuários com a função de administrador têm acesso especial a todos os recursos, funções e dados do sistema porque os administradores podem substituir as regras de ACL e passar em todas as verificações de função. Conceda este privilégio com cuidado.

Quando os usuários têm a função de **administrador**, todas as políticas na instância estão disponíveis para eles, independentemente do domínio atribuído. Eles podem inserir um domínio específico e, em seguida, somente as políticas nesse domínio ou superior serão visíveis e processadas durante uma transação relevante. Quando um administrador modifica uma política que está em um domínio superior ou no domínio global, o sistema

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

cria automaticamente um novo registro para o domínio atual desse administrador. Ele não modifica a política original, a aplicação ou o registro do módulo. Este novo registro substitui o original.

Para fazer mudanças em uma política em um domínio de nível inferior, vá para esse domínio e modifique a política. Esta abordagem cria o registro de política em seu domínio que substitui o registro de política de nível superior.

Não altere a política de nível superior e, em seguida, altere o campo **Domínio** dessa política. Esta abordagem não cria um registro de política no domínio de nível inferior, nem mantém o registro de política para o domínio de nível superior.

O campo **sys_overrides** indica que uma política, aplicação ou módulo em um nível inferior na hierarquia substitui um registro em um nível superior. O sistema define automaticamente este campo quando um administrador tenta modificar uma política, aplicação ou módulo que pertença a outro domínio superior na hierarquia.

Em vez de alterar o registro de nível superior, a tentativa de atualização é alterada para uma inserção e o campo **sys_overrides** é definido para indicar a política de nível superior, a aplicação ou o módulo que está sendo substituído. Posteriormente, quando os registros de uma transação relevante forem carregados, a política, a aplicação ou o módulo específico do domínio será usado em vez do original.

Domínios para administração de processos

Por padrão, a administração de processos sempre usa o domínio do registro para determinar quais políticas aplicar.

O domínio do registro tem precedência sobre o domínio do usuário. Se não houver políticas no domínio do registro, a administração delegada verificará se há políticas no próximo nível mais alto da hierarquia de domínio. A pesquisa de políticas de domínio continua na hierarquia de domínio até atingir o domínio global. Se não houver políticas de domínio inferiores na hierarquia de domínio, a administração de processos usará as políticas para o domínio global.

Por exemplo, Fred Luddy é um usuário no domínio Acme que pode ver registros nos domínios secundários da Acme: Atlanta, Acme: San Diego e Acme: NY. Quando este usuário abre um registro no domínio Acme: San Diego, a administração de processos verifica primeiro se há políticas no domínio Acme: San Diego. Se não houver políticas neste nível da hierarquia de domínio, a administração de processos verificará se há políticas do domínio Acme. Se não houver políticas no domínio Acme, a administração de processos usará as políticas para o domínio global pois não há outros domínios superiores na hierarquia de domínio.

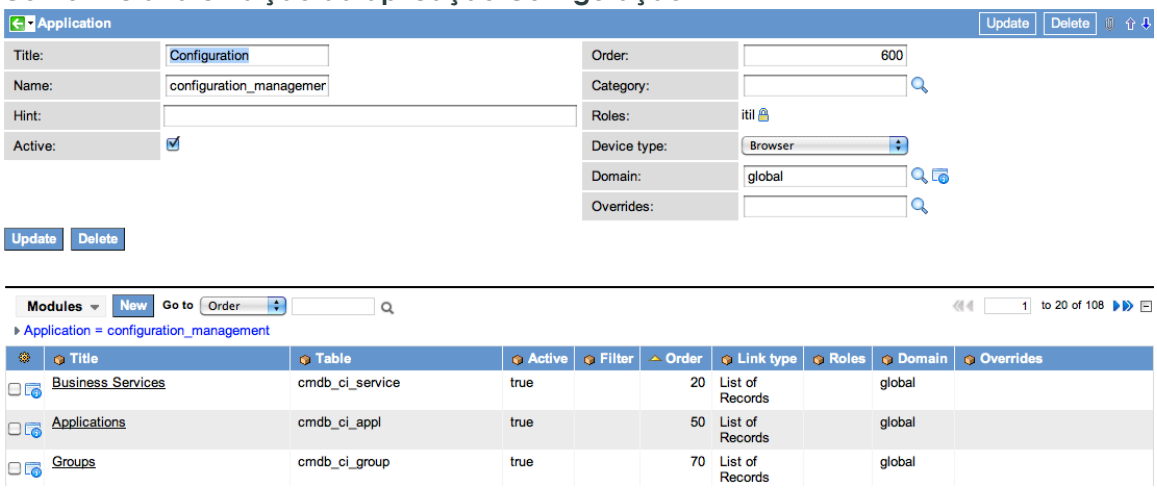
Administração de processos de amostra com aplicações específicas do domínio

O exemplo a seguir ilustra a administração de processos com aplicações e módulos específicos de domínio.

Como administrador do domínio da Oceanic, David Loo decide personalizar a aplicação de configuração. Para começar, David revisa os módulos disponíveis no módulo da aplicação Configuração.

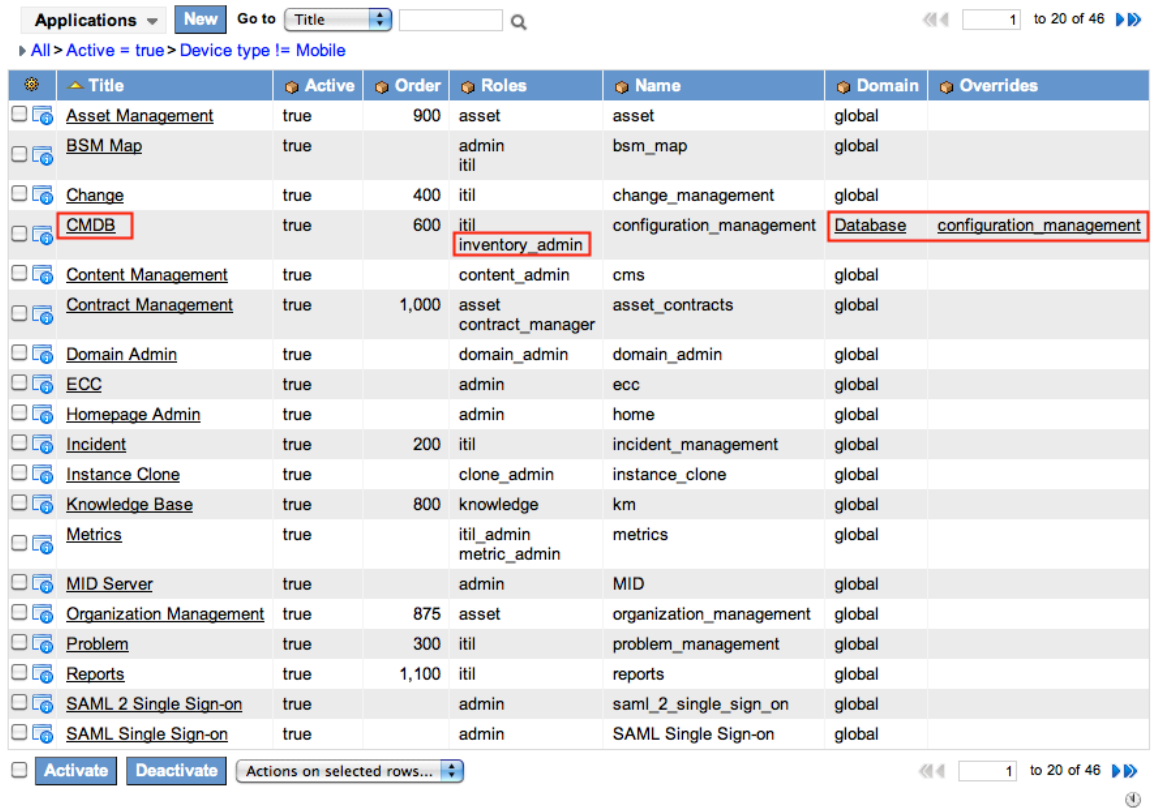
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Como iniciar a exibição da aplicação Configuração



David decide renomear a aplicação de configuração para CMDB e permitir que a função inventory_admin veja a aplicação.

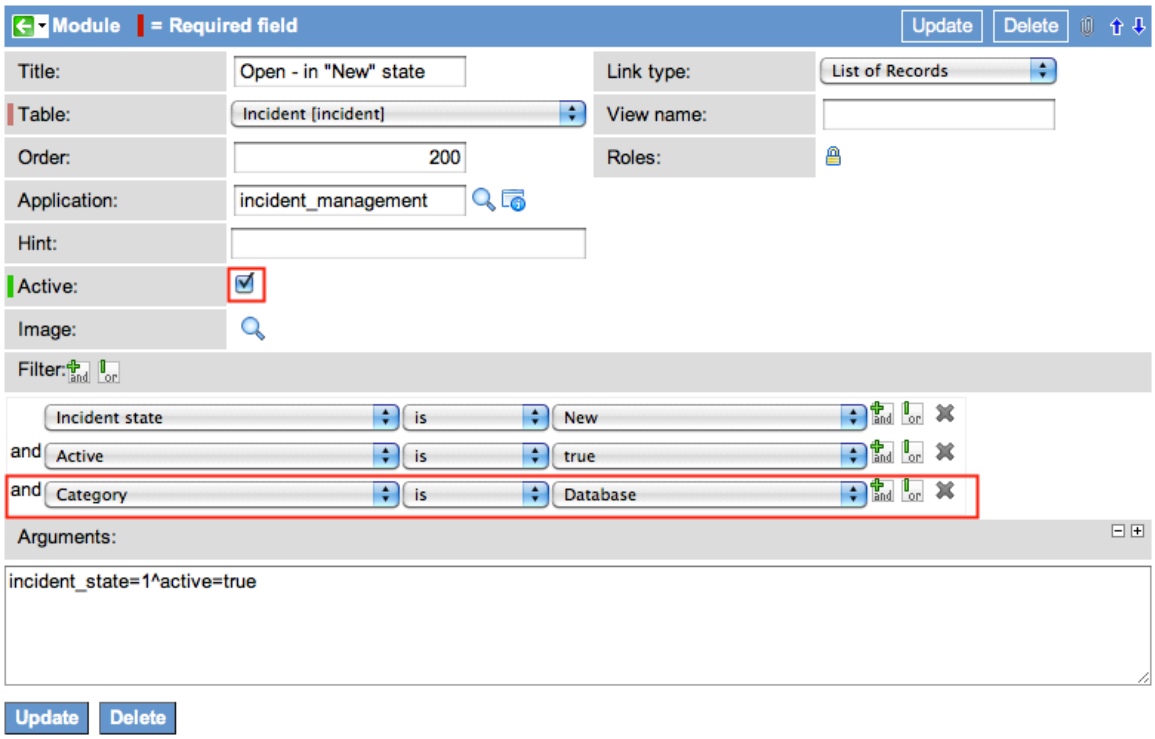
Amostra de mudanças específicas do domínio para a aplicação Configuração



Em seguida, David decide mudar a aplicação Incident ativando o módulo **Aberto - em estado "Novo"** e adicionando um novo item de filtro para mostrar incidentes em aberto na categoria Oceanic.

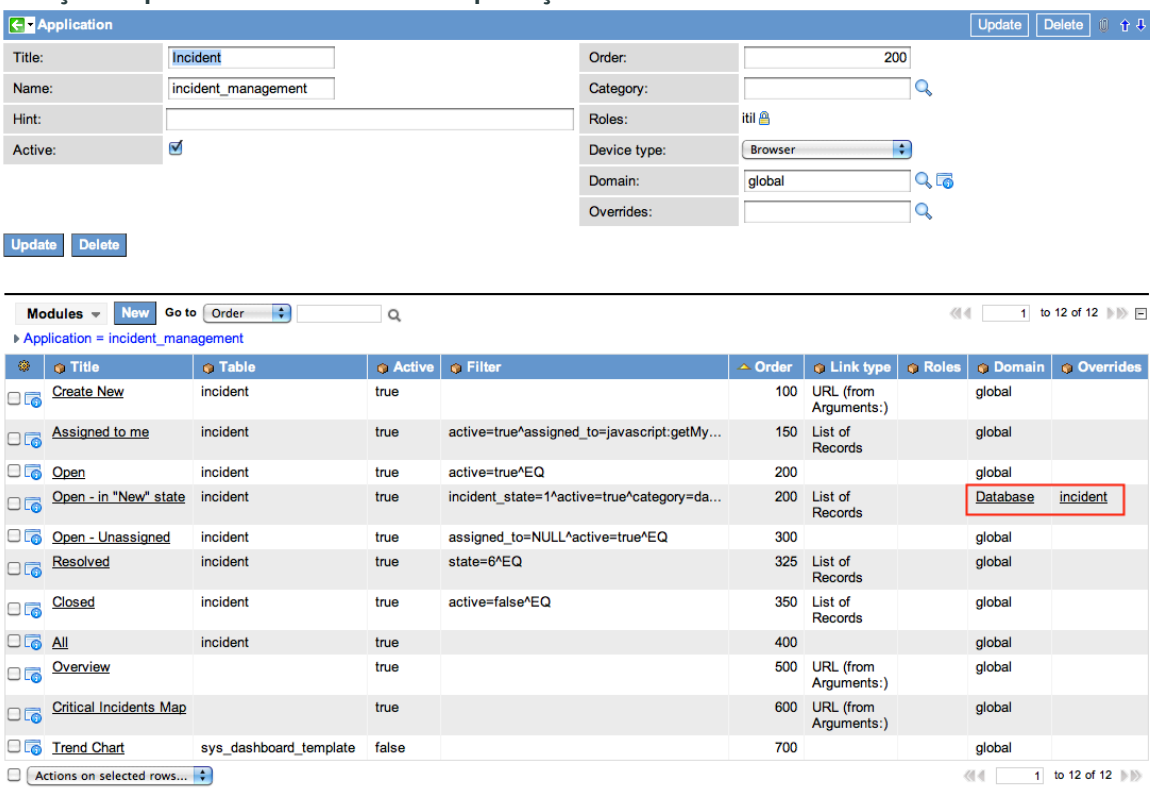
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exemplo de mudanças específicas do domínio para o módulo Aberto - estado "Novo"



Isso cria uma nova entrada de módulo na aplicação em vez de substituir o módulo existente no domínio global.

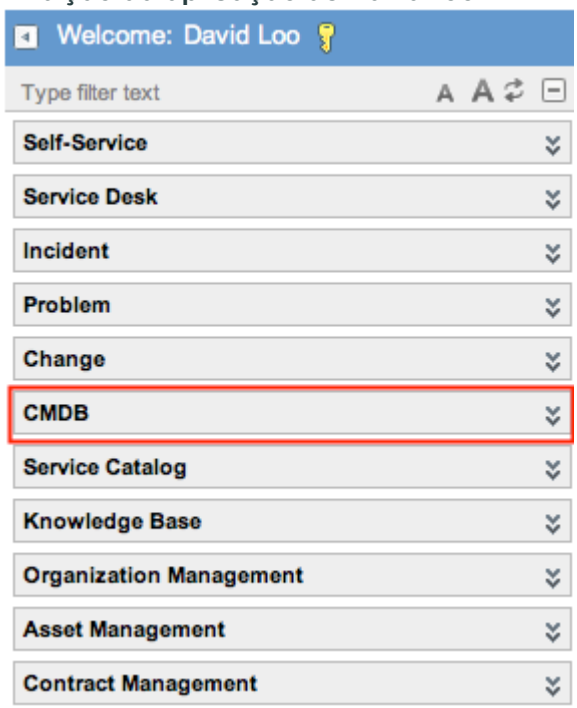
Exibição específica do domínio da aplicação Incident



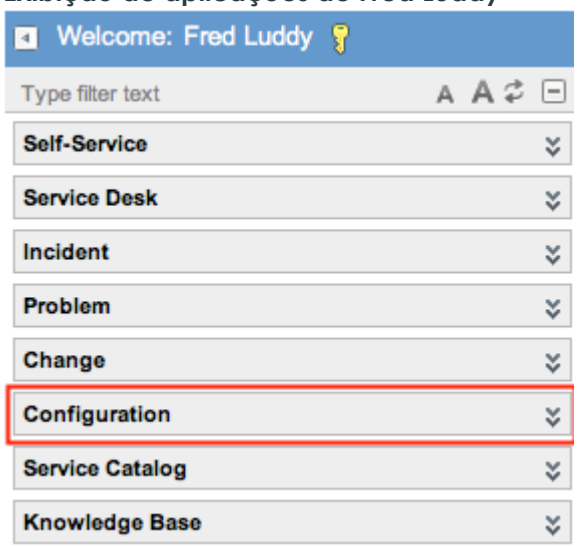
Se outro administrador de outro domínio, como Fred Luddy, fizer login e olhar a aplicação Configuração, as configurações do domínio global serão exibidas.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exibição da aplicação de David Loo



Exibição de aplicações de Fred Luddy



Como habilitar o registro em log de domínio detalhado e mensagens de depuração

O registro em log de domínio e as mensagens de depuração permitem que você solucione problemas de erros de configuração do domínio.

Antes de Iniciar

Função necessária: administrador
Certifique-se de que você é a instância mais recente para melhor desempenho.

Procedimento

1. Na Central de Separação de domínios, navegue até **Administrador de domínio**.
2. Clique em **Configurar Domain Center**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Para **Habilitar registro em log de domínio detalhado**, marque a caixa de seleção **Sim**.
4. Clique em **Atualizar**.

Exibição de uma mensagem de domínio em tempo real

Você pode exibir mensagens de domínio em tempo real dos logs do sistema.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Habilitar registro em log de domínio detalhado: Navegue até **Tudo** > **Administrador do Domínia Central de Separação de domínios** > > **Configurar Domain Center** > **Permitir registro em log de domínio detalhado** > **Sim** (ou defina a propriedade `glide.sys.domain.verbose` para **Verdadeira**).
2. Navegue até **Diagnóstico do sistema** > **Depuração da Sessão** > **Ativar Tudo**.
   Como esta é uma revisão em tempo real, não há necessidade de permitir a execução da sessão de depuração antes de verificar os arquivos de log.
3. Navegue até o console de depuração da sessão para exibir os logs de domínio do sistema detalhados.
4. Pesquise o texto Consulta em relação à tabela.

   Esta consulta encontra mensagens de log neste formato:

```
08:36:43.974: [Domain Paths] Query against table incident restricted by
 domain values [Database Atlanta[db53580b0a0a0a6501aa37c294a2ba6b],
Database[287ee6fea9fe198100ada7950d0b1b73],
Database San Diego[db53a9290a0a0a650091abebccf833c6], global, NY
 DB[5f74727dc0a8010e01efe33a251993f9]]
```

   Neste exemplo, o usuário que visualizou a tabela Incident viu somente os registros correspondentes aos domínios do banco de dados Atlanta, banco de dados, banco de dados San Diego, global e banco de dados de NY.

Exibição de uma mensagem de histórico do domínio

Exiba mensagens de domínio histórico no arquivo de log para solucionar problemas de separação de domínios.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Habilitar registro em log de domínio detalhado: Navegue até **Tudo** > **Administrador do Domínia Central de Separação de domínios** > > **Configurar Domain Center** > **Permitir registro em log de domínio detalhado** > **Sim** (ou defina a propriedade `glide.sys.domain.verbose` para **Verdadeira**).
2. Navegue até **Diagnóstico do sistema** > **Depuração da Sessão** > **Ativar Tudo**.
3. Deixe a sessão de depuração ser executada por um período de tempo, como um dia, antes de verificar os arquivos de log.
4. Navegue até **Logs do sistema** > **Utilitários** > **Download do arquivo de log do nó**.
5. Abra o registro do dia que você deseja exibir.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Os arquivos de log usam o formato de nomenclatura `localhost_log.`<aaaa-mm-dd> .txt .

6. Clique no link relacionado ao log de **Download**.
7. Abra o arquivo de log baixado em um editor de texto e pesquise mensagens de log com o seguinte formato:

   Consulta em relação à tabela incident restrita por valores de domínio `[global, Software [8a4dde73c6112278017a6a4baf547aa7]]`

   Neste exemplo, um usuário viu somente registros da tabela Incident que correspondiam aos domínios global e de Software.

Solução de problemas de erros da separação de domínios

Se você encontrar problemas da Separação de domínios, revise esta lista de soluções.

Erro ou sintoma	Solução
Um sys_id de domínio aponta para um domínio não existente	Este erro ocorre quando um registro de dados, como um usuário ou um registro de tarefa, tem um valor de coluna `sys_domain` cujo `sys_id` não existe na tabela de domínio atual. O domínio `sys_id` pode ter sido excluído acidentalmente ou pode se referir a uma tabela de domínio anterior se você alterou a tabela de domínio. Para corrigir o erro, abra uma lista da tabela que contém o erro e filtre o valor `sys_domain` inválido. Em seguida, insira manualmente o valor `sys_domain` correto ou remova-o. **Nota:** Você pode ter `sys_ids` de domínio inválido em qualquer tabela que faça referência à tabela de domínio. Por exemplo, IDs de domínio inválidas podem ocorrer nas tabelas Domínio de visibilidade do usuário `[sys_user_visibility]`, Domínio de visibilidade do grupo `[sys_user_group_visibility]` e Domínio contido `[domain_contains]`.
Um caminho de domínio ou número de domínio sys_id aponta para o domínio incorreto	Este erro ocorre quando uma consulta de número de domínio ou de caminho de domínio está fora de sincronia com o nome de domínio real. Este erro pode ocorrer com números de domínio quando adicionar domínios requer renumeração ou durante a conversão de números de domínio em caminhos de domínio. Para corrigir o erro, verifique os resultados em Central de Separação de domínios. Se o erro persistir, você poderá editar manualmente o valor das colunas `sys_domain_path` ou `sys_domain_number` para apontar para o domínio apropriado.
A estrutura da árvore do domínio está corrompida	Este erro ocorre se houver uma série de relacionamentos de domínio que criam um loop infinito entre os domínios. Para corrigir o erro, abra uma lista da tabela de domínio e edite manualmente os valores do domínio "contém" para não formar um loop.

Central de Separação de domínios

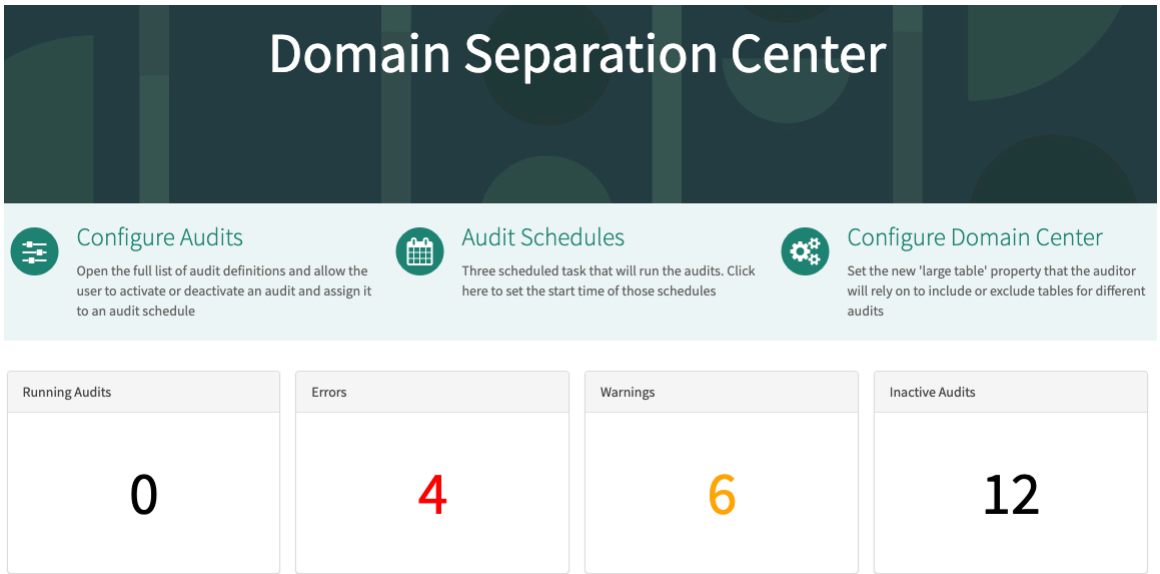
Audite seus domínios regularmente para revelar problemas.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Visão geral

A Central de Separação de domínios é um painel onde você pode programar e configurar auditorias para todos os domínios armazenados na tabela domain_audit_definition. O painel permite que você revise os resultados da auditoria e se aprofunde nos erros e avisos do domínio. Você pode encontrar o painel da Central de Separação de domínios em `<ServiceNow-instance-name>/domaincenter`.

A Central de Separação de domínios fornece várias auditorias. Você não pode criar a sua própria. Você pode, no entanto, configurar a frequência de execução. As auditorias são executadas em todos os domínios armazenados na tabela domain_audit_definition.



Configuração de auditorias

Você pode configurar se uma auditoria está ativa e com que frequência ela é executada.

1. Na Central de Separação de domínios, selecione **Configurar auditorias**.

   A página **Configurar auditorias é** exibida.

2. Configure cada auditoria que você deseja ativar. As auditorias estão inativas por padrão.
   a. Selecione uma auditoria.
   b. Marque a caixa **Ativa** para ativar a auditoria.
   c. Especifique a frequência de execução da auditoria no campo **Frequência**.

      A Central de separação de domínios executa todas as auditorias marcadas com a mesma frequência ao mesmo tempo. Não selecione **Diariamente** para auditorias executadas em tabelas grandes.

   d. Repita essas etapas para cada auditoria que você deseja ativar.
3. Selecione **Salvar**.

Cronogramas de auditorias

Configure uma ou mais auditorias para serem executadas diariamente, semanalmente ou mensalmente. O programador especifica em que dias e horas executar essas auditorias. Todas as auditorias com a mesma frequência de programação são executadas sequencialmente a partir do horário configurado.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

1. Na Central de Separação de domínios, selecione **Cronogramas de auditorias**.

   A página **Programação de auditoria** é exibida.

2. Configure os cronogramas de auditorias.
   a. Selecione um nome de programação.
   b. Especifique a hora do dia para executar a auditoria.

      As unidades de tempo são medidas com o relógio de 24 horas, ou seja, 14 é igual a 2 PM.

   c. Para cronogramas semanais, selecione o dia da semana para executar a auditoria, em que 1 é o domingo.
   d. Para cronogramas mensais, selecione o dia do mês para executar a auditoria.
   e. Repita o procedimento para os outros cronogramas.
3. Selecione **Salvar** para salvar as mudanças de configuração.
4. Selecione **Executar agora** para executar todas as auditorias programadas para execução na frequência mostrada na parte superior do painel direito, por exemplo, se o título do painel for **Programação de auditoria de domínio - Diariamente**, todas as auditorias executadas diariamente serão executadas.

Para ver o status de uma auditoria em execução, na Central de Separação de domínios, selecione o número na caixa **Auditorias em execução**.

Execução de auditorias imediatamente

As auditorias normalmente são executadas conforme programado. Você pode, no entanto, executar todas as auditorias sob comando.

1. Na Central de Separação de domínios, selecione **Cronogramas de auditorias**.

   A página **Programação de auditoria** é exibida.

2. Selecione o nome da programação de auditoria que você deseja executar, por exemplo, diária, semanal ou mensal.
3. Selecione **Executar agora**.

Para ver o status de uma auditoria em execução, na Central de Separação de domínios, selecione o número na caixa **Auditorias em execução**.

Configuração da Central de Separação de domínios

1. Na Central de Separação de domínios, selecione **Configurar Domain Center**.
2. Na página **Configurar Domain Center**, para **Habilitar registro em log de detalhes no domínio**, selecione **Sim** para armazenar logs detalhados que ajudam a diagnosticar problemas relacionados ao domínio. O registro em log detalhado pode causar problemas de desempenho.

   Esses logs se referem aos logs do lado do servidor na tabela syslog_domain. Para obter informações sobre como exibir os logs, consulte Exibir auditorias com avisos e falhas.

3. No slushbucket, selecione e mova todas as suas tabelas grandes para a coluna **Selecionada**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

As auditorias diárias não devem ser executadas em tabelas grandes. Os nomes de tabelas esmaecidos na coluna **Selecionada** são grandes e não podem ser movidos para a coluna **Disponível**.

4. Selecione **Atualizar**.

Exibição de auditorias com avisos e falhas

No painel, **Erros** e **Avisos** fornecem informações detalhadas sobre auditorias que encontraram problemas. Os logs relacionados ao domain separation residem no servidor na tabela syslog_domain.

1. Na Central de Separação de domínios, selecione o número na caixa **Erros** ou **Avisos**.

   A página **Erros** ou **Avisos** é exibida, respectivamente.

2. Selecione uma das auditorias na lista.

   A página exibe informações detalhadas sobre problemas com a auditoria selecionada. As mensagens em **Detalhes do resultado da auditoria** se referem aos valores na tabela syslog_domain para auditorias de tabela que revelaram erros ou avisos.

3. Para ver os logs no servidor que fornecem informações sobre auditorias de aviso ou erro:
   a. Copie o valor de **ID de detalhe** no painel esquerdo de um aviso ou erro.
   b. No Navegador de filtros do HI, insira *syslog_domain.do*.

      A página Log de domínio é exibida.

   c. No campo de pesquisa **Origem**, insira `=<Detail-ID>` (sem espaço após o sinal de igual), por exemplo, =f6a00fd29a85b300a9503a81b9169678.

      A página Log de domínio exibe somente os logs relacionados à auditoria com a ID de detalhe que você especificou. Cada linha na tabela especifica um registro diferente no qual a auditoria encontrou problemas. Observe que o campo **Mensagem** nesta página corresponde aos valores exibidos na coluna **Mensagem** do Domain Service Center. O formato da mensagem corresponde ao tipo de auditoria.

4. Selecione:
   - **Executar auditoria novamente**— Execute uma auditoria novamente para ver se ela ainda encontra um aviso ou erro.
   - **Desativar auditoria**— Desative uma auditoria.
   - **Copiar detalhes**— Copia os detalhes da auditoria para a área de transferência.

Exibição de auditorias em execução e pendentes

As auditorias ativas são executadas periodicamente ou na fila para execução, conforme programado. Você pode exibir o status à medida que são executadas.

1. Selecione o número na caixa **Auditorias em execução** para exibir as auditorias que estão em execução no momento ou com execução pendente.

   A página **Auditorias em execução** é exibida.

2. Selecione uma auditoria para obter mais informações sobre ela.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Visualização de auditorias inativas

1. Selecione o número na caixa **Auditorias inativas**.

   A página **Auditorias inativas** exibe todas as auditorias que estão desativadas no momento.

2. Selecione uma das auditorias para exibir mais informações sobre ela.
3. Para ativar uma auditoria, selecione a caixa **Ativa** e use o campo **Frequência** para especificar a frequência de execução da auditoria.
4. Selecione **Atualizar**.

Configuração da Central de separação de domínios

Especifique quais tabelas em domínios são grandes e se você deseja registro em log detalhado.

Antes de Iniciar

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

Você pode programar auditorias para execução diária, semanal ou mensal. As auditorias executadas em tabelas grandes podem levar um tempo significativo. Por esse motivo, evite executar auditorias diárias em tabelas grandes. Iniciar uma nova auditoria em uma que está levando mais de um dia para ser executada pode ter consequências negativas.

O registro em log detalhado pode fornecer mais informações sobre os problemas encontrados durante as auditorias, no entanto, pode causar problemas de desempenho.

Procedimento

1. Na Central de separação de domínios, selecione **Configurar Domain Center**.
   A página Configurar Domain Center é exibida.
2. Selecione **Sim** para **Habilitar registro em log detalhado do domínio**, para armazenar logs detalhados que ajudam a diagnosticar problemas relacionados ao domínio.
   Esses logs se referem aos logs do lado do servidor na tabela de Log do domínio [syslog_domain]. Para obter informações sobre como exibir os logs, consulte a seção Exibir auditorias com avisos e falhas.
3. Na lista, mova todas as suas tabelas grandes para a coluna **Selecionada**.
   As auditorias diárias não devem ser executadas em tabelas grandes. Os nomes de tabelas esmaecidos na coluna **Selecionada** são grandes e não podem ser movidos para a coluna **Disponível**.
4. Selecione **Atualizar**.
5. Se você tiver tabelas grandes que nunca devem ser auditadas, defina a propriedade do sistema *com.glide.domain.audit.big_tables.additional* como uma lista separada por vírgulas desses nomes de tabela.

Configuração de auditorias

Configure se uma auditoria está ativa e com que frequência ela é executada.

Antes de Iniciar

Função necessária: administrador

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Na Central de separação de domínios, clique em **Configurar auditorias**.
   T será exibido.
2. Na página Configurar auditorias, configure cada auditoria que você deseja ativar.
   As auditorias estão inativas por padrão.

   a. Clique em uma auditoria.

   b. Clique na caixa de seleção **Ativa** para ativar a auditoria.

   c. Especifique a frequência de execução da auditoria no campo **Frequência**.
   A Central de separação de domínios executa todas as auditorias marcadas com a mesma frequência ao mesmo tempo. Não selecione **Diariamente** para auditorias executadas em tabelas grandes.

   d. Repita as etapas a-c para cada auditoria que você deseja ativar.

3. Clique em **Salvar**.

Programação de auditorias

Especifique a hora e o dia em que as auditorias são executadas.

Antes de Iniciar

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

Foram configuradas uma ou mais auditorias para serem executadas diariamente, semanalmente ou mensalmente. O programador especifica em que dias e horas executar essas auditorias. Todas as auditorias com a mesma frequência de programação são executadas sequencialmente a partir do horário configurado.

Procedimento

1. Na Central de Separação de domínios, clique em **Cronogramas de auditorias**.
   A página Programação de auditoria é exibida.
2. Configure os cronogramas de auditorias.

   a. Clique em um nome de programação.

   b. Especifique a hora do dia para executar a auditoria.
   As unidades de tempo usam o relógio de 24 horas (ou seja, 14 é igual a 2 PM).

   c. Para cronogramas semanais, selecione o dia da semana para executar a auditoria, em que 1 é o domingo.

   d. Para cronogramas mensais, selecione o dia do mês para executar a auditoria.

   e. Repita o procedimento para os outros cronogramas.

3. Clique em **Salvar** para salvar as mudanças de configuração.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Opcional: Clique em **Executar agora** para executar todas as auditorias programadas para execução na frequência mostrada na parte superior do painel direito.
   Por exemplo, se o título do painel for **Programação de auditoria de domínio - Diariamente**, **Executar agora** executará imediatamente todas as auditorias programadas para execução diária.

O que Fazer Depois
Para ver o status de uma auditoria em execução, na Central de Separação de domínios, clique no número na caixa **Auditorias em execução**.

Execução de auditorias imediatamente

As auditorias normalmente são executadas conforme programado. Você pode, no entanto, executar todas as auditorias sob comando.

Antes de Iniciar
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa
Você não pode executar auditorias individuais manualmente. Você pode, no entanto, executar todas as auditorias configuradas com a mesma frequência de programação. Por exemplo, você pode executar todas as auditorias configuradas para serem executadas diariamente.

Procedimento

1. No Centro de Separação de domínios, clique em **Cronogramas de auditorias**.
2. Clique no nome da programação de auditoria que você deseja executar (por exemplo, diária, semanal ou mensal).
3. Clique em **Executar Agora**.

O que Fazer Depois
Para ver o status de uma auditoria em execução, no Centro de Separação de domínios, clique no número na caixa **Auditorias em execução**.

Exibição de auditorias com avisos e erros

a Central de Separação de domínios fornece detalhes sobre erros e avisos de auditoria.

Antes de Iniciar
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa
No painel Central de Separação de domínios, **Erros** e **Avisos** fornecem informações detalhadas sobre auditorias que encontraram problemas. Os logs relacionados ao Domain Separation residem no servidor na tabela syslog_domain. Erros são problemas que requerem atenção imediata. Avisos não levam a falhas, mas apresentam práticas recomendadas, por exemplo, não tornar o nome de domínio muito longo.

Procedimento

1. Na Central de Separação de domínios, clique no número na caixa **Erros** ou **Avisos**.
   A página **Erros** ou **Avisos** é exibida.
2. Clique em uma das auditorias na lista.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A página exibe informações detalhadas sobre problemas com a auditoria selecionada. As mensagens em **Detalhes do resultado da auditoria** se referem aos valores na tabela syslog_domain no servidor para auditorias de tabela que revelaram erros ou avisos.

3. Para ver os logs no servidor que fornecem informações sobre auditorias de aviso ou erro:

   a. Copie o valor de **ID de detalhe** no painel esquerdo de um aviso ou erro.

   b. Na instância que executa a Central de Separação de domínios, no **Navegador de filtros**, insira *syslog_domain.list*.
   A página Log de domínio é exibida.

   c. No campo de pesquisa da coluna **Origem**, insira `=<Detail-ID>` (sem espaço após o sinal de igual), por exemplo, `=f6a00fd29a85b300a9503a81b9169678`.
   A página Log de domínio exibe somente os logs relacionados à auditoria com a ID de detalhe que você especificou. Cada linha na tabela especifica um registro diferente no qual a auditoria encontrou problemas. Observe que o campo **Mensagem** nesta página corresponde aos valores exibidos na coluna **Mensagem** do Domain Service Center. As informações incluídas na mensagem correspondem ao tipo de auditoria.

4. Opcional: Selecione uma das seguintes propriedades:
   - **Executar auditoria novamente**— Execute uma auditoria novamente para ver se ela ainda encontra um aviso ou erro.
   - **Desativar auditoria**— Desative uma auditoria.
   - **Copiar detalhes**— Copia os detalhes da auditoria para a área de transferência.

Exibição de resultados em execução e pendentes

Você pode exibir auditorias em execução e pendentes para ver seu status.

Antes de Iniciar
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa
As auditorias ativas são executadas periodicamente ou na fila para execução, conforme programado. Você pode exibir o status à medida que são executadas.

Procedimento

1. Clique no número na caixa **Auditorias em execução** para exibir as auditorias que estão em execução no momento ou com execução pendente.
   A página Auditorias em execução aparece.
2. Clique em uma auditoria em execução ou pendente para ver informações sobre ela.

Visualização de auditorias inativas

Você pode exibir todas as auditorias inativas em um lugar e, opcionalmente, ativá-las.

Antes de Iniciar
Função necessária: administrador

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Clique no número na caixa **Auditorias inativas**.
   A página Auditorias inativas exibe todas as auditorias que estão desativadas no momento.
2. Clique em uma das auditorias para exibir mais informações sobre ela.
3. Opcional: Ative uma auditoria ao clicar na caixa **Ativa** e especificar a frequência de execução da auditoria no campo **Frequency**.
4. Clique em **Atualizar**.

Autenticação

A autenticação do ServiceNow® valida a identidade de um usuário que acessa uma instância e, em seguida, autoriza o usuário a recursos que correspondem à função do usuário ou à função de trabalho.

Primeiros passos

Single Sign-on (SSO) para vários provedores

Nome de usuário e senha configurados em provedores de identidade, que têm uma conta de usuário correspondente no banco de dados.

Entrada e saída do OAuth

A autenticação baseada em OAuth valida a identidade do cliente que tenta estabelecer uma relação de confiança no sistema usando um protocolo de autenticação.

Política de acesso de API

A política de acesso de API define as permissões e o acesso a uma API que pode ser controlada por meio de uma política.

Autenticação do token Digest

Nome de usuário e segredo na tabela, executa uma operação de hash que é específica do usuário, como SHA1, SHA 256 ou MD5. Esse valor deve ser anexado como parte do sufixo do URL, que funciona no parâmetro de consulta.

Autenticação com limite de tempo

Autenticação multifator (MFA)

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configure a autenticação baseada em links na instância ServiceNow. O link configurado pode ser compartilhado por e-mail ou SMS com o usuário, permitindo que utilize esses links para fazer login na instância.

A MFA permite que você forneça o segundo nível de autenticação, o que inclui o uso de senha de um app de autenticação, chave de hardware, autenticador biométrico, SMS ou e-mail.

Autenticação baseada em certificados

Certificados codificados por PEM exclusivos mapeados para usuários, em vez de nome de usuário e senha, para autenticação baseada em certificados.

Registro de autoatendimento

Use o registro pelo próprio usuário externo para integrar um grande volume de usuários externos em sua instância.

LDAP

Faça a integração com um diretório LDAP (Lightweight Directory Access Protocol) para simplificar o processo de login do usuário

Você pode usar vários métodos diferentes para autenticar usuários. As credenciais do usuário são correspondidas a diferentes credenciais salvas para cada método.

Nota:

- O plug-in SSO Okta foi descontinuado.
- Para saber mais sobre as propriedades de segurança que afetam o processamento de autorização, consulte Controle de acesso em Configurações de proteção de segurança da instância.
- Você pode usar o SAML e a Autenticação Digest por meio da aplicação Multiple Provider SSO.

Autenticação adaptável

Use a estrutura de política de autenticação adaptável para impor controles de autenticação contextual aos usuários certos no momento certo. A autenticação adaptável usa políticas de autenticação para avaliar as solicitações de autenticação e negar ou permitir o acesso à sua instância com base nas condições de política especificadas.

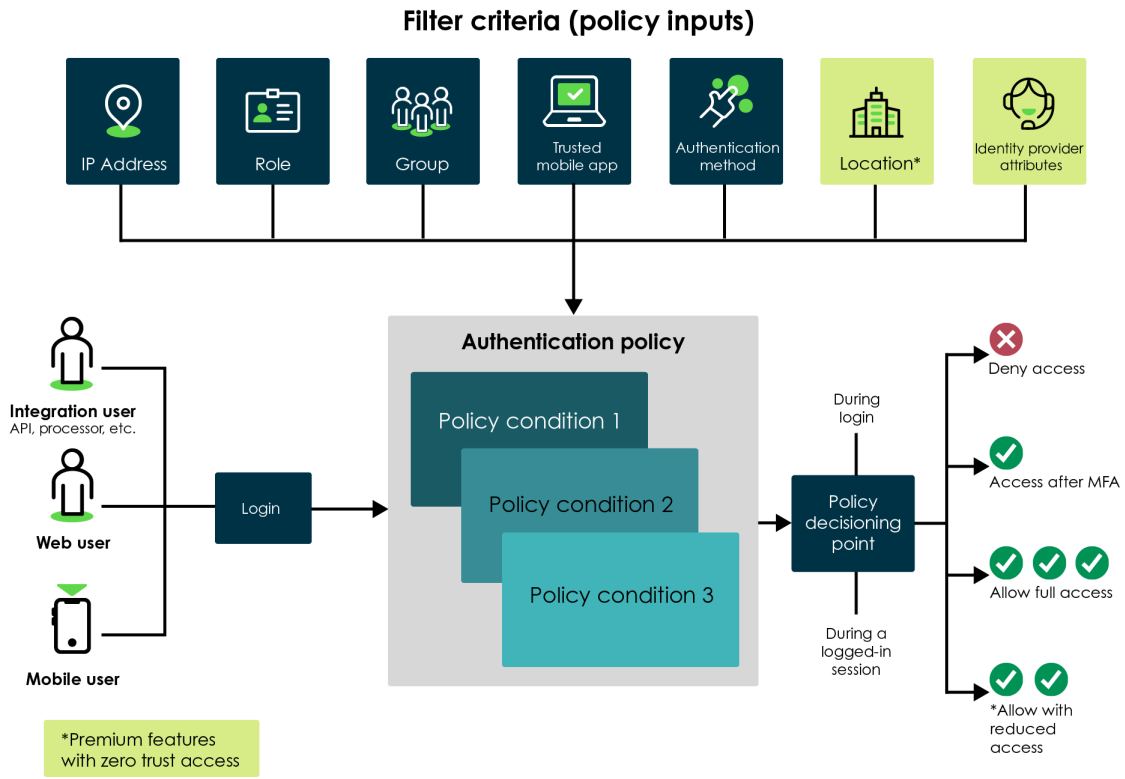
Use as políticas e contextos de autenticação adaptável para restringir o acesso de usuários e APIs com base em critérios como endereço IP, função do usuário e grupo de usuários à

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

sua instância. Você pode configurar as políticas de autenticação internas de acordo com seus requisitos de segurança.

Por exemplo, um administrador pode configurar *Allow Access Policy* para permitir logins de usuários somente dentro de um intervalo confiável de endereços IP e que sejam membros de uma função específica. Quando atribuída a *Post-authentication context*, a política de acesso nega o acesso de endereços IP não confiáveis.

Para definir uma mensagem personalizada no idioma da sua instância, você precisa adicionar a chave, o par de valores em `sys_ui_message.list` e atualizar o registro `sys_ui_message`. Ao fazer login com uma senha incorreta, a mensagem personalizada no idioma preferencial será exibida.



Componentes da autenticação adaptável

Políticas de autenticação

As políticas de autenticação avaliam as solicitações de autenticação com base nas condições de política especificadas e permitem ou negam o acesso, dependendo da saída da avaliação das condições de política. Por exemplo, o acesso será permitido somente se todas as condições de política especificadas na **Política de permissão de acesso** forem avaliadas como verdadeiras.

As políticas de autenticação usam as informações fornecidas pelos critérios de filtro para comparar com as condições da política a fim de determinar se o acesso à instância deve ser concedido. Por exemplo, um critério de filtro fornece o endereço IP de um usuário; logo, uma condição de política determina se este endereço está dentro do intervalo específico antes de conceder acesso. Saiba mais sobre políticas de autenticação em Políticas de autenticação.

Contextos da política de autenticação

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Os contextos da política de autenticação definem como e quando as políticas são aplicadas durante o processo de login. O contexto de pré-autenticação é executado antes que uma tela de login seja mostrada ao usuário O contexto de pós-autenticação é executado depois que o usuário insere as credenciais. Para usar uma política, ela deve ser atribuída a um contexto de política. Para obter detalhes sobre esses contextos, consulte Contextos da política de autenticação.

Critérios de filtro

Os critérios de filtro (também chamados de entradas de política) são usados como entradas para as condições de política. As condições de política usam essas entradas para verificar e atender aos requisitos das solicitações de autenticação. Essas entradas fornecem informações como função do usuário, intervalo de IP e provedor de identidade. Para obter mais detalhes sobre os critérios de filtro, consulte Critérios de filtro.

Propriedades da autenticação

Use as propriedades da autenticação para controlar se a autenticação adaptável está ativa em sua instância. Você também pode usar as propriedades para habilitar a depuração e definir as mensagens que os usuários veem quando o acesso é bloqueado. Para obter detalhes sobre estas propriedades, consulte Como configurar as propriedades da autenticação adaptável.

Políticas de acesso de REST API

Você pode usar os critérios de filtro da estrutura de autenticação adaptável para restringir o acesso a REST APIs ServiceNow de entrada. Para obter mais informações, consulte Políticas de acesso de REST API.

Separação de domínio e autenticação adaptável

A autenticação adaptável é compatível com instâncias separadas por domínio no nível de condição da política de autenticação. As condições da política afetam o domínio no **Domínio** de registros no campo [sys_domain]. As condições de política no domínio global afetam todos os domínios.

Eventos de autenticação adaptável

É possível usar a tabela de eventos de autenticação adaptável para saber sobre os eventos que ocorreram especificamente em relação ao recurso de autenticação adaptável. Para obter mais informações, consulte Eventos de autenticação adaptável.

Como ativar a autenticação adaptável

Você pode ativar o plug-in Adaptive Authentication (com.snc.adaptive_authentication) para a Autenticação adaptável se tiver a função de administrador.

Antes de Iniciar

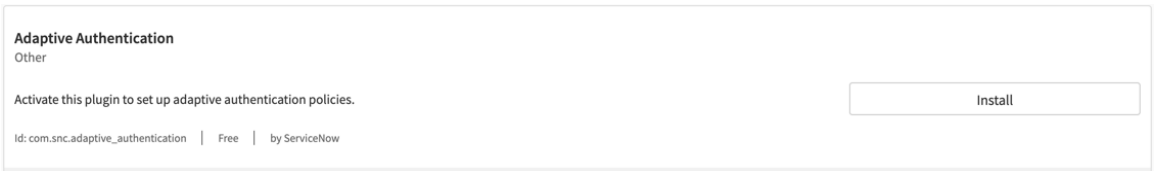
Função necessária: administrador

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

Procedimento

1. Navegue até **Todos** > **Aplicações do sistema** > **Todas as aplicações disponíveis** > **Todas**.
2. Busque pelo plug-in **Autenticação adaptável** (com.snc.adaptive_authentication) usando o critério de filtro e a barra de pesquisa.



   Pesquise o plug-in pelo nome ou ID. Se não conseguir encontrar um plug-in, talvez seja necessário solicitá-lo ao pessoal ServiceNow.

3. Selecione **Instalar** para iniciar o processo de instalação.

   Nota: Quando a separação de domínio e o administrador delegado estão habilitados em uma instância, o usuário administrativo deve estar no domínio **global**. Caso contrário, será exibido o seguinte erro: `A instalação da aplicação não está disponível porque há outra operação em execução: ativação de plug-in para <plugin name>.`

   Você verá uma mensagem após a conclusão da instalação.

O que Fazer Depois

Configure suas políticas de autenticação para aplicar controles de autenticação contextual em sua instância.

Depois que suas políticas estiverem configuradas: Habilite a autenticação adaptável usando a política **Habilitar política de autenticação**. Para obter mais detalhes sobre as propriedades de autenticação adaptável, consulte Como configurar as propriedades da autenticação adaptável.

Critérios de filtro

Os critérios de filtro (também chamados de entradas de política) são usados como entradas para as condições de política a fim de verificar e atender aos requisitos de uma solicitação de autenticação.

Use critérios de filtro para fornecer políticas de autenticação de informações, como endereço IP, funções ou grupos de um usuário. Adicione esses critérios na seção **Condições da política** de suas políticas.

Existem sete tipos de critérios de filtro usados na autenticação adaptável. Suas políticas de autenticação podem usar um ou mais desses critérios para avaliar as solicitações de autenticação.

Tipos de critérios de filtro

Tipo	Descrição
Critério de filtragem de IP	Filtra usuários com base nos endereços IP do usuário. IPv4 e IPv6 são compatíveis.
Critérios de filtro por função	Use os critérios de filtro para filtrar usuários com base em suas funções.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tipos de critérios de filtro

Tipo	Descrição
Critérios de filtro por grupo	Filtra usuários com base no grupo de usuários que pertence.
Critérios para filtro de local	Use os critérios para filtro de local para filtrar usuários com base na localização deles.
Critérios de filtro de atributos do provedor de identidade	Use os atributos do Provedor de Identidade que são recebidos da resposta SAML do IdP como um critério de filtro para autenticação.

Critérios genéricos

Além dos tipos listados anteriormente, há quatro critérios de filtro genéricos. Esses critérios não aparecem no navegador de filtros, mas você pode selecioná-los ao adicionar entradas de política às suas políticas de autenticação.

Tipos de critérios de filtro genéricos

Tipo	Descrição
Esquema de autenticação	Use para filtrar com base no esquema de autenticação do usuário. Esse critério tem duas opções de seleção: • Nome de usuário e senha, o que denota um login local • SSO, que denota um login baseado em Multi-SSO (SAML, OIDC ou Digest). **Nota:** Esse critério de filtro está disponível somente quando o plug-in **Integration - Multiple Provider Single Sign-On Installer**[com.snc.integration.sso.multi.installer] estiver instalado.
Provedor de identidade	Use para filtrar com base no provedor de identidade do usuário. Use-o juntamente com os critérios do esquema de autenticação para ter controle granular sobre o processo de login. Esse critério é uma referência à tabela **Provedores de identidade** [sso_properties]. **Nota:** Esse critério de filtro está disponível somente quando o plug-in **Integration - Multiple Provider Single Sign-On Installer**[com.snc.integration.sso.multi.installer] estiver instalado.
MFA baseada em função	Use para filtrar com base no recurso de MFA baseada em função. Esse critério é um critério de filtro do tipo booliano que indica se a MFA baseada em função está habilitada para o usuário.
MFA baseada no usuário	Use para filtrar com base no recurso de MFA baseada no usuário. Esse critério é um critério de filtro do tipo booliano que indica se a MFA baseada no usuário está habilitada para o usuário.
aplicativo para celular Trusted	Filtro de aplicativo Trusted Mobile para habilitar o acesso do app pela instância.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Filtro de IP

Use critérios de filtro IP para filtrar os usuários com base nos endereços IP deles. IPv4 e IPv6 são compatíveis.

Os critérios de filtro por IP permitem filtrar usuários com base nos endereços IP do usuário. Você pode configurar uma política de autenticação para permitir ou negar acesso a um endereço específico ou intervalo de endereços.

Como criar critérios de filtro por IP

Os critérios de filtro por IP permitem filtrar usuários com base nos endereços IP do usuário. Você pode configurar uma política de autenticação para permitir ou negar acesso a um endereço específico ou intervalo de endereços.

Antes de Iniciar

Função necessária: administrador

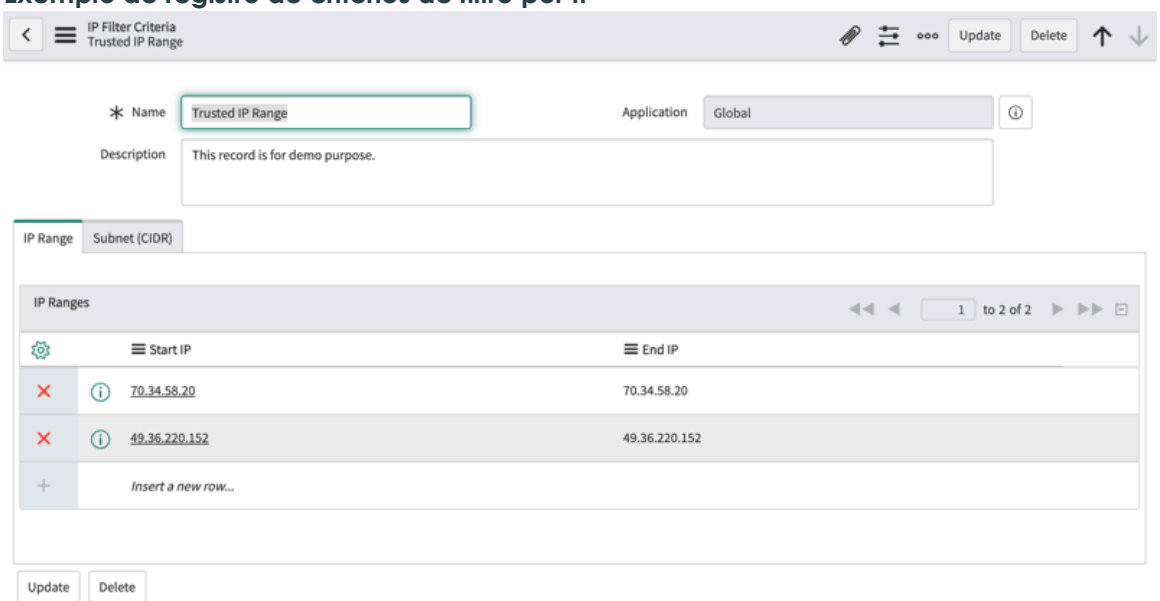
Procedimento

1. Navegue até **Todos** > **Autenticação adaptável** > **Critérios de filtro** > **Critérios de filtro por IP**.
2. Clique em **Novo**.
3. No formulário, preencha os seguintes campos.

Formulário de critérios de filtro por IP

Campo	Descrição
Nome	Nome para identificar a rede IP.
Descrição	Descrição resumida da rede IP.
Aplicação	Escopo da aplicação.

Exemplo de registro de critérios de filtro por IP



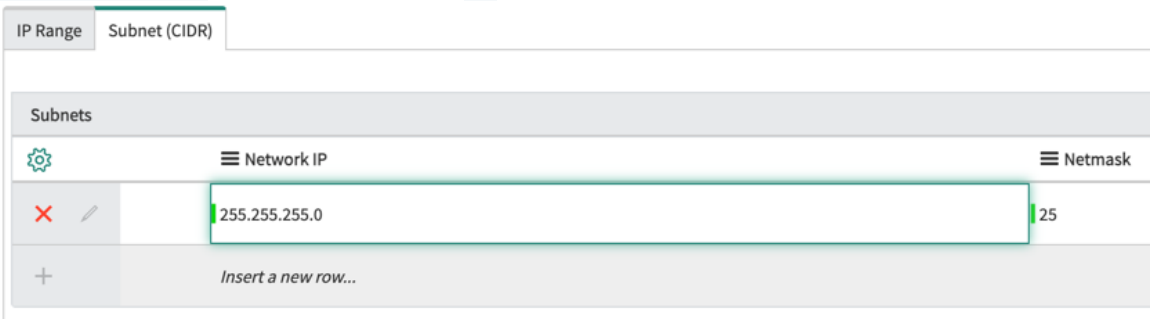
4. Clique com o botão direito no cabeçalho do formulário e clique em **Salvar**.
5. Na guia **Intervalo de IP**, clique duas vezes em **Inserir uma nova linha**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você pode inserir um único endereço IP ou vários intervalos de endereços IP. Por exemplo, para um intervalo de endereços IP, insira `192.0.2.0` na coluna **IP inicial** e `192.0.2.255` na coluna **IP final**.

> **Nota:** Para um único endereço IP, certifique-se de inserir o mesmo endereço IP nas colunas **IP inicial** e **IP Final**. Ao inserir um endereço IP na coluna **IP inicial**, deixe a coluna **IP final** em branco e salve o registro. A coluna **IP final** é preenchida automaticamente com o mesmo endereço do **IP inicial**.

6. Na guia **Sub-rede (CIDR)**, clique duas vezes em **Inserir uma nova linha**. Insira o endereço IP da rede e a máscara de rede no formato Roteamento entre domínios sem classe (CIDR). Por exemplo, insira `255.255.255.0` como IP de rede e `25` como máscara de rede.



Filtro de função

Use os critérios de filtro para filtrar usuários com base em suas funções.

Os critérios de filtro por função permitem filtrar usuários com base nas funções. Você pode configurar uma política de autenticação para permitir ou negar acesso a uma lista de funções do usuário.

Como criar critérios de filtro por função

Os critérios de filtro por função permitem filtrar usuários com base nas funções. Você pode configurar uma política de autenticação para permitir ou negar acesso a uma lista de funções do usuário.

Antes de Iniciar

Função necessária: administrador

Procedimento

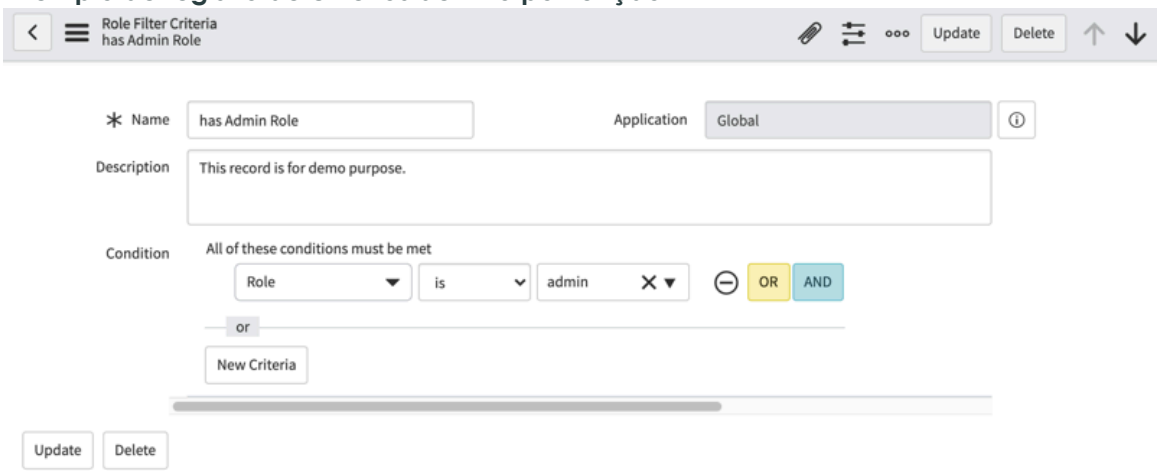
1. Navegue até **Todos** > **Autenticação adaptável** > **Critérios de filtro** > **Critérios de filtro por função**.
2. Clique em **Novo**.
3. No formulário, preencha os seguintes campos.

Formulário de critério de filtro por função

Campo	Descrição
Nome	Nome para identificar a função.
Aplicação	Escopo da aplicação.
Descrição	Descrição resumida da função.

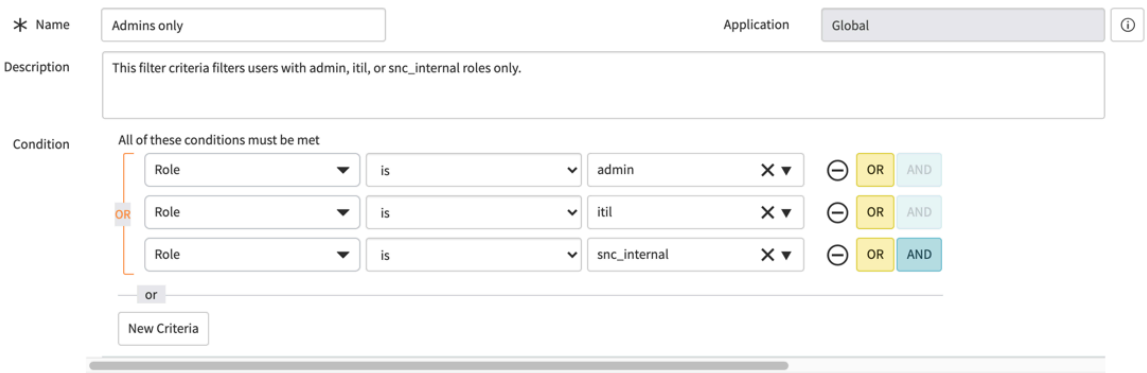
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exemplo de registro de critérios de filtro por função



4. Em **Funções para critérios**, clique duas vezes em **Inserir uma nova linha**.
5. Crie uma condição para uma função específica usando o Construtor de condições. Por exemplo, você pode criar uma condição que permita somente usuários com funções "admin", "itil" ou "snc_internal". Para obter mais informações sobre o Construtor de condições, consulte Como criar uma declaração de condição usando o Construtor de condições.

   Nota: Atualmente, a referência com pontos não é compatível com os critérios de filtro por função.



Filtro de grupo

Filtra usuários com base no grupo de usuários que pertence.

Critérios de filtro por grupo permite ou nega usuários com base no grupo de usuários que pertence.

Como criar critérios de filtro por grupo

Critérios de filtro por grupo permite ou nega usuários com base no grupo de usuários que pertence.

Antes de Iniciar
Função necessária: administrador

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

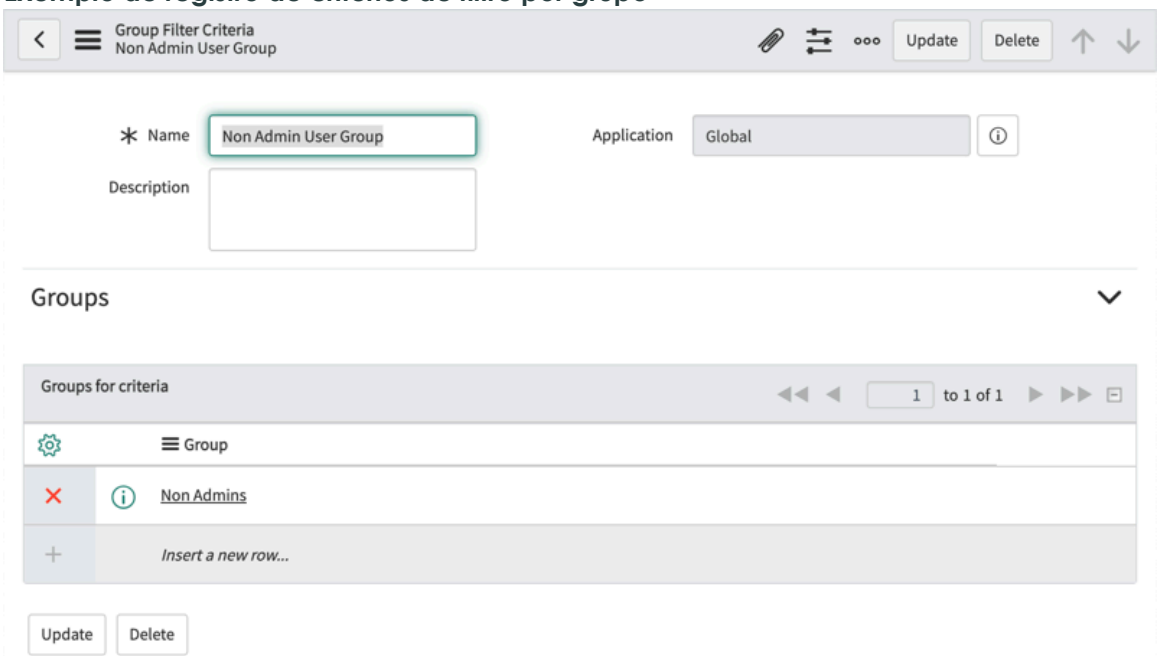
Procedimento

1. Navegue até **Todos** > **Autenticação adaptável** > **Critérios de filtro** > **Critérios de filtro por grupo**.
2. Clique em **Novo**.
3. No formulário, preencha os seguintes campos.

Critérios de filtro por grupo

Campo	Descrição
Nome	Nome para identificar o grupo.
Descrição	Descrição resumida do grupo.
Aplicação	Escopo da aplicação.

Exemplo de registro de critérios de filtro por grupo



4. Na guia **Grupos para critérios**, clique duas vezes em **Inserir uma nova linha**.
5. Clique no ícone de pesquisa , pesquise e selecione um grupo de usuários.
6. Clique no ícone salvar .

Filtro de localização

Os critérios do filtro de localização podem ser usados como entrada de filtro para usuários com base na localização do usuário.

O filtro de localização é um critério de filtro que os administradores podem usar ao criar as políticas de autenticação com base na localização física do dispositivo.

Nota:

- Os critérios de filtro de localização são um plug-in pago e requer licença.
- A instância deve estar em ADCv2. Se a instância não estiver em ADCv2, as informações de localização do usuário não estarão disponíveis.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Os critérios de filtro de localização permitem que você execute o seguinte:

- Agir como entrada de política para condições de política para verificar e atender aos requisitos de autenticação.
- Forneça a capacidade de criar políticas de autenticação adaptável com base no **país**.
- Permita ou não o acesso de instância de regiões.
- Use a política de pré-autenticação ou pós-autenticação baseada em localização geográfica para:
  - Impeça o acesso de países sancionados, fora de uma região com controles de privacidade rígidos, a critério da empresa.
  - Permita o acesso de áreas somente dentro de regiões escolhidas pela empresa com políticas de privacidade.
  - Configure a lista de países permitidos para autenticação.

Casos de uso

A seguir estão alguns dos casos de uso para critérios de filtro de local para Autenticação adaptável:

- Bloquear o acesso à instância de um país.
- Permitir o acesso à instância somente de um país.
- Impor autenticações em etapas ou MFA para logins de determinado país.
- Reduzir ou limitar as funções com base no país do usuário.
- Os critérios de filtro de local podem ser usados para MFA, ZTA (Confiança zero), contexto de pré-autenticação e contexto de pós-autenticação.

Identificação do local

Os serviços de localização de usuários são fornecidos por terceiros - MaxMind.

A localização do usuário é identificada por meio da VPN a partir do cabeçalho x-forwarded-for. Caso não haja nenhum cabeçalho preenchido pelo serviço, somente o IP da VPN (local) será exibido como o local do usuário.

Nota: Se houver locais incorretos exibidos após a configuração do filtro de local, consulte o artigo da base de conhecimento para solucionar o problema.

Ativar acesso baseado no local

Ative a **Confiança zero - Acesso baseado no local** (`com.snc.zero_trust_location_access`) para permitir que os administradores configurem políticas de autenticação adaptável com base na localização do usuário.

Antes de Iniciar

Função necessária: admin

- Plug-in dependente: autenticação adaptável
- Tipo de plug-in: pago e requer licença.
- A instância deve estar em ADCv2. Se a instância não estiver em ADCv2, então as informações de local do usuário não estarão disponíveis.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegue até **Todos** > **Aplicações do sistema** > **Todas as aplicações disponíveis** > **Todas**.
2. Encontre o plug-in **Confiança zero - Acesso baseado no local** (`com.snc.zero_trust_location_access`) usando os critérios de filtro e a barra de pesquisa.

   Pesquise o plug-in pelo nome ou ID. Se não conseguir encontrar um plug-in, talvez seja necessário solicitá-lo ao pessoal ServiceNow.
3. Selecione **Instalar** para iniciar o processo de instalação.

   Nota: Quando a separação de domínio e o administrador delegado estão habilitados em uma instância, o usuário administrativo deve estar no domínio **global.** Caso contrário, será exibido o seguinte erro: `A instalação da aplicação não está disponível porque há outra operação em execução: ativação de plug-in para <plugin name>.`

   Você verá uma mensagem após a conclusão da instalação.

Criar critérios para filtro de localização

Use os critérios para filtro de localização a fim de filtrar entradas para autenticação de usuários com base na localização deles.

Antes de Iniciar

Função necessária: admin

Plug-in necessário: **Confiança Zero - Acesso baseado em local** (`com.snc.zero_trust_location_access`).

Propriedade: habilite a propriedade de autenticação adaptável.

Nota: Os administradores só poderão criar a política com base em filtros de localização se a localização estiver disponível para a sessão do usuário atual.

Procedimento

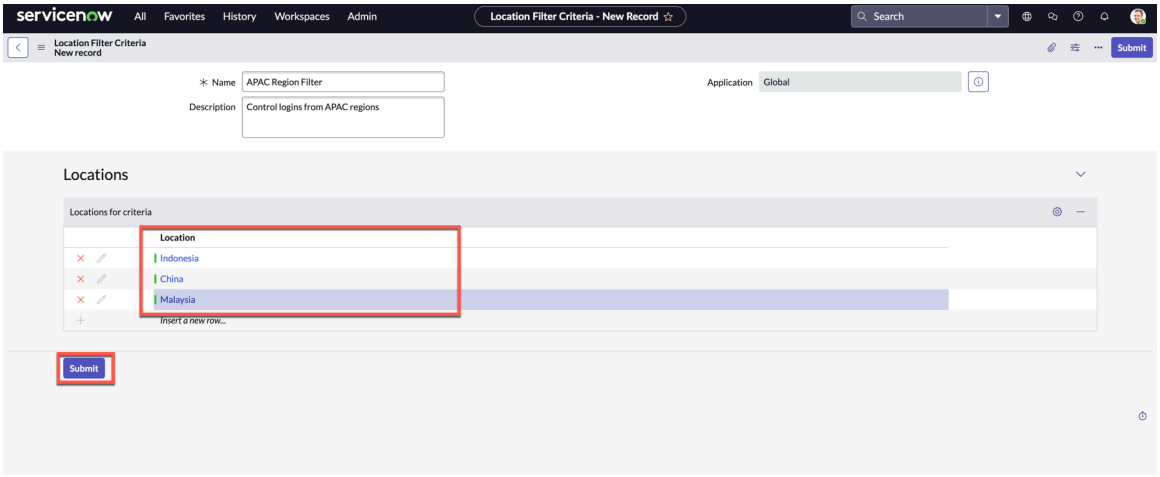
1. Navegue até **All** > **Autenticação adaptável** > **Critérios de filtro** > **Critérios de filtro de localização**.
2. Selecione **Novo**.
3. No formulário, preencha os seguintes campos.

Formulário de critérios para filtro de local

Campo	Descrição
Nome	Nome para identificar os critérios.
Descrição	Breve descrição dos critérios.
Aplicação	Escopo da aplicação.

4. Nas seções **Localizações**, na guia Localizações para critérios, clique duas vezes para **Inserir uma nova linha**.
5. Especifique as localizações.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



6. Selecione **Enviar**.

Tutorial: Use o critério para filtro de local

Descreve as etapas para usar critérios para filtro de local na política de autenticação e restringir o acesso aos usuários com base em suas localizações.

Antes de Iniciar

Função necessária: admin

Plug-in necessário: **Confiança Zero - Acesso baseado em local** (`com.snc.zero_trust_location_access`).

Propriedade: habilite a propriedade de autenticação adaptável.

Nota: Os administradores só poderão criar a política com base em filtros de localização se a localização estiver disponível para a sessão do usuário atual.

O procedimento a seguir descreve como criar e usar os critérios para filtro de local em uma política de autenticação.

Procedimento

1. Navegue até **Todos** > **Autenticação adaptável** > **Critérios de filtro** > **Filtro de local**.
2. Selecione **Novo**.
3. No formulário, preencha os seguintes campos.

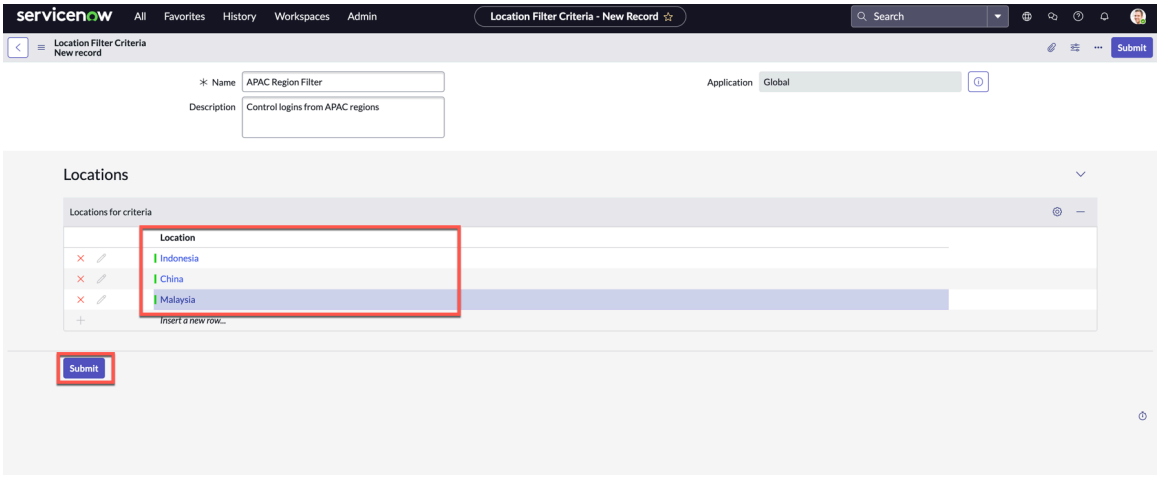
Formulário de critérios para filtro de local

Campo	Descrição
Nome	Nome para identificar os critérios.
Descrição	Breve descrição dos critérios.
Aplicação	Escopo da aplicação.

4. Nas seções **Localizações**, na guia Localizações para critérios, clique duas vezes para **Inserir uma nova linha**.
5. Especifique as localizações.

   Por exemplo, use algumas das regiões APAC para controlar os logins dos usuários provenientes da APAC.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Com base nos critérios definidos no exemplo, você pode controlar logins da `Indonésia`, `China`e `Malásia` para sua instância.

6. Selecione **Enviar**.
7. Use os critérios de filtro criados em qualquer contexto de autenticação (pré, pós, MFA) e Acesso à sessão.

   Para saber mais sobre a configuração com base no contexto de autenticação e no Acesso à sessão, consulte:

   - Contexto de pré-autenticação do filtro de local
   - Contexto de pós-autenticação do filtro de local
   - Filtro de local no contexto de MFA
   - Filtro de local para Acesso à sessão

   Você pode usar a mensagem de erro - ID de propriedade (`glide.auth.policy.ui.error.message`) para exibir uma mensagem de erro personalizada para o usuário quando houver uma tentativa falha de login devido a uma política de autenticação.

Uso do contexto de pré-autenticação do filtro de local

Use o critério do filtro de local criado no Contexto de pré-autenticação.

Antes de Iniciar

Função necessária: admin

Plug-in necessário: **Confiança Zero - Acesso baseado em local** (`com.snc.zero_trust_location_access`).

Crie um Filtro de local com os países que você deseja restringir o acesso dos usuários. Para obter mais informações, consulte Criar critérios para filtro de localização.

Procedimento

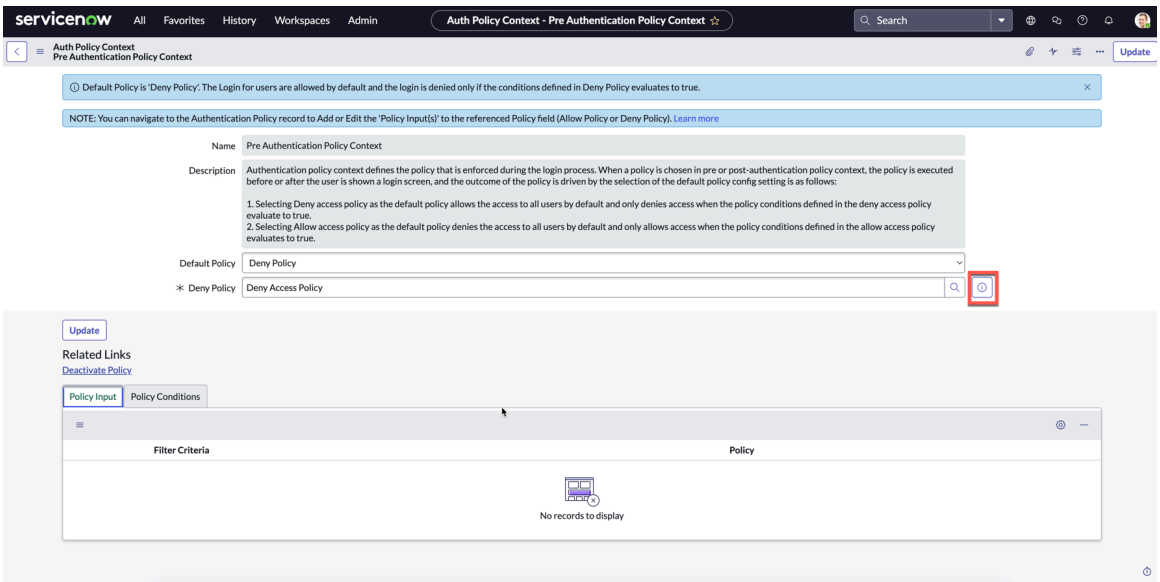
1. Navegue até **Todos** > **Autenticação adaptável** > **Contexto da política de autenticação** > **Contexto de pré-autenticação**.

   Quando uma política é escolhida no contexto da política de pré-autenticação:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Selecionar a política de Negar acesso como padrão permite o acesso a todos os usuários e só nega o acesso quando a condição da política de negar acesso estiver selecionada como verdadeira.
- Selecionar a política de Aprovar acesso como padrão nega o acesso a todos os usuários e só aprova o acesso quando a condição da política de permitir acesso estiver selecionada como verdadeira.

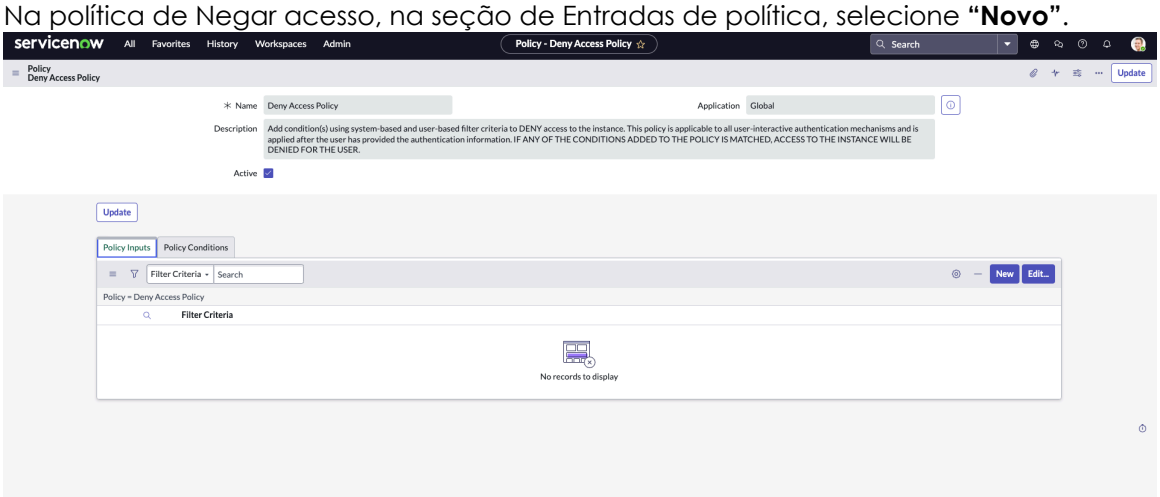
O exemplo mostra como você pode restringir os logins dos locais especificados. Você pode escolher a política de Negar acesso e a política associada (Negar acesso) como a política de pré-autenticação e especificar suas entradas e condições.



2. Selecione o ícone de informações para abrir o registro **Política de negação**.

> **Nota:** O exemplo descrito nesta tarefa é de **Política de negação**. Você também pode usar a **Política de permissão** e definir as condições relacionadas para controlar os logins.

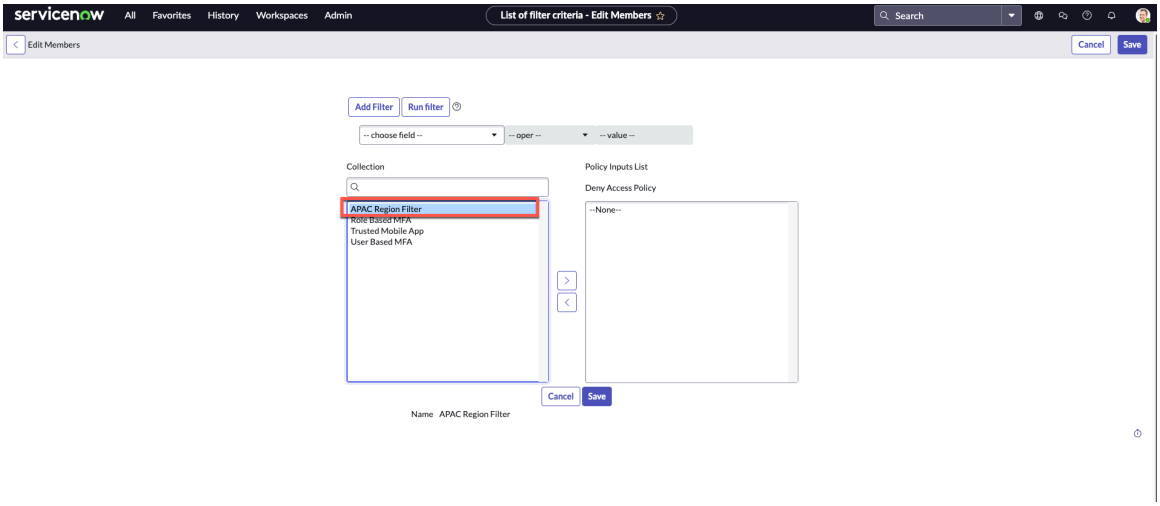
3. Na política de Negar acesso, na seção de Entradas de política, selecione **"Novo"**.



4. Adicione a entrada do filtro de local e **"Salvar"**.

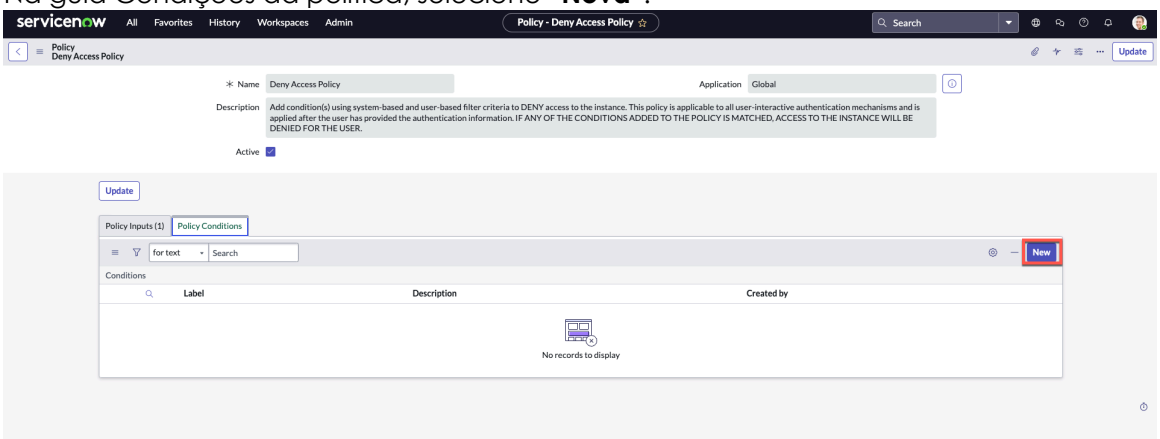
Por exemplo, região APAC.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

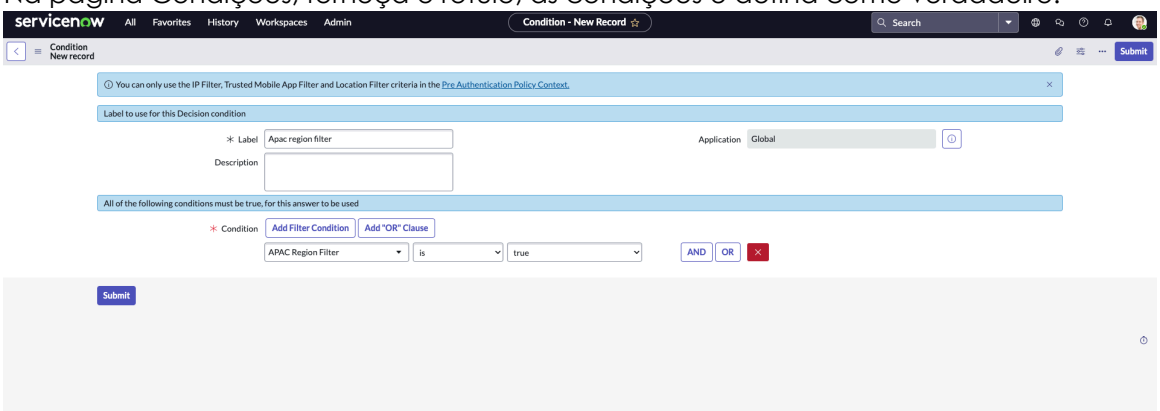


O filtro é adicionado como **Entrada de política**.

5. Na guia Condições da política, selecione **"Nova"**.



6. Na página Condições, forneça o rótulo, as condições e defina como verdadeiro.



Nota:

- Neste exemplo, a seleção de verdadeiro como uma condição implica que os usuários que fizerem login a partir das regiões configuradas não poderão se conectar a instância.
- Se a condição for definida como falsa, somente os usuários das regiões configuradas poderão se conectar a instância, e os outros usuários não poderão se conectar a instância.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

7. Selecione **Enviar**.
   Os usuários que selecionam o link da instância e fazem login a partir dos países configurados recebem uma mensagem de erro sobre o acesso negado (essa mensagem de erro é configurada pelos seus administradores na página de propriedades da política).

Uso do contexto de pós-autenticação do filtro de local

Usando o critério do filtro de local criado no Contexto de pós-autenticação.

Antes de Iniciar

Função necessária: admin

Plug-in necessário: **Confiança Zero - Acesso baseado em local** (`com.snc.zero_trust_location_access`).

Crie um Filtro de local com os países que você deseja restringir o acesso dos usuários. Para obter mais informações, consulte Criar critérios para filtro de localização.

Procedimento

1. Navegue até **"Todos"** > **"Autenticação adaptável"** > **"Contexto da política de autenticação"** > **"Contexto de pós-autenticação"**.

   Quando uma política é escolhida no contexto da política de pós-autenticação:

   - Selecionar a política de Negar acesso como padrão permite o acesso a todos os usuários e só nega o acesso quando a condição da política de negar acesso estiver selecionada como verdadeira.
   - Selecionar a política de Aprovar acesso como padrão nega o acesso a todos os usuários e só aprova o acesso quando a condição da política de permitir acesso estiver selecionada como verdadeira.

   O exemplo mostra como você pode configurar um usuário `itil` com uma condição para acessar somente a instância a partir de um local específico (EUA). E os usuários `itil` não podem fazer login a partir de outros países.

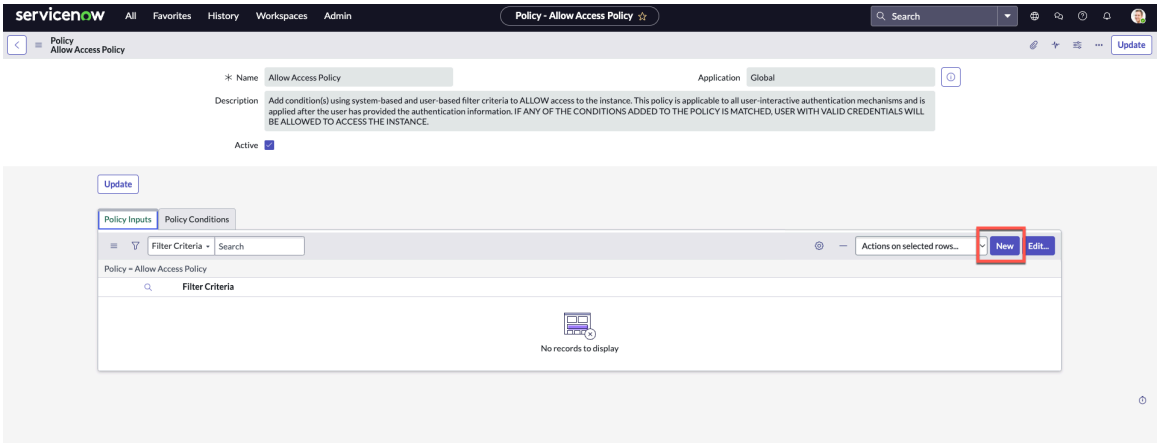
   Depois que os usuários fornecem suas credenciais na página de login. Você pode escolher a política de Permitir acesso e a política associada (Permitir acesso) como a política de pós-autenticação e especificar suas entradas e condições.

2. Selecione o ícone de informações para abrir o registro **Política de permissão**.

   Nota: O exemplo descrito nesta tarefa é de **Política de permissão**. Você também pode usar a **Política de negação** e definir as condições relacionadas para controlar os logins.

3. Na política de Permitir acesso, na seção de Entradas de política, selecione **"Novo"**.

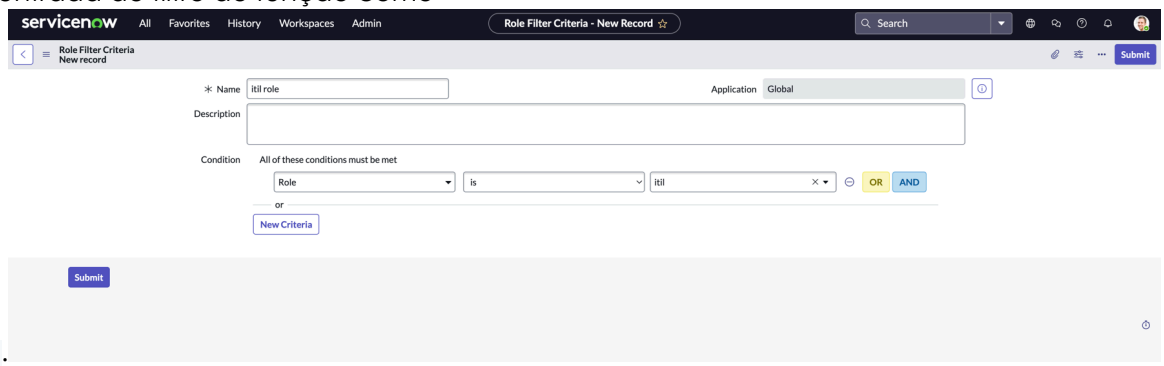
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Adicione os critérios de filtragem de função e de local.

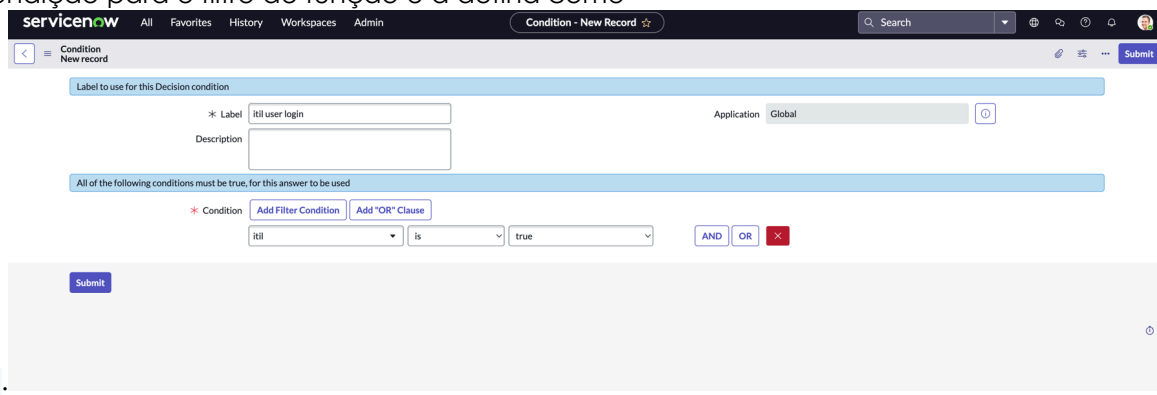
a. Como adicionar critérios de filtro de função:

- Crie entrada de filtro de função como



`itil`.

- Crie uma Condição para o filtro de função e a defina como



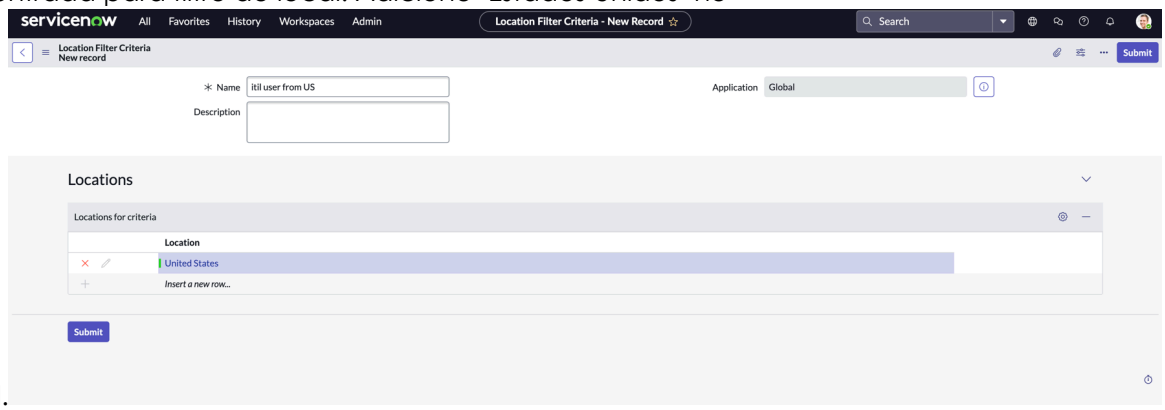
`verdadeira`.

Para obter mais informações sobre como criar filtros de função, consulte Como criar critérios de filtro por função.

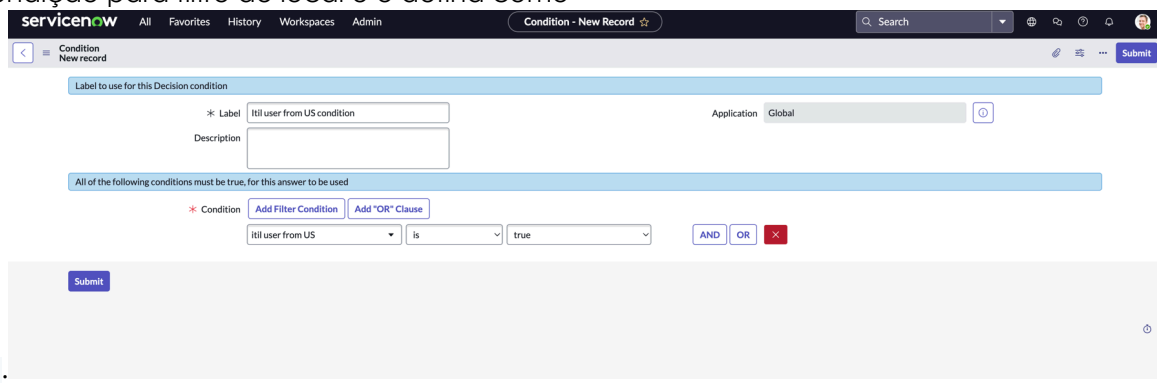
b. Adição de critérios para filtro de local:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Crie entrada para filtro de local. Adicione "Estados Unidos" no Local.



- Crie uma Condição para filtro de local e o defina como `verdadeiro`.

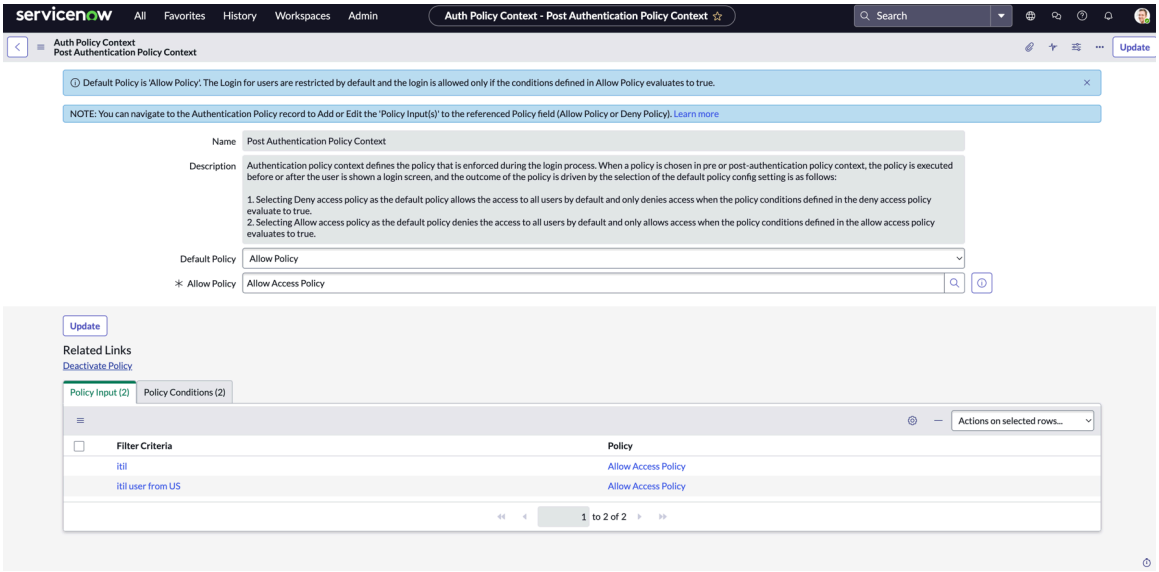


Para obter mais informações sobre como criar filtros de função, consulte Criar critérios para filtro de localização.

A política de permissão de acesso mostra as entradas e as condições da política criadas nas etapas anteriores:

- Entradas de política: itil, usuário itil dos EUA
- Condições da política: login do usuário itil, condição de usuário itil dos EUA.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Nota:

- Neste exemplo, a seleção de verdadeiro como uma condição implica que os usuários `itil` que fazem login a partir dos EUA (país configurado) podem se conectar a instância.
- Se a condição for definida como falsa, os usuários `itil` dos EUA (país configurado) não poderão se conectar a instância, e os outros usuários não poderão se conectar a instância.

5. Selecione **"Enviar"** ou **"Atualizar"** para atualizar o contexto de pós-autenticação.
   Os usuários `itil` que selecionam o link da instância, especificam suas credenciais e, em seguida, se conectam fora do país configurado (EUA) recebem uma mensagem de erro sobre o acesso negado (mensagem de erro que é configurada pelos seus administradores na página de propriedades da política).

Uso do filtro de local no contexto de MFA

Use o critério do filtro de local criado no Contexto de MFA.

Antes de Iniciar

Função necessária: admin

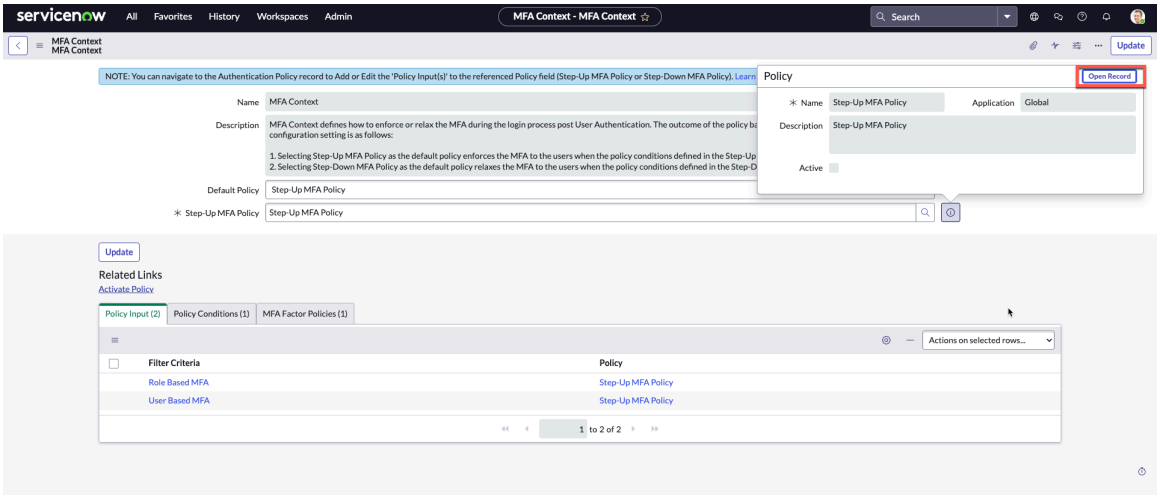
Plug-in necessário: **Confiança Zero - Acesso baseado em local** (`com.snc.zero_trust_location_access`).

O procedimento a seguir descreve como você pode criar um Filtro de local com os países que você quiser configurar o MFA como um segundo fator de autenticação para os usuários com base em localização.

Procedimento

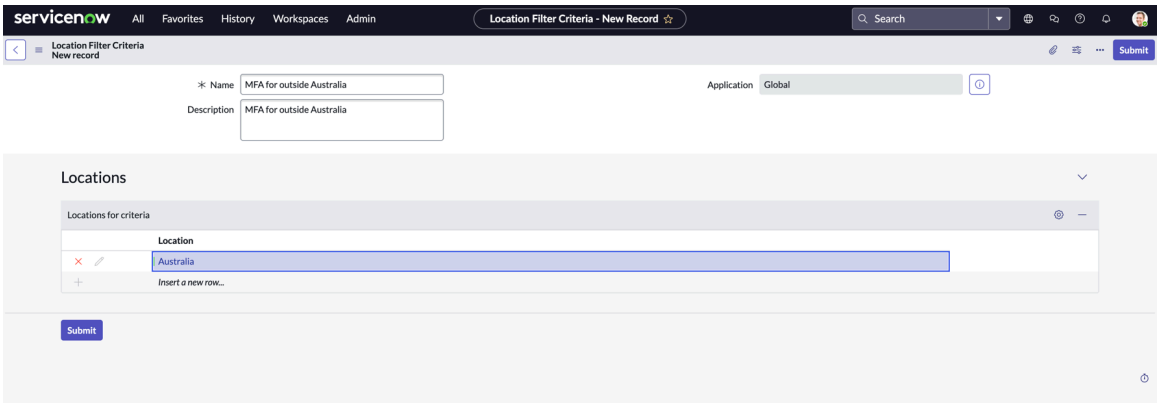
1. Navegue até **"Todos"** > **"Autenticação adaptável"** > **"Contexto da política de autenticação"** > **"Contexto de MFA"**.
2. Na página **Contexto de MFA**, selecione o ícone de informações da **Política de MFA em etapa crescente** e abra o registro.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

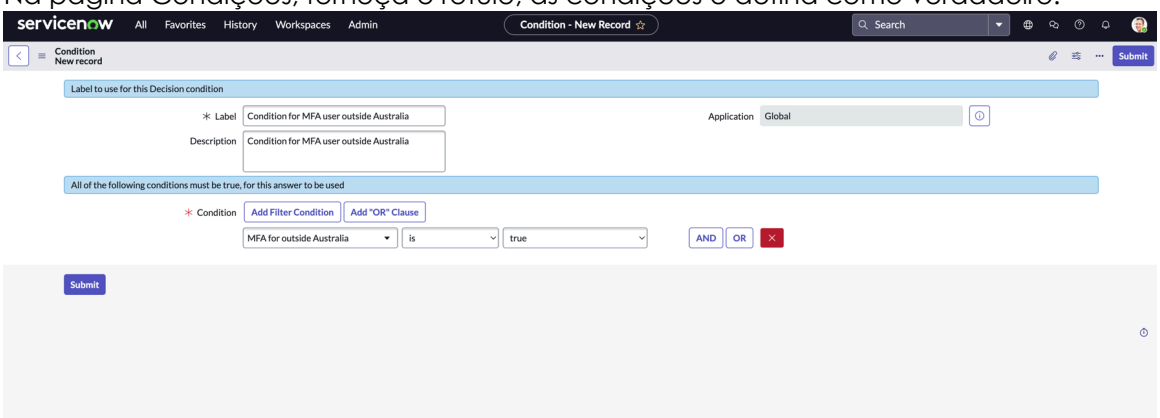


3. Na página Política de MFA em etapa crescente, na guia Entradas de política, selecione **"Novo"**.
4. Adicione a entrada do Filtro de local e **"Enviar"**.

   Por exemplo, se quiser exibir a MFA para usuários que fazem login na instância de fora da Austrália.



5. Na página Política de MFA em etapa crescente, selecdione a guia Condições de política e selecione **"Nova"**.
6. Na página Condições, forneça o rótulo, as condições e defina como verdadeiro.



7. Selecione **Enviar**.
8. Na página Política de MFA em etapa crescente, ative a Política de MFA se ela estiver **Desativada**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

9. Selecione **"Atualizar"** para atualizar a configuração.

   Os usuários fora do país configurado (Austrália) que selecionarem o link da instância e especificarem suas credenciais serão mostrados a tela de MFA para fornecer as credenciais do segundo fator de autenticação para fazerem login na instância.

Usar filtro de local para acesso à sessão

Use os critérios de filtro de local criados em Acesso à sessão para reduzir as funções com base no local do usuário.

Antes de Iniciar

Função necessária: admin

Plug-in necessário: **Confiança Zero - Acesso baseado em local** (`com.snc.zero_trust_location_access`).

O procedimento a seguir descreve como criar um filtro de local com os países que você deseja remover ou limitar as funções aos usuários com base no local.

Procedimento

1. Navegue até **"Todos"** > **"Acesso de confiança zero"** > **"Configurações de função de acesso à sessão"**.
2. Para criar uma configuração de função de acesso à sessão, selecione **"Novo"**.
3. No formulário, preencha os campos:

Configuração de função de acesso à sessão

Campo	Descrição
Nome	Nome da configuração
Descrição	Descrição resumida da configuração
Política	Escolha a política de acesso. Use o ícone de pesquisa para exibir a lista de políticas. **Nota:** Você precisa adicionar a entrada e as condições do filtro de local abrindo o registro de políticas.
Ação	**"Remover funções"** ou **"Limitar funções"**. ◦ **Remover funções**: quando o usuário configurado está conectado, a lista de funções fornecida na função ou na lista agrupada é removida da sessão logada. ◦ **Limitar a funções**: quando o usuário configurado está conectado, somente as funções selecionadas são fornecidas ao usuário e todas as outras funções são removidas da sessão logada.
Lista de funções	Escolha a função na lista de funções.
Lista agrupada	Escolha a função na lista agrupada.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Selecione **"Enviar"**.

   O login para usuários com base nos países configurados ocorre da seguinte forma:

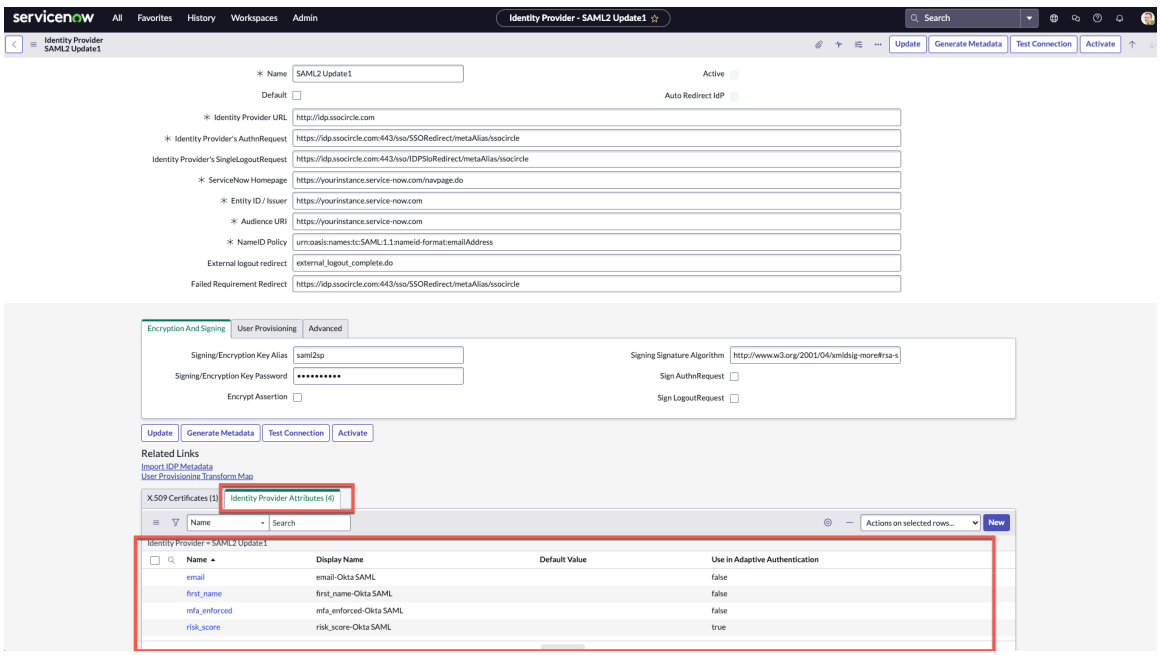
   - Se for **Remover funções**, os usuários dos países configurados no filtro de local serão removidos com as funções configuradas para a sessão.
   - Se for **Limitar às funções**, os usuários dos países configurados no filtro de local terão apenas as funções que foram configuradas para a sessão.

   Para aprender mais sobre como remover ou limitar funções de uma sessão, consulte Tutorial: usar o acesso Zero Trust.

Filtro de atributos do provedor de identidade

Use os Atributos do provedor de identidade que são recebidos como resposta do SAML (Security Assertion Markup Language, Linguagem de marcação de segurança) vindos do Provedor de identidade como critério de filtro para autenticação.

Para obter todos os atributos de um IdP por meio da resposta do SAML, execute um teste de conexão com o IdP. Após um teste de conexão bem-sucedido, os atributos são adicionados a uma nova guia na página de configuração do provedor de Identidade.



Você também pode adicionar atributos selecionando **"Novo"** na seção "Atributos do provedor de identidade" e usar esses atributos para a Autenticação adaptável definindo como `verdadeiro`.

Os **Atributos do provedor de identidade** são exibidos com os seguintes detalhes:

Formulário de critérios para filtro de local

Campo	Descrição
Nome	Nome do atributo fornecido pelo Provedor de Identidade.
Nome de exibição	Nome de exibição é o nome detalhado usado para os critérios de filtro.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formulário de critérios para filtro de local

Campo	Descrição
	Nota: Você pode fornecer um nome legível como um Nome de exibição. Em alguns casos, o Nome de exibição fornecido pelos Provedores de Identidade é longo e não pode ser lido.
Valor Padrão	O valor padrão é usado para avaliação de critérios de filtro caso o atributo esteja ausente na resposta do SAML.
Usar na autenticação adaptável	Opção para usar o Atributo na Autenticação adaptável.

Nota: Os atributos preenchidos do IdP Azure têm nome e nome de exibição com limitação de caracteres devido ao tamanho do nome do atributo.

Você também pode adicionar novos atributos selecionando **"Novo"** na seção **Atributos dos provedores de identidade**.

Se o uso na autenticação adaptável estiver definido como verdadeiro, o atributo selecionado será adicionado como critério de filtro nos critérios de filtro genéricos. Por exemplo, **risk_score** definido como `verdadeiro`. A página Critérios de filtro genérico tem um novo filtro criado.

Uso de Atributo de provedor de identidade como critério de filtro

Use o Atributo de provedor de identidade (IDP) da resposta do SAML (Security Assertion Markup Language, Linguagem de marcação de segurança) como critério de filtro para uma política de autenticação.

Antes de Iniciar

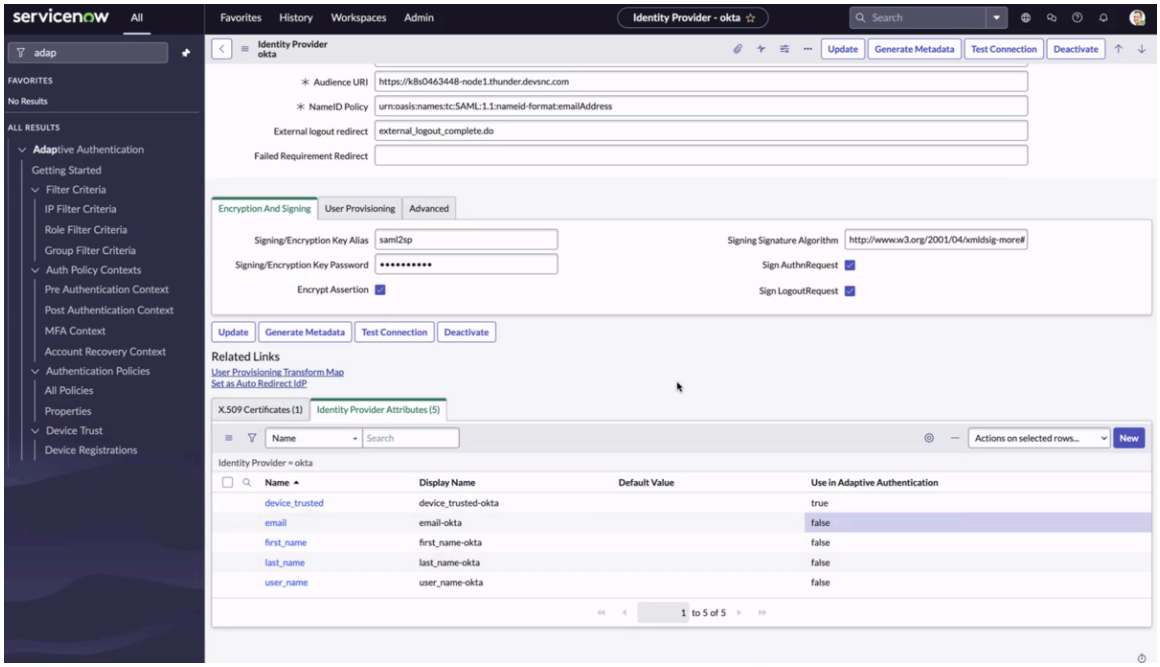
Função necessária: admin

Você pode criar uma política de acesso à sessão usando o contexto de política (pré-autenticação, pós-autenticação, autenticação multifator) e critérios de filtro (função, grupo, IP, local) com políticas de entrada e condições.

O procedimento a seguir mostra as etapas necessárias para configurar o atributo IdP da resposta do SAML como uma entrada de política para controlar a autenticação no contexto de **pós-autenticação**, de **autenticação multifator (MFA)**e de **acesso baseado em política de Confiança Zero**.

Os atributos do IDP Okta estão exibidos na captura de tela a seguir. Você deve definir o Uso na Autenticação adaptável como verdadeiro para usá-lo no contexto de políticas de **Pós-autenticação**, de **Autenticação multifator (MFA)**e de **acesso baseado em política de Confiança Zero**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Nota: Políticas de acesso de pós-autorização, MFA e Confiança Zero são executadas depois que os usuários inserem as credenciais ou a resposta do SSO.

Procedimento

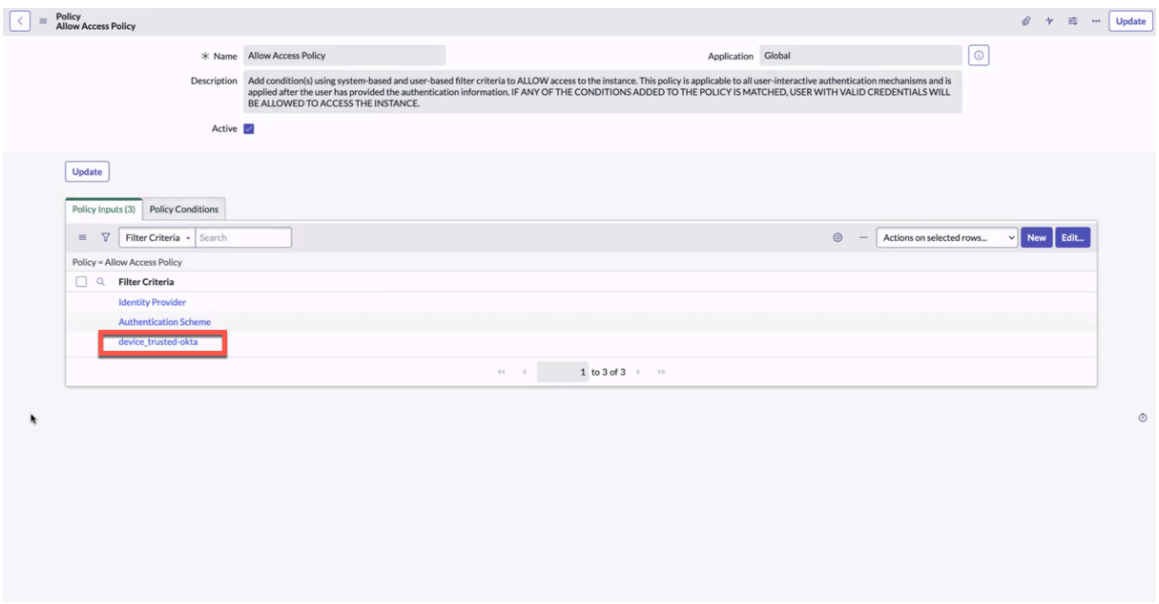
1. Uso do atributo IDP em contexto da política de pós-autenticação.
   Exemplo: configuração para habilitar logins a partir dos atributos de IDP Okta se o dispositivo for confiável.

   a. Navegue até **"Todos"** > **"Autenticação adaptável"** > **"Contextos da política de autenticação"** > **"Contexto da política de pós-autenticação"**.

   b. Selecione **"Permitir política"** e abra o registro de política.

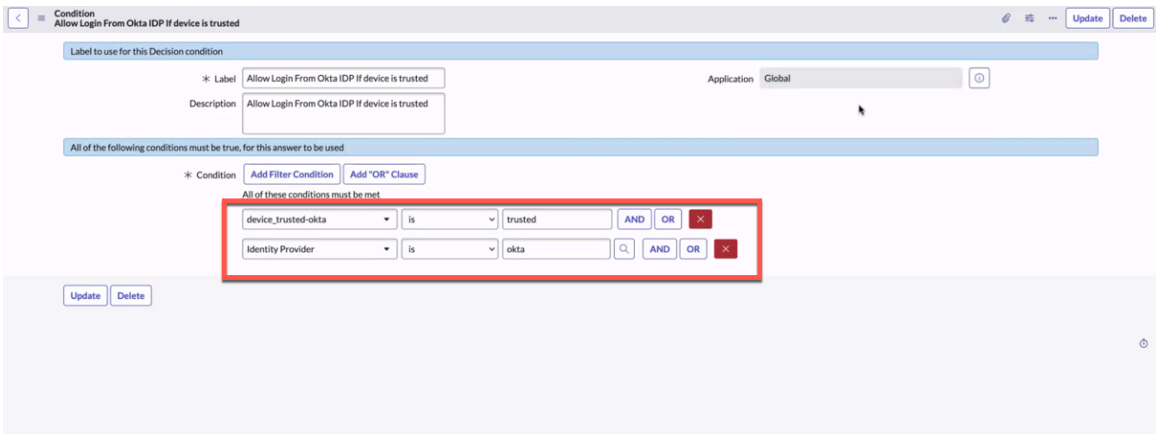
   c. Na Entrada de política, crie a Entrada de política e a Condição de política.

   - **Entrada de política**: Adicionar **device_trusted-okta**.



© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- **Condições da política**: **device_trusted-okta** é `confiável` e o **Provedor de identidade** é `okta`.



Com base nessa configuração, quando o dispositivo for confiável no Okta (IdP), o usuário será autenticado na instância.

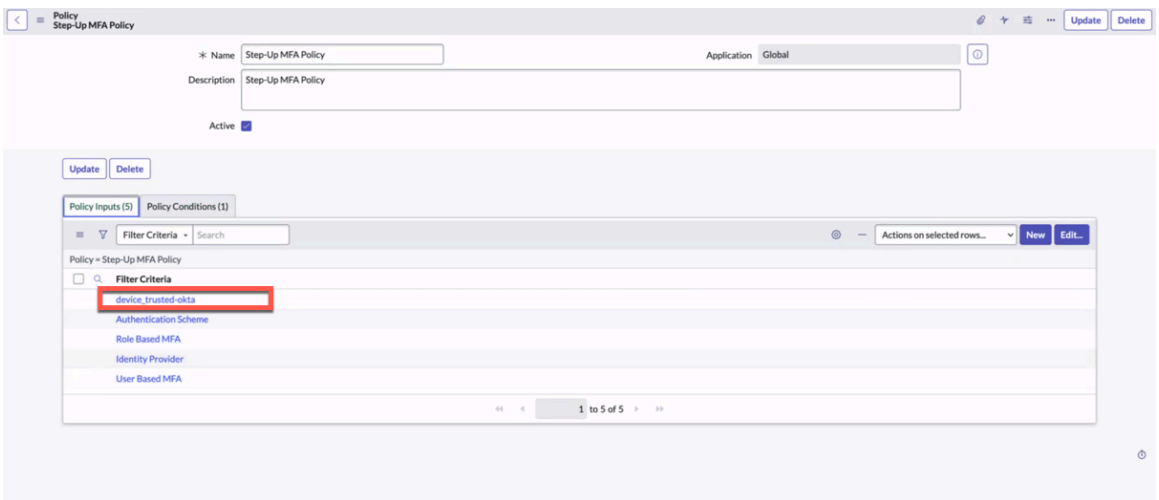
Para obter mais informações sobre como criar um Contexto de pós-autenticação com políticas de entrada e condição, consulte Contexto de pós-autenticação.

2. Uso do atributo IDP em contexto de política MFA.
Exemplo: configuração para habilitar MFA a partir dos atributos IDP Okta se o dispositivo não for confiável.

a. Navegue até **"Todos"** > **"Autenticação adaptável"** > **"Contextos da política de autenticação"** > **"Contexto da política de autenticação MFA "**.

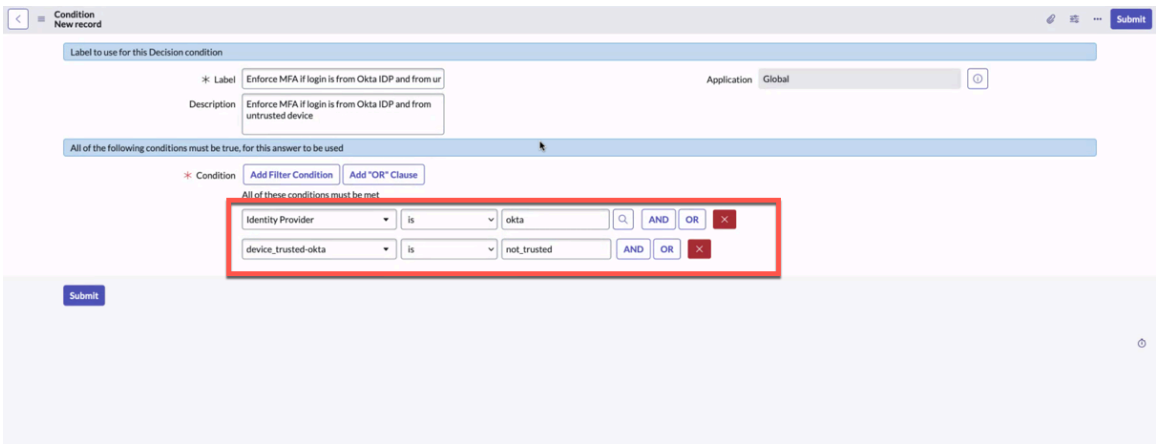
b. Na Entrada de política, crie a Entrada de política e a Condição de política.

- **Entrada de política**: Adicionar **device_trusted-okta**.



© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- **Condições da política**: **device_trusted-okta** é `not_trusted (não confiável)` e o **Provedor de identidade** é `okta`.



Com base nessa configuração, quando o dispositivo for "não confiável" no Okta (IdP), o usuário terá que passar por um segundo fator de autenticação para se conectar à instância.

Para obter mais informações sobre como criar um Contexto de autenticação MFA com políticas de entrada e condição, consulte Contexto de MFA (autenticação multifator).

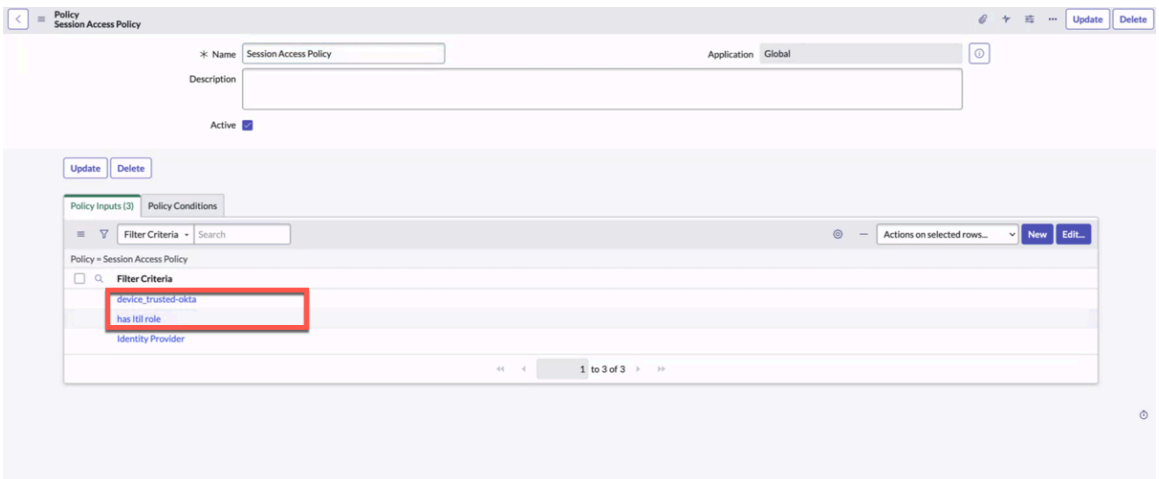
3. Uso do atributo IDP para acesso em sessões com política de Confiança Zero
   Exemplo: configuração para reduzir o privilégio da função `itil` dos atributos IDP Okta se o dispositivo não for confiável.

   a. Navegue até **"Todos"** > **"Acesso de confiança zero"** > **"Configurações de função de acesso à sessão"**.

   b. Crie uma configuração de função de acesso à sessão

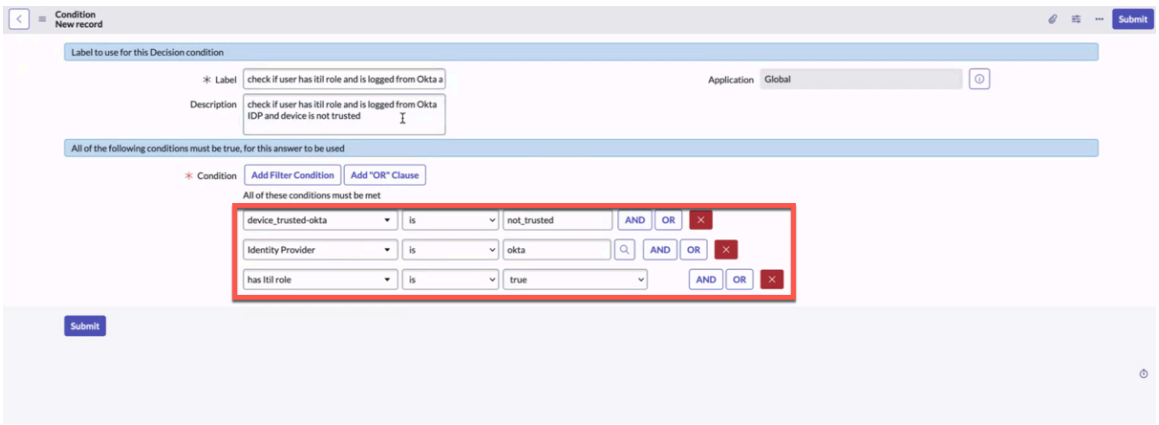
   c. Na Entrada de política, crie a Entrada de política e a Condição de política.

   - **Entrada de política**: Adicionar **device_trusted-okta** e **tem a função itil**.



© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- **Condições da política**: **device_trusted-okta** é `not_trusted (não confiável)`, **Provedor de identidade** é `okta` e **tem função itil** é `verdadeiro`.



Com base nesta configuração, quando o usuário `itil` usar um dispositivo que é não confiável pelo Okta (IdP), os privilégios do usuário serão reduzidos para a sessão conectada.

Para obter mais informações sobre como criar uma política de acesso a sessões de Confiança Zero com políticas de entrada e condição, consulte Zero Trust Access.

Contextos da política de autenticação

Use contextos da política de autenticação para determinar como e quando sua instância aplica políticas de autenticação.

Os contextos de autenticação definem como e quando uma política é aplicada durante o processo de login. Atribua uma política a um contexto de política para definir entradas e condições relacionadas a como sua instância lida com a autenticação.

Contexto de pré-autenticação

No contexto de pré-autorização, as políticas são executadas quando um usuário acessa a instância pela primeira vez, antes de ver a tela de login. Você pode usar o contexto de pré-autorização para permitir ou negar o acesso antes que os usuários sejam solicitados a fornecer credenciais de login com base na política selecionada. Como essas políticas são avaliadas antes de um usuário inserir qualquer informação, elas não conseguem levar em conta critérios como funções ou grupos de um usuário.

Para obter mais detalhes sobre este contexto, consulte Contexto de pré-autenticação.

Contexto de pós-autenticação

No contexto de pós-autorização, as políticas são executadas depois que os usuários inserem as credenciais ou a resposta do SSO. Sua instância permite ou nega o acesso com base na política selecionada. Como seus usuários se identificaram por meio das credenciais de login deles, a política pode usar as informações do usuário para determinar se deve conceder acesso.

Para obter mais detalhes sobre este contexto, consulte Contexto de pós-autenticação.

Contexto de MFA (autenticação multifator)

As políticas atribuídas ao contexto de MFA definem se ela deve ser aplicada durante o processo de login. A aplicação da MFA à sua instância é determinada pela configuração

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

de políticas neste contexto. Para obter mais detalhes sobre este contexto, consulte Contexto de MFA (autenticação multifator).

Contexto de recuperação de conta

Os administradores podem configurar a recuperação de conta (ACR) para executar atividades de recuperação, como lidar com erros de configuração de SSO ou certificados expirados. Para usar a recuperação de conta, registre pelo menos uma conta de administrador como um usuário de recuperação de conta. O Single Sign-on não pode ser ativado em sua instância até que pelo menos uma conta seja configurada. Para obter mais informações sobre o contexto aplicável, consulte Contexto de recuperação de conta.

Contexto de validação de sessão

Você pode usar o Contexto de validação de sessão com a estrutura de política de Autenticação adaptável. A estrutura utiliza políticas de autenticação para avaliar as solicitações de autenticação (sessão) para negar ou permitir o acesso com base nas condições da política. Para obter mais informações, consulte Contexto de validação de sessão.

Política padrão

No contexto da política, você pode definir uma política padrão no campo **Política padrão**. Este padrão define como sua instância responde ao resultado da sua política. As opções de política padrão disponíveis são determinadas pelo contexto que você está usando. Obtenha mais detalhes sobre essas opções nos documentos que descrevem esses contextos individuais.

Contexto de pré-autenticação

O contexto da política de pré-autenticação define como e quando uma política é aplicada durante o processo de login. A política usada neste contexto é executada antes que os usuários vejam a tela de login.

Registro do contexto de pré-autenticação

No contexto de pré-autorização, as políticas são executadas quando um usuário acessa a instância pela primeira vez, antes de ver a tela de login.

Você pode usar o contexto de pré-autenticação para permitir ou negar o acesso antes que os usuários sejam solicitados a fornecer credenciais de login com base na política selecionada. Como essas políticas são avaliadas antes de um usuário inserir qualquer informação, elas não conseguem levar em conta critérios como funções ou grupos de um usuário.

Use os campos no registro de contexto da política de pré-autenticação para definir como sua instância usa a política.

Formulário do contexto de pré-autenticação

Campo	Descrição
Nome	Nome do contexto da política. Este campo é estático e não pode ser alterado.
Descrição	Descrição do contexto
Política padrão	Define o comportamento padrão desse contexto ao avaliar a política. Selecione uma das seguintes opções.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formulário do contexto de pré-autenticação

Campo	Descrição
	Política de permissão Nega o acesso a todos os usuários por padrão e só permite o acesso quando as condições da política selecionada no campo **Permitir política** são avaliadas como verdadeiras. Política de negação Permite o acesso a todos os usuários por padrão e só nega o acesso quando as condições da política selecionada no campo **Negar política** são avaliadas como verdadeiras.
Política de permissão	A política usada nesse contexto. Este campo aparece somente quando o campo **Política padrão** está definido como **Política de permissão**.
Política de negação	A política usada nesse contexto. Este campo aparece somente quando o campo **Política padrão** está definido como **Política de negação**.

Nota:

Você só pode usar os critérios Filtro de IP, Filtro de aplicativo para celular confiável e Filtro de local no Contexto da política de pré-autenticação.

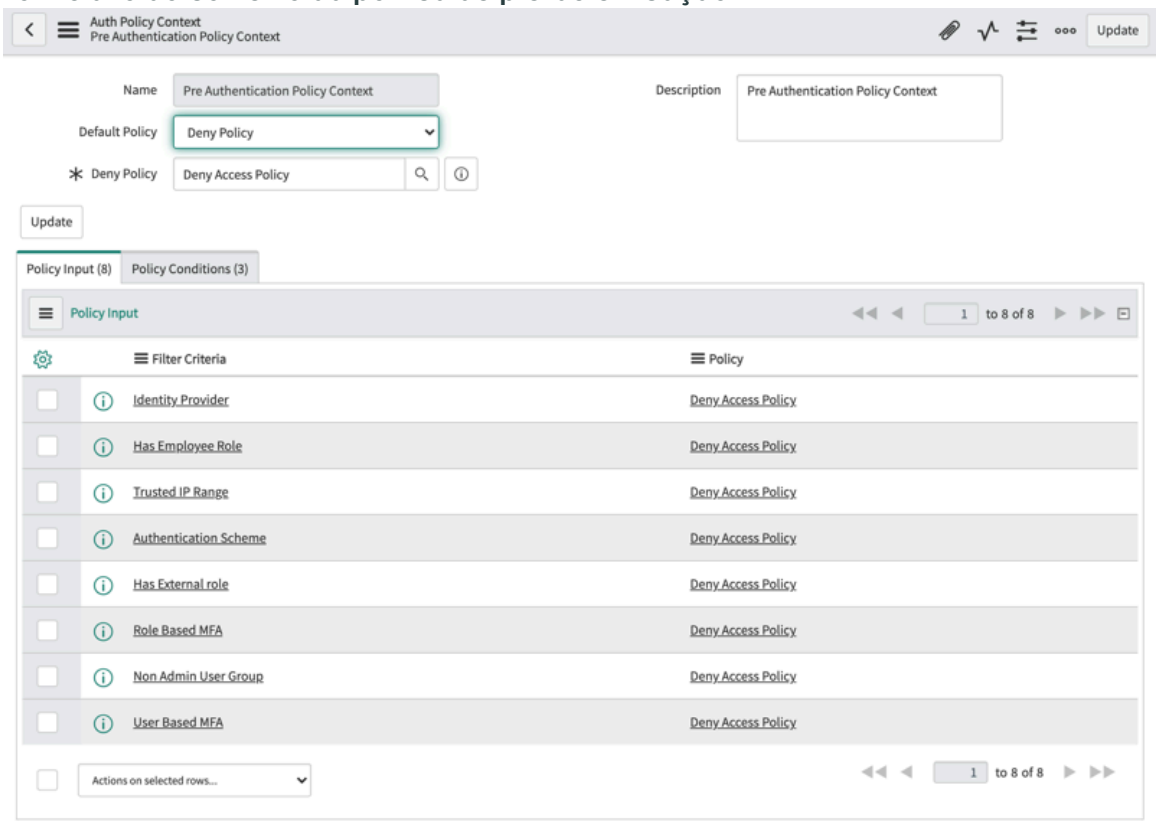
Entradas e condições da política

As guias **Entradas de política** e **Condições de política** exibem as entradas e as condições da política selecionada no campo **Política de permissão** ou **Política de negação**. Essas guias servem como referência, mas não podem ser usadas para mudar as entradas ou condições da política. Para modificar sua política, navegue até ela usando o ícone de referência ( ) ao lado do campo **Política de permissão** ou **Política de negação**.

Este exemplo mostra um registro de contexto de política de pré-autenticação configurado para negar acesso por padrão. O contexto usa uma política chamada **Política de negação de acesso**, que tem um conjunto de entradas e condições que são exibidas nas guias **Entrada de política** e **Condição de política**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formulário do contexto da política de pré-autenticação



Contexto de pós-autenticação

O contexto da política de pós-autenticação define como e quando uma política é aplicada durante o processo de login. A política usada neste contexto é executada depois que os usuários veem a tela de login.

Registro do contexto de pós-autenticação

No contexto de pós-autorização, as políticas são executadas depois que os usuários inserem as credenciais ou a resposta do SSO. Sua instância permite ou nega o acesso com base na política selecionada. Como seus usuários se identificaram por meio das credenciais de login deles, a política pode usar as informações do usuário (como função ou grupo) para determinar se deve conceder acesso.

Use os campos no registro de contexto da política de pós-autenticação para definir como sua instância usa a política.

Formulário do contexto de pós-autenticação

Campo	Descrição
Nome	Nome do contexto da política. Este campo é estático e não pode ser alterado.
Descrição	Descrição do contexto
Política padrão	Define o comportamento padrão desse contexto ao avaliar a política. Selecione uma das seguintes opções. Política de permissão

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formulário do contexto de pós-autenticação

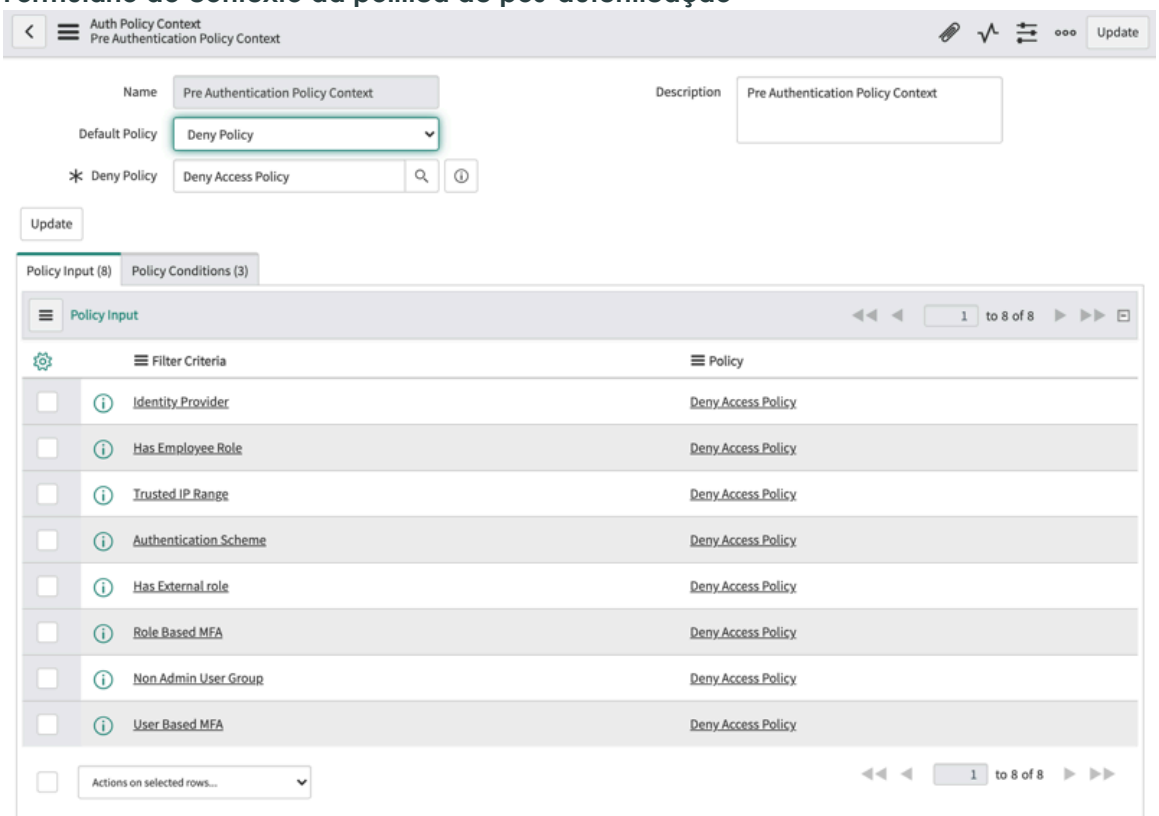
Campo	Descrição
	Nega o acesso a todos os usuários por padrão e só permite o acesso quando as condições da política selecionada no campo **Permitir política** são avaliadas como verdadeiras. Política de negação Permite o acesso a todos os usuários por padrão e só nega o acesso quando as condições da política selecionada no campo **Negar política** são avaliadas como verdadeiras.
Política de permissão	A política usada nesse contexto. Este campo aparece somente quando o campo **Política padrão** está definido como **Política de permissão**.
Política de negação	A política usada nesse contexto. Este campo aparece somente quando o campo **Política padrão** está definido como **Política de negação**.

Entradas e condições da política

As guias **Entradas de política** e **Condições de política** exibem as entradas e as condições da política selecionada no campo **Política de permissão** ou **Política de negação**. Essas guias servem como referência, mas não podem ser usadas para mudar as entradas ou condições da política. Para modificar as configurações da sua política, navegue até ela usando o ícone de referência (ⓘ) ao lado do campo **Política de permissão** ou **Política de negação**.

Este exemplo mostra um registro de contexto de política de pós-autenticação configurado para negar acesso por padrão. O contexto usa uma política chamada **Política de negação de acesso**, que tem um conjunto de entradas e condições que são exibidas nas guias **Entrada de política** e **Condição de política**.

Formulário do contexto da política de pós-autenticação



© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Contexto de MFA (autenticação multifator)

O contexto da política de MFA (autenticação multifator) usa a política para definir como e quando uma MFA é aplicada durante o processo de login.

Registro de contexto de MFA

O contexto da política de MFA (Autenticação multifator) define se os usuários devem fornecer uma segunda forma de autenticação ao fazer login. Diferente das políticas de pós-autenticação e pré-autenticação, esse contexto não nega o acesso à sua instância. A política selecionada nesse contexto tem precedência sobre configurações baseadas em usuário ou em função para autenticação multifator.

Para acessar o contexto de MFA, navegue até **Todos** > **Autenticação multifator** > **Contexto de MFA**.

Use os campos no registro de contexto da política de pós-autenticação para definir como sua instância usa a política.

Nota:

- Se a política padrão for a **Política de MFA em etapa crescente**, a autenticação multifator será mostrada aos usuários caso a política configurada na **Política de MFA em etapa crescente** seja avaliada como verdadeira. A política tem precedência sobre a configuração baseada em função ou em usuário.
- A MFA com login SSO estará disponível apenas se a propriedade `glide.authenticate.mfa.with.multisso.enabled` estiver definida como verdadeira.
- Você pode navegar até o registro da Política de autenticação para adicionar ou editar as "Entradas de política" nos campos de política referenciados (**Política de MFA em etapa crescente** ou **Política de MFA em etapa decrescente**).

Formulário de contexto de MFA

Campo	Descrição
Nome	Nome do contexto da política. Este campo é estático e não pode ser alterado.
Descrição	Descrição do contexto
Política padrão	Define o comportamento padrão desse contexto ao avaliar a política. Selecione uma das seguintes opções. Política de MFA em etapa crescente Aplica a MFA aos usuários quando as condições de política definidas no campo **Política de MFA em etapa crescente** são avaliadas como verdadeiras. Política de MFA em etapa decrescente Aplica a MFA por padrão. A MFA não é aplicada apenas quando as condições de política definidas no campo **Política de MFA em etapa decrescente** são avaliadas como verdadeiras.
Política de MFA em etapa crescente	A política usada nesse contexto. Este campo aparece somente quando o campo **Política padrão** está definido como **Política de MFA em etapa crescente**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formulário de contexto de MFA

Campo	Descrição
Política de MFA em etapa decrescente	A política usada nesse contexto. Este campo aparece somente quando o campo **Política padrão** está definido como **Política de MFA em etapa decrescente**.

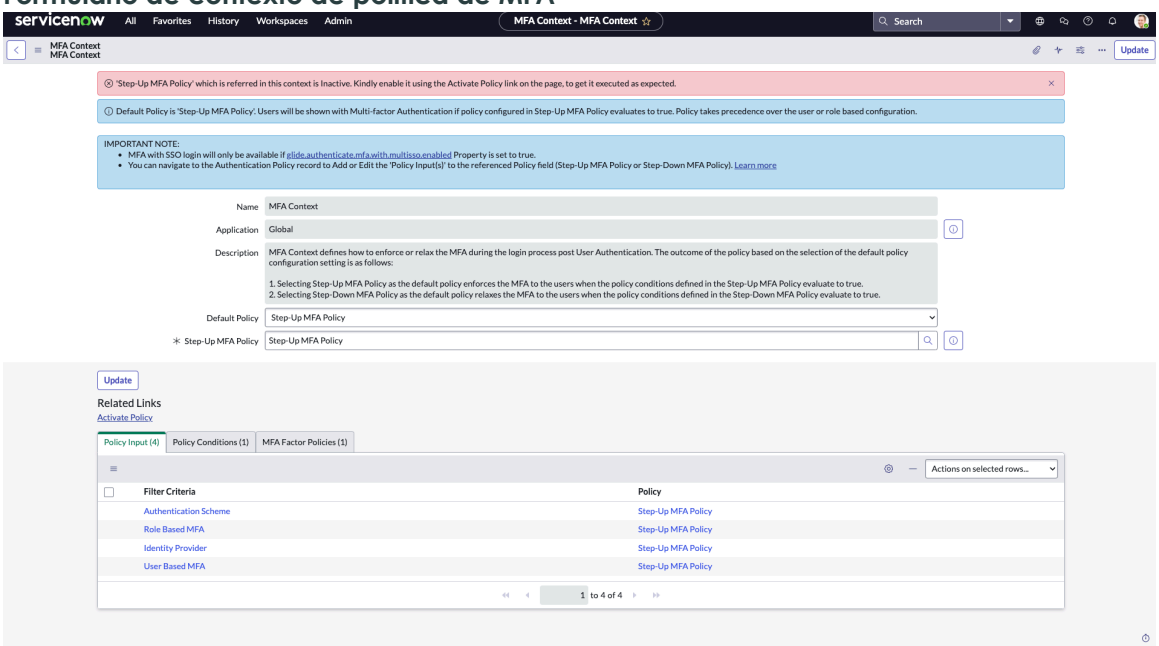
Entradas e condições da política

As guias **Entradas de política** e **Condições de política** exibem as entradas e as condições da política selecionada no campo **Política de MFA em etapa crescente** ou **Política de MFA em etapa decrescente**. Essas guias servem como referência, mas não podem ser usadas para mudar as entradas ou condições da política. Para modificar as configurações da sua política, navegue até ela usando o ícone de referência (ⓘ) ao lado do campo **Política de MFA em etapa crescente** ou **Política de MFA em etapa decrescente**.

Nota: As condições de política podem ser criadas aqui, mas como prática recomendada, é recomendável adicionar novas condições de política na página de política.

Este exemplo mostra um registro de contexto de MFA configurado usando uma política de MFA em etapa crescente. Essa política padrão significa que a MFA é aplicada apenas quando as condições definidas na política são avaliadas como verdadeiras. O contexto usa uma política chamada **Política de MFA em etapa crescente**, que tem um conjunto de entradas e condições que são exibidas nas guias **Entrada de política** e **Condição de política**.

Formulário de contexto de política de MFA



Contexto de recuperação de conta

O contexto de recuperação de conta usa uma política para definir como e quando a recuperação de conta pode ser estabelecida.

Os administradores podem exibir e modificar esse contexto e a política associada navegando até **SSO de vários provedores** > **Recuperação de conta** > **Contexto de recuperação de conta**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Por padrão, a política é a **Política de permissão**. Por padrão, o login é restrito para os usuários e será permitido somente se as condições definidas na **Política de permissão** forem avaliadas como verdadeiras.

Use os campos no registro de contexto de recuperação de conta para definir como sua instância usa a política.

Formulário de contexto de recuperação de conta

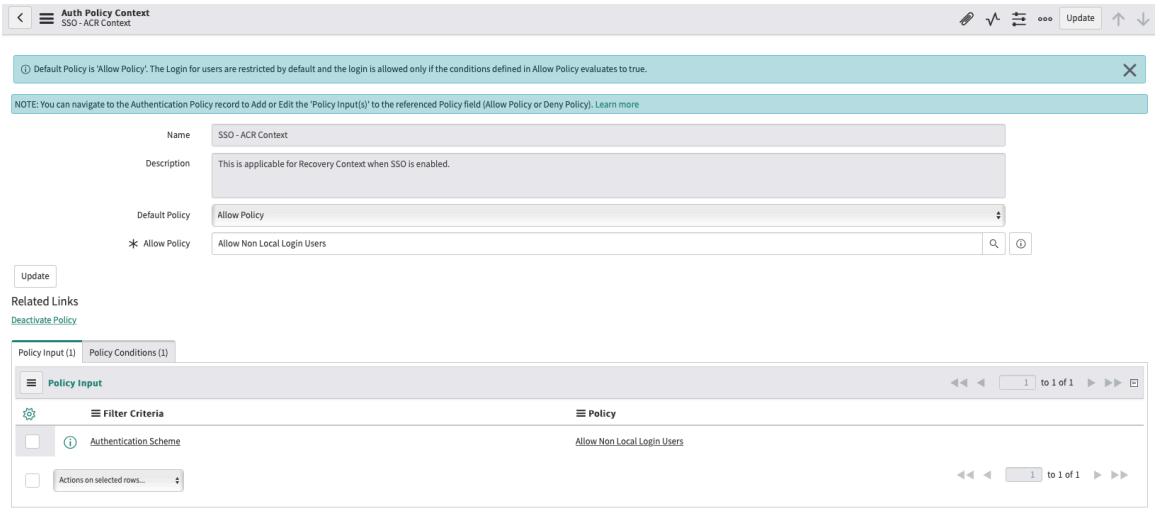
Campo	Descrição
Nome	Nome do contexto da política. Este campo é estático e não pode ser alterado.
Descrição	Descrição do contexto
Política padrão	Define o comportamento padrão desse contexto ao avaliar a política. Selecione uma das seguintes opções: • Política de permissão • Política de negação
Política de permissão	Este campo aparece somente quando o campo **Política padrão** está definido como **Política de permissão**.
Política de negação	Este campo aparece somente quando o campo **Política padrão** está definido como **Política de negação**.

Entradas e condições da política

As guias **Entradas de política** e **Condições de política** exibem as entradas e as condições da política selecionada no campo **Política de permissão** ou **Política de negação**. Essas guias servem como referência, mas não podem ser usadas para mudar as entradas ou condições da política. Para modificar as configurações da sua política, navegue até ela usando o ícone **Visualizar este registro** situado ao lado do campo **Política de permissão** ou **Política de negação**.

Nota: As condições de política podem ser criadas aqui, mas como prática recomendada, é recomendável adicionar novas condições de política na página de política.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Contexto de validação de sessão

Use o Contexto de validação de sessão como uma camada adicional de proteção contra sequestro de sessão ou de cookies.

Você pode usar o Contexto de validação de sessão com a estrutura de política Autenticação adaptável. A estrutura utiliza políticas de autenticação para avaliar as solicitações de autenticação para negar ou permitir o acesso com base nas entradas e condições da política.

A política de Contexto de validação de sessão pode ser utilizada em conjunto com a política de pós-autenticação, em que o administrador pode impor restrições de IP a todos ou determinados usuários durante a sessão conectada.

O recurso de Contexto de validação de sessão avalia os endereços IP com base nas condições definidas e permite acesso à instância em uma sessão. Os resultados do Contexto de validação de sessão são os seguintes:

- Política de negação: definir a política de negação de acesso como a política padrão permite que os usuários continuem a sessão por padrão. A sessão é encerrada somente quando uma das condições de política definidas na política de negação de acesso é avaliada como verdadeira.
- Política de permissão: definir a política de permissão de acesso como a política padrão encerra a sessão do usuário imediatamente, a menos que uma das condições de política definidas na política de permissão de acesso seja avaliada como verdadeira.

Nota:

- Por padrão, o Contexto de validação de sessão de uma política de autenticação é definido como **Política de permissão**.
- O Contexto de validação de sessão é implementado por meio da Política de permissão. Não é recomendável definir o contexto como Política de negação.

O Contexto de validação de sessão funciona com base no seguinte mecanismo:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Captura o endereço IP do usuário na criação da sessão a partir da solicitação do usuário e o armazena na sessão e no banco de dados.
- Rejeita uma solicitação quando o endereço IP difere daquele da sessão ou fora dos intervalos de IP válidos definidos pelo cliente que você definiu.

Nota: O Contexto de validação da sessão:

- Está somente disponível para usuários autenticados.
- Não é aplicável a sessões de usuário convidado ou aplicativos para celular nativos.
- É opcional e com base no requisito de que ele pode ser configurado.
- É somente executado para solicitações após o login.

Benefícios da validação de sessão

O Contexto de validação de sessão oferece os seguintes benefícios:

- Restringe o acesso a ServiceNow® quando os sequestradores copiam os cookies da sessão do usuário de um dispositivo para outro para representar a sessão.
- Restringe o acesso à sessão do usuário se ele estiver usando uma rede não segura.
- Configura as diversas regras e intervalos de IP por grupo de usuários ou função para logins de usuário.

Registro de contexto de validação de sessão

As políticas no contexto de validação da sessão executam as solicitações após o login.

Use os campos no registro de contexto da política de validação de sessão para definir como sua instância usa a política.

Formulário de contexto de validação de sessão

Campo	Descrição
Nome	Nome do contexto da política. Este campo é estático e não pode ser alterado.
Descrição	Descrição do contexto.
Política padrão	Define o comportamento padrão desse contexto ao avaliar a política. Selecione uma das seguintes opções. Política de permissão Nega o acesso a todos os usuários por padrão e só permite o acesso quando as condições no campo **Política de permissão** são avaliadas como verdadeiras. Política de negação Permite o acesso a todos os usuários por padrão e só nega o acesso quando as condições no campo **Política de negação** são avaliadas como verdadeiras.
Política de permissão	A política usada nesse contexto. Este campo aparece somente quando o campo **Política padrão** está definido como **Política de permissão**.
Política de negação	A política usada nesse contexto. Este campo aparece somente quando o campo **Política padrão** está definido como **Política de negação**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você pode escolher a **Política de validação de sessão** como Política de permissão ou Política de negação com base na entrada e nas condições da política.

Nota:

Você só pode usar os critérios de filtro IP, Função e Grupo para a política de Validação de sessão.

Entradas e condições da política

As guias **Entradas de política** e **Condições de política** exibem as entradas e as condições da política selecionada no campo **Política de permissão** ou **Política de negação**. Essas guias servem como referência, mas não podem ser usadas para mudar as entradas ou condições da política. Para modificar sua política, navegue até ela usando o ícone de referência ( ) ao lado do campo **Política de permissão** ou **Política de negação**.

Ativar contexto de validação de sessão

Use o Contexto de validação de sessão para restringir o acesso à ServiceNow® quando agentes mal-intencionados copiarem os cookies de sessão de um usuário de um dispositivo para outro para representar a sessão ou restringir o acesso à sessão do usuário se ele estiver usando uma rede não segura.

Antes de Iniciar

Função necessária: administrador

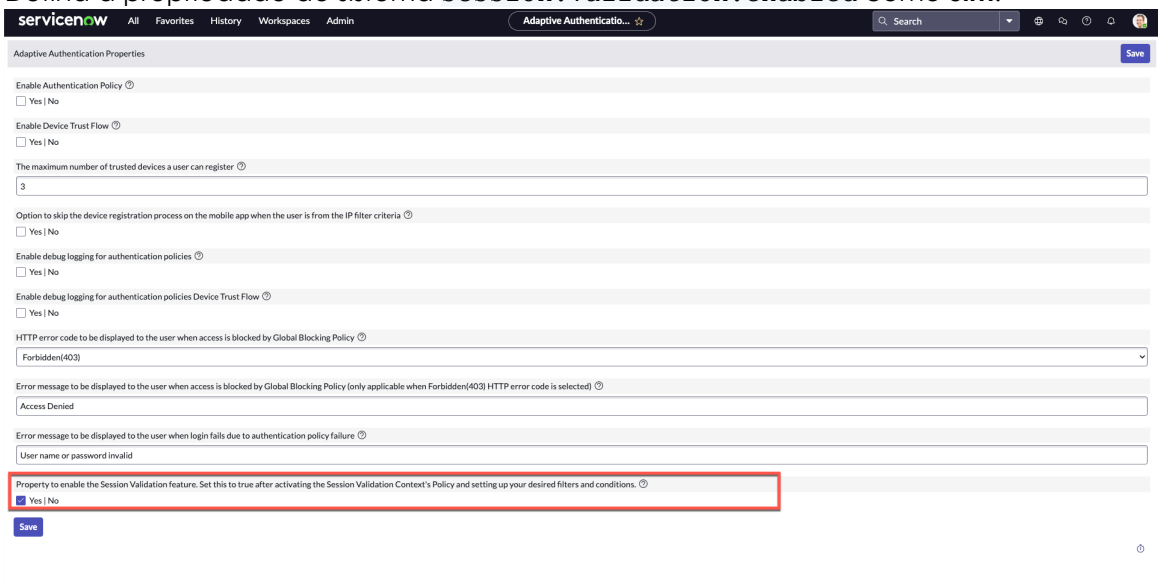
Para usar a validação de sessão, você deve seguir as seguintes etapas:

Procedimento

1. Navegar até **Todos** > **Autenticação adaptável** > **Políticas de autenticação** > **Todas as políticas**.
2. Selecione a **Política de validação de sessão** na página Políticas (`sys_authentication_policy_list.do`).
3. Especifique as **Entradas da política** e **Condições da política**.
4. Defina as condições como **verdadeiras** ou **falsas** para os filtros que você adicionou.
5. Marque a caixa de seleção **Ativo** para ativar a política depois que você configurar a Política de validação de sessão com entradas e condições de política.
6. Marque uma caixa de seleção **Forçar AuthnRequest** para o provedor de identidade padrão na tabela sso_properties se a instância tiver o SSO configurado.
7. Navegar até **Todos** > **Autenticação adaptável** > **Políticas de autenticação** > **Propriedades**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

8. Defina a propriedade do sistema `session.validation.enabled` como **Sim**.



Resultados

O recurso de Validação de sessão será ativado. É possível configurar as entradas e condições da política para que a política use o recurso. Para saber mais, consulte Tutorial: como configurar a validação de sessão.

Tutorial: como configurar a validação de sessão

Configure a validação de sessão na estrutura de Autenticação adaptável para criar uma camada adicional de proteção contra sequestro de sessão ou de cookies.

Antes de Iniciar

Função necessária: administrador

Plug-in necessário: **Autenticação adaptável** (com.snc.adaptive_authentication)

Para configurar a validação de sessão, você deve seguir as seguintes etapas:

Procedimento

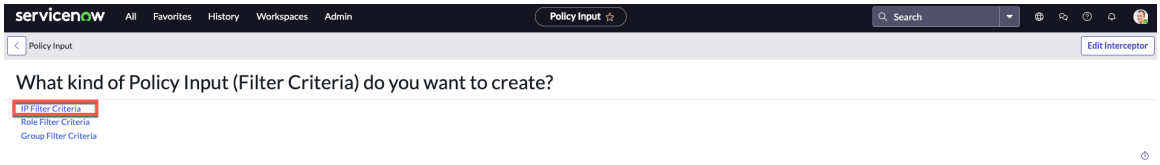
1. Navegar até **Todos** > **Autenticação adaptável** > **Políticas de autenticação** > **Todas as políticas**.
2. Selecione a **Política de validação de sessão** na página Políticas (`sys_authentication_policy_list.do`).
3. Selecione **Entradas de política**.

   a. Selecione **Novo** ou **Editar**.

   b. Escolha o tipo de entrada de política (critérios de filtro) que você deseja criar.

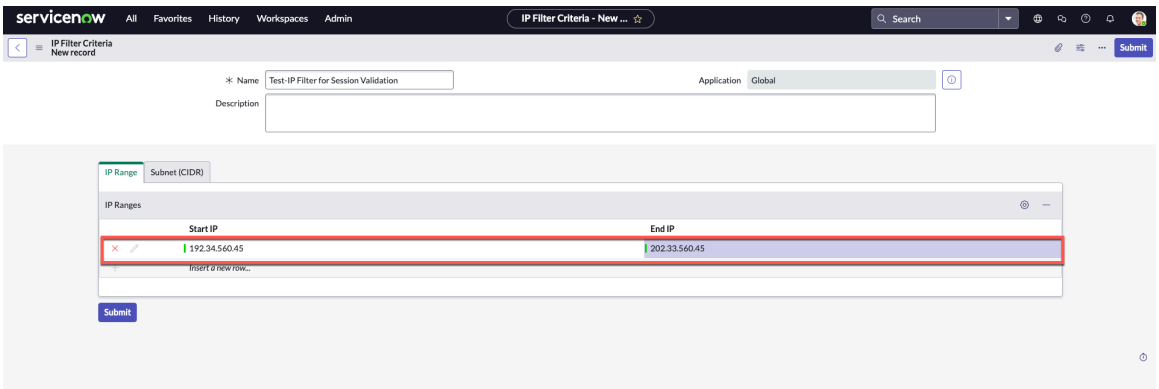
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

As opções disponíveis são Critérios de filtro de IP, Função e de Grupo. Escolha **Critério de filtro de**



IP.

c. Preencha o formulário com os detalhes do filtro e informe o **Intervalo de IPs**.



Para saber mais sobre como criar um filtro de IP, consulte Como criar critérios de filtro por IP.

d. Selecione **Enviar**.

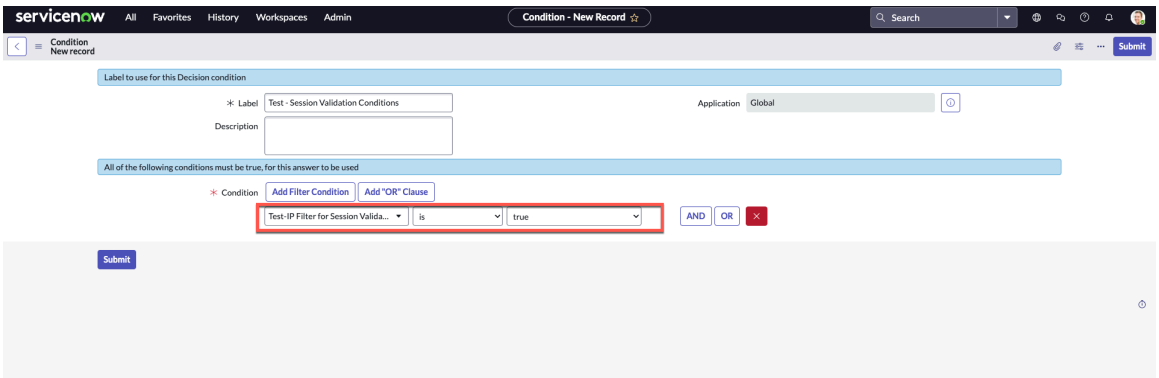
4. Selecione **Condições de política** na página Política de validação de sessão.

a. Selecione **Novo**.

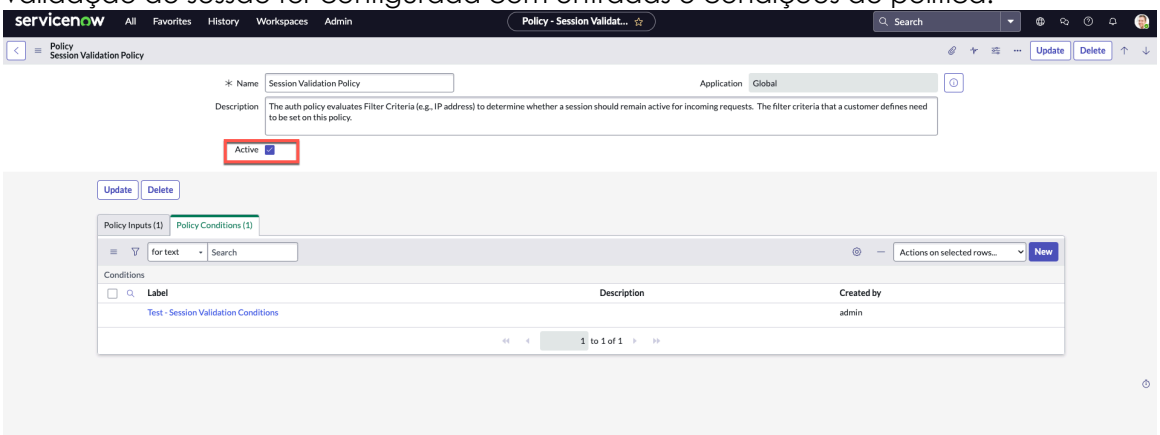
b. Preencha o formulário e defina a Condição para a entrada de política.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

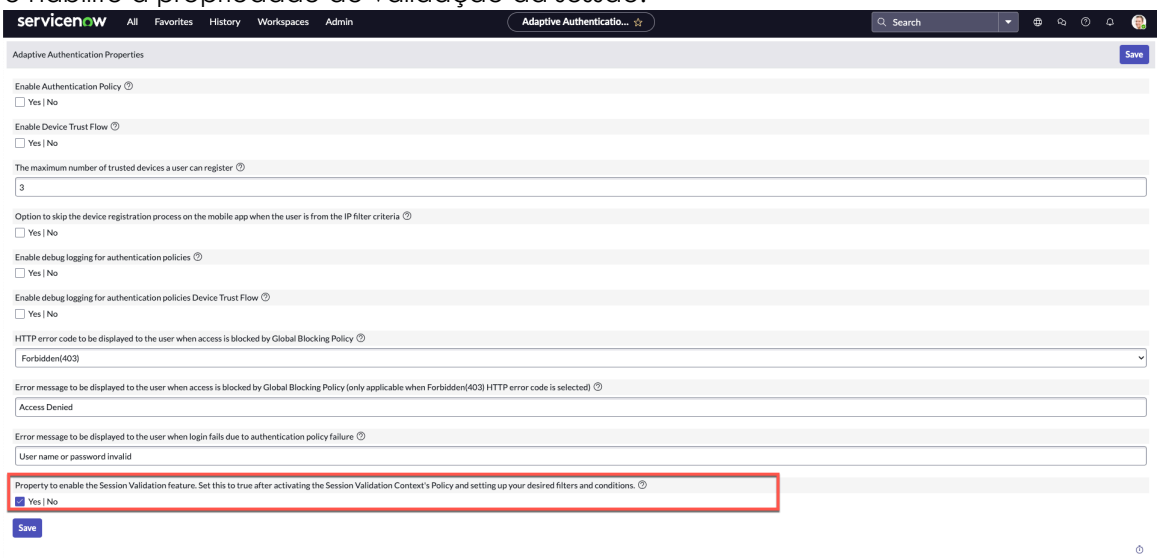
Nota: Você pode definir as condições como `verdadeiras` ou `falsas` com base na configuração da entrada de política. Neste exemplo, foi definida como `verdadeira`. Neste caso, definir a condição como verdadeira permite que somente o usuário com o endereço IP configurado faça login.



5. Marque a caixa de seleção `Ativo` para ativar a política depois que a Política de validação de sessão for configurada com entradas e condições de política.



6. Navegar até **Todos** > **Autenticação adaptável** > **Políticas de autenticação** > **Propriedades** e habilite a propriedade de validação da sessão.



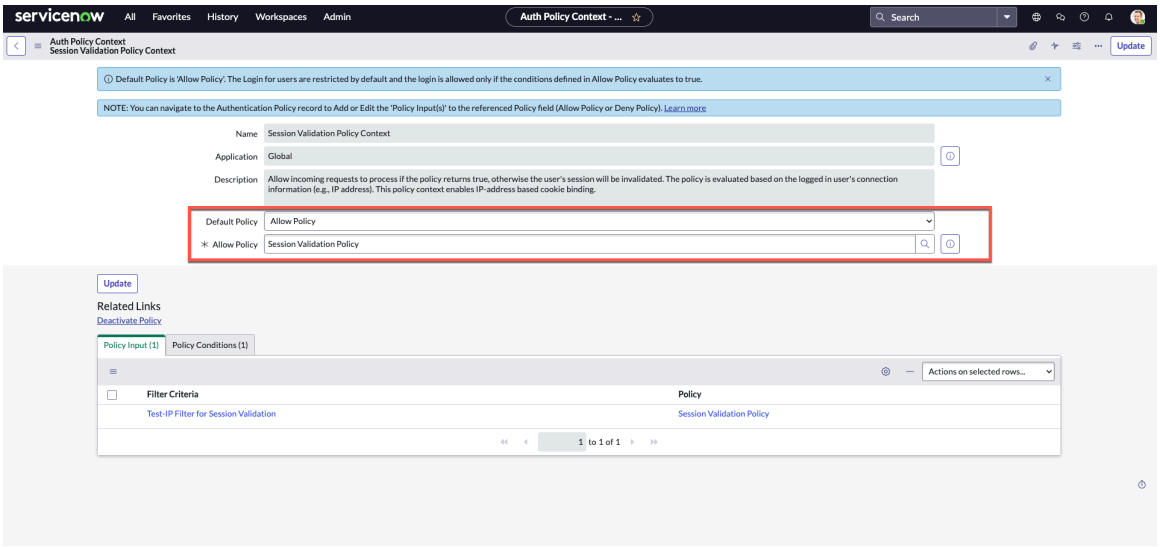
7. Navegue até **Todos** > **Autenticação adaptável** > **Contextos da política de autenticação** > **Contexto da validação de sessão**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

8. Configure a Política padrão como **Política de permissão** ou **Política de negação** para definir o contexto de validação da sessão de acordo com a entrada e as condições da política.

   Nota: Por padrão:

   - O contexto de validação da sessão é definido como **Política de permissão**.
   - A Política de permissão está selecionada como **Política de validação de sessão**.



Resultados

A configuração avalia a sessão de login com base no seguinte:

- Restringe o acesso à instância ServiceNow® quando os sequestradores copiam os cookies da sessão do usuário de um dispositivo para outro para representar uma sessão.
- Restringe o acesso à sessão do usuário se ele estiver usando uma rede não segura.

Políticas de autenticação

As políticas de autenticação avaliam as solicitações de autenticação com base nas condições de política especificadas e permitem ou negam o acesso, dependendo da saída da avaliação das condições de política. Por exemplo, o acesso será permitido somente se todas as condições de política especificadas na **Política de permissão de acesso** forem avaliadas como verdadeiras.

Use as políticas de autenticação internas ou crie uma política de autenticação de acordo com seus requisitos de segurança. Você pode encontrar as políticas da sua instância navegando até **Autenticação adaptável** > **Políticas de autenticação** > **Todas as políticas**.

Nota: A qualquer momento, a Política de permissão de acesso ou a Política de negação de acesso podem ser executadas, mas não ambas.

Política	Descrição
Política de permissão de acesso	Nega todas as solicitações de autenticação por padrão. Permite somente as solicitações de autenticação que correspondem às condições de política especificadas.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Política	Descrição
Política de pré-autenticação de permissão de acesso	Permite a política de pré-autenticação de acesso.
Permissão para que usuários não locais façam login	Escolha esta política para permitir que usuários que não sejam locais façam login. Usado no contexto de fluxos de recuperação do SSO.
Política de negação de acesso	Permite as solicitações de autenticação por padrão. Nega somente as solicitações de autenticação que correspondem às condições de política especificadas.
Política de bloqueio global	Nega as solicitações de acesso de usuários e APIs antes da autenticação. Esta política pode ser usada como uma alternativa ao Controle de acesso de endereços IP.
Política de validação de sessão	A política de autenticação avalia os critérios de filtro (por exemplo, endereço IP) para determinar se uma sessão deve permanecer ativa para as solicitações de entrada. Você deve definir os critérios de filtro nesta política.
Política de negação de login local	Escolha esta política para bloquear todos os logins locais. Usado no contexto de fluxos de recuperação do SSO.
Política de MFA em etapa decrescente	Escolha a **Política de MFA em etapa decrescente** como a política padrão em situações em que os usuários não precisam de autenticação MFA. Quando as condições de política definidas na Política de MFA em etapa crescente são avaliadas como verdadeiras, os usuários não precisam fazer login usando a MFA.
Política de MFA em etapa crescente	Escolha a **Política de MFA em etapa crescente** como a política padrão para exigir a autenticação de MFA quando as condições da política definidas nessa Política forem avaliadas como verdadeiras.

Como configurar uma política de autenticação

Configure uma política de autenticação para definir entradas e condições a serem usadas para conceder acesso a uma instância ou aplicar a autenticação multifator.

Antes de Iniciar

Função necessária: administrador

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Autenticação adaptável** > **Políticas de autenticação** > **Todas as políticas**.

   Nota: Para ver exemplos de políticas concluídas, você pode avaliar estas políticas em sua instância:

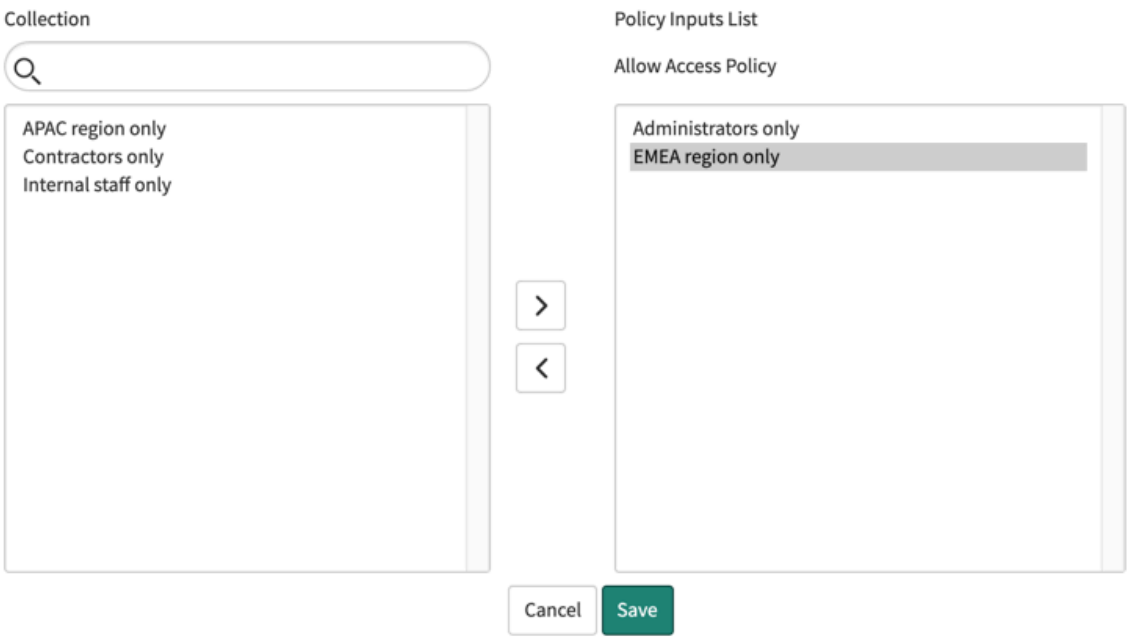
   - POLÍTICA DE DEMONSTRAÇÃO: permite login local somente para administradores do intervalo de IPs confiáveis
   - POLÍTICA DE DEMONSTRAÇÃO: permite login local somente para administradores
   - POLÍTICA DE DEMONSTRAÇÃO: restringe a autenticação baseada em nome de usuário e senha para usuários específicos

2. Clique no botão **Novo** para criar um novo registro de política.
3. No formulário da **Política**, preencha os seguintes campos.

Formulário de política

Campo	Descrição
Nome	Nome da sua política.
Aplicação	A aplicação com escopo para a política. Este campo é preenchido automaticamente com a aplicação atual.
Descrição	Descrição da política
Ativo	Se esta política está ativa.

4. Na guia **Entradas de política**, clique em **Editar**.
5. Selecione um ou mais critérios de filtro na lista **Coleção** e mova-os para a **Lista de entradas de política** na **Política de permissão de acesso**.



Nota: Para obter informações sobre como criar seus próprios critérios de filtro para usar nesta seção, consulte Critérios de filtro.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

6. Na guia **Condições da política**, clique em **Novo**.
7. No formulário, preencha os campos:

Formulário de condições

Campo	Descrição
Rótulo	Nome para identificar a condição.
Descrição	Descrição da condição.
Condição	Combinação lógica de várias entradas de política (critérios de filtro) para avaliar solicitações de autenticação. Por exemplo, você pode criar condições que permitem somente prestadores de serviços de uma lista de endereços IP confiáveis.

8. Opcional: Repita a etapa 7 para criar condições de política adicionais.

> **Nota:** Se várias condições de política forem criadas, a saída final da política de acesso dependerá da lógica OU da saída de todas as condições de política. Isso significa que a política será avaliada como verdadeira se qualquer uma das condições de política for atendida.

9. Clique em **Salvar**.

Como adicionar uma política de autenticação a um contexto de política de autenticação

Adicione uma política de autenticação a um dos contextos de política de autenticação. O contexto de autenticação usa as entradas e condições da política para determinar se os usuários têm acesso concedido à instância ou se a MFA é aplicada aos usuários.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Navegue até **Todos** > **Autenticação adaptável** > **Contextos da política de autenticação** e selecione uma das entradas de acordo com suas necessidades.

   Contexto de pré-autenticação

   Use o contexto de pré-autorização para avaliar sua política antes que o usuário veja a tela de login. Os usuários têm acesso concedido ou negado com base nesta avaliação.

   Contexto de pós-autenticação

   Use o contexto de pós-autorização para avaliar sua política depois que o usuário inserir as credenciais de login. Os usuários têm acesso concedido ou negado com base nesta avaliação. Como ela ocorre depois que a instância identifica o usuário, as políticas nesse contexto podem fazer a avaliação com base nos dados do usuário, como a função ou grupo que pertencem.

   Contexto de MFA

   Use o contexto da MFA para determinar se um usuário deve usar a autenticação multifator ao fazer login.

   Contexto de validação de sessão

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Use o contexto de validação de sessão para avaliar o endereço IP configurado com base nas condições definidas como um filtro e permitir o acesso à instância em uma sessão.

2. No campo **Política padrão**, selecione um valor.
   O valor neste campo determina como o contexto usa o resultado das condições da sua política.

   As opções disponíveis neste campo dependem do contexto selecionado. Para obter detalhes sobre esses contextos, consulte Contextos da política de autenticação.

3. Atribua uma política ao contexto.
   O nome do campo depende do contexto selecionado.

   Contexto de pré-autenticação e de pós-autenticação

   Esses contextos têm um campo de **Política de negação** ou **Política de permissão**, dependendo da seleção no campo **Política padrão**.

   Contexto de MFA

   Esses contextos têm um campo de **Política de MFA em etapa crescente** ou **Política de MFA em etapa decrescente**, dependendo da seleção no campo **Política padrão**.

   Contexto de validação de sessão

   Este contexto tem um campo de **Política de permissão** ou **Política de negação**, dependendo da seleção no campo **Política padrão**.

4. Clique em **Atualizar**.
   Depois de atualizar o registro, você pode ver as entradas e as condições da política nas guias **Entrada de política** e **Condições de política**.

Eventos de autenticação adaptável

É possível usar a tabela de eventos de autenticação adaptável para se informar sobre os eventos.

Abaixo, há alguns dos logs que é possível rastrear na tabela de eventos de autenticação adaptável:

- `glide.adaptive.auth.log.success.event`: para conhecer os eventos `success` de pós-autenticação e logins na API.
- `glide.adaptive.auth.log.mfa.relax.event`: para conhecer os eventos `mfa_relaxation` do contexto de MFA.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

- Para o contexto pré-autenticação, políticas de acesso à REST API do tipo "`pre_auth`": por padrão, há o registro em log dos eventos de `falha`. `Não é possível` registrar eventos de `sucesso` em log.
- Para o contexto pós-autenticação, políticas de acesso à REST API com um tipo diferente de "`pre_auth`": por padrão, há o registro em log dos eventos de `falha`. Para que ocorra o registro em log dos eventos de `sucesso`, é necessário ativar a propriedade `glide.adaptive.auth.log.success.event`.
- Para MFA: por padrão, há o registro em log dos eventos de `Imposição de MFA`.
- Para que ocorra o registro em log dos eventos de Abrandamento de MFA, é necessário ativar a propriedade `glide.adaptive.auth.log.mfa.relax.event`. O evento de `Abrandamento de MFA` registraria em log o mesmo evento que `Imposição de MFA`, mas com o campo `Resultado` preenchido com `Falso`.

Como configurar as propriedades da autenticação adaptável

Depois de ativar a Autenticação adaptável, configure as propriedades da autenticação adaptável de acordo com seus requisitos de segurança.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Navegar até **Todos** > **Autenticação adaptável** > **Políticas de autenticação** > **Propriedades**.
2. Configure as seguintes propriedades:

Propriedades da autenticação adaptável

Propriedade	Descrição	Valor
Habilitar política de autenticação (glide.authenticate.auth.policy.enabled)	Opção para habilitar a política de autenticação	Sim | Não
Habilitar registro em log da depuração das políticas de autenticação (glide.authenticate.policy.debug)	Opção para habilitar registro em log de depuração nas políticas de autenticação.	Sim | Não
Código de erro HTTP que será exibido para o usuário quando o acesso estiver bloqueado pela Política de bloqueio global (glide.authenticate.global.blocking_policy.error_code)	Código de erro HTTP exibido durante o login quando a Política de bloqueio global bloqueia o login do usuário.	Selecione entre: ◦ Proibido (403) ◦ Não encontrado (404)
Mensagem de erro que será exibida ao usuário quando o acesso estiver bloqueado pela Política de Bloqueio Global (somente aplicável quando o código de erro HTTP "Proibido (403)" for selecionado) (glide.authenticate.global.blocking_policy.error_message)	Mensagem de erro exibida quando a Política de bloqueio global bloqueia o acesso.	Campo de texto
Habilitar fluxo de confiança do dispositivo (glide.authenticate.preauth.allow.trusted.device)	Opção para habilitar o fluxo de dispositivo confiável.	Sim | Não

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Propriedade	Descrição	Valor
Número máximo de dispositivos confiáveis que um usuário pode registrar (glide.trusted.device.max.count)	É o número máximo de dispositivos confiáveis que um usuário pode registrar.	Campo de texto
Ignorar o registro do dispositivo para o fluxo de confiança do dispositivo se o usuário for da rede confiável (glide.authenticate.preauth.skip.user.registration)	Opção para ignorar o registro se o usuário estiver tentando se registrar na rede confiável	Sim | Não
Propriedade para habilitar o recurso de validação de sessão. Defina como verdadeiro depois de ativar a política do contexto de validação de sessão e configurar os filtros e condições desejados (session.validation.enabled)	Opção para habilitar o recurso de validação de sessão. Defina como verdadeiro depois de ativar a política do contexto de validação de sessão e configurar os filtros e condições desejados.	Sim | Não

Tutorial: como configurar uma autenticação adaptável

Use essas etapas de exemplo para configurar a autenticação adaptável em uma instância.

Para usar este tutorial, você deve ter uma instância com a Autenticação adaptável ativada. Para obter detalhes sobre esse processo, consulte Como ativar a autenticação adaptável.

Os exemplos orientarão você na criação de uma nova política e na aplicação a uma instância. Neste tutorial, você vai:

Criar um registro de critérios de filtro

Crie um registro de critérios de filtro por grupo para usar como uma entrada para sua política. Esse registro permite que sua política determine o acesso com base no grupo de um usuário. Nessas etapas, você define um ou mais grupos que a política usará para determinar o acesso.

Como criar uma política

Crie uma política que determina se um usuário pode acessar a instância. Essa política usa o registro de critérios de filtro por grupo criado como entrada. Nessas etapas, você também define condições de política que definem como a política usa a entrada de política para determinar o acesso do usuário.

Como configurar um contexto de política

Configure o **Contexto da política de pós-autenticação** para usar sua nova política. Quando configurada, sua instância nega acesso a usuários dentro do grupo definido no registro de critérios de filtro.

Criar um registro de critérios de filtro

Aprenda a criar um registro de critérios para usar como uma entrada de política para sua política de autenticação adaptável.

Antes de Iniciar

Função necessária: administrador

Para negar acesso à sua instância com base em grupos de usuários, você deve criar um registro de critérios de filtro por grupo. Esse registro define um grupo de usuários ou um conjunto de grupos de usuários que sua política pode conceder ou negar acesso. Neste

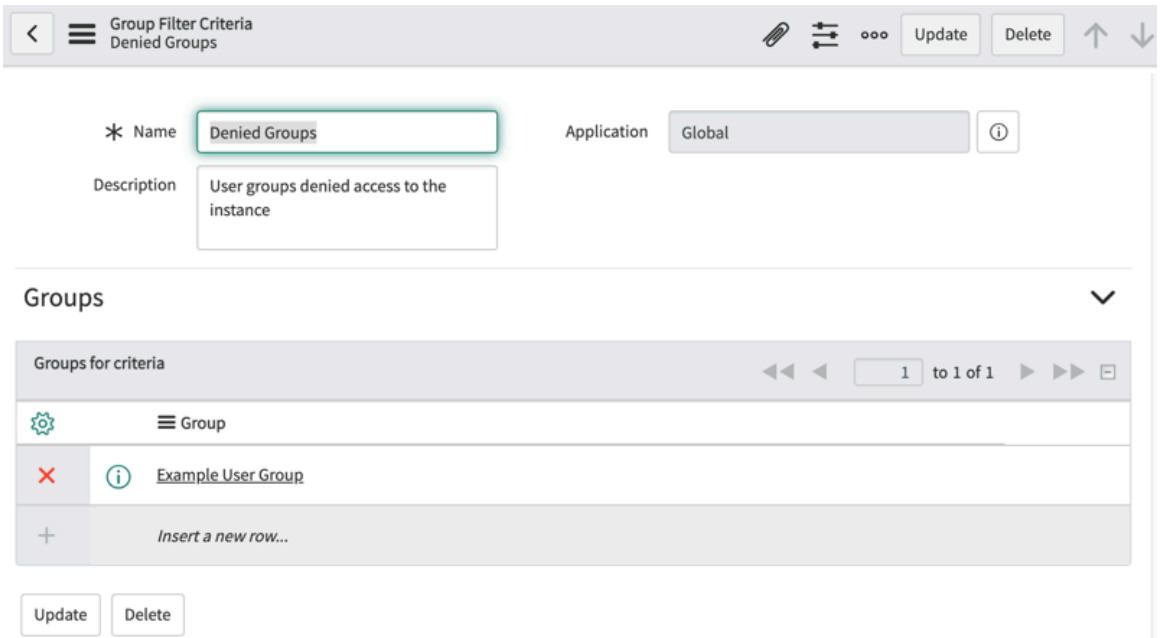
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

exemplo, você criará um registro de critérios de filtro por grupo para um único grupo de usuários.

Para obter detalhes sobre grupos de usuários e como eles são usados em sua instância, consulte Explorando a administração de usuários.

Procedimento

1. Navegue até **Todos** > **Autenticação adaptável** > **Critérios de filtro** > **Critérios de grupo**.
2. Clique em **Novo** para criar um novo registro.
3. No campo **Nome**, insira um nome para seu registro.
   Por exemplo, `Grupos negados`.
4. No campo **Descrição**, insira uma descrição resumida.
   Por exemplo, `Grupos de usuários têm acesso negado à instância`.
5. Na lista **Grupos para critérios**, clique duas vezes em **Inserir uma nova linha...**.
6. Insira o nome de um grupo de usuários ou clique no ícone de referência ( ) para selecionar um grupo de uma lista.
   Se quiser criar um novo grupo de usuários para seus critérios de filtro, clique no ícone de referência ( ) e, em seguida, clique no botão **Novo**. Para obter mais detalhes sobre como criar grupos de usuários, consulte Criar um grupo de usuários.
7. Depois de adicionar o grupo de usuários, clique em **Enviar** para salvar o registro de critérios.



Como criar uma política

Aprenda a criar uma política para negar acesso a grupos de usuários definidos em seus critérios de filtro por grupo.

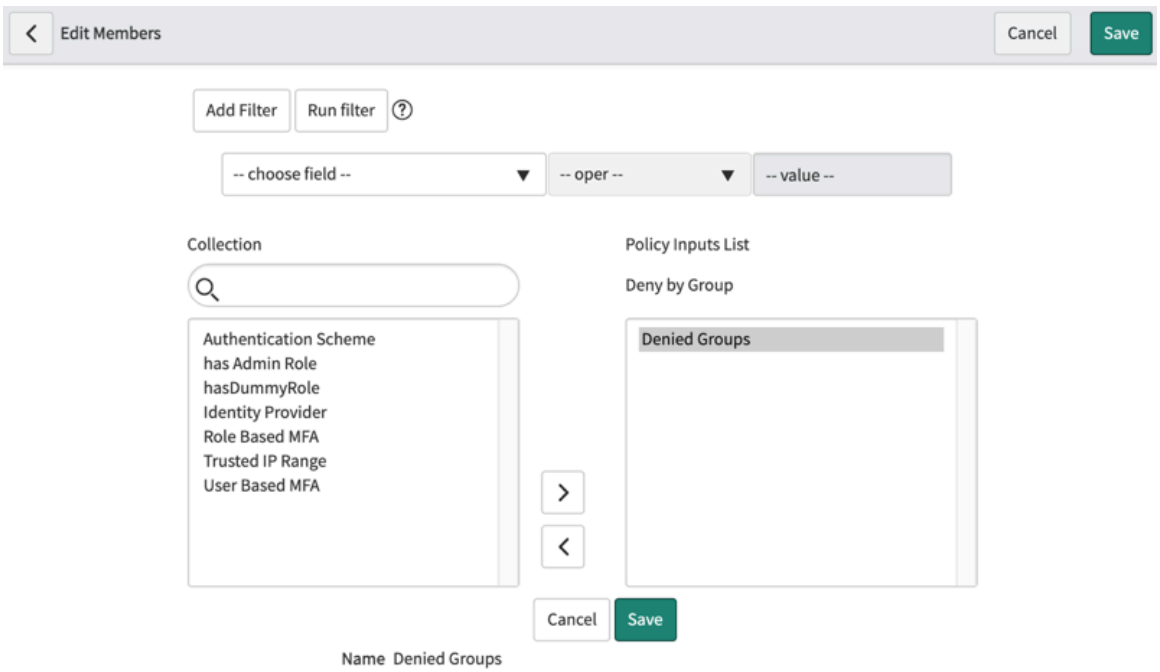
Antes de Iniciar

Função necessária: administrador

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

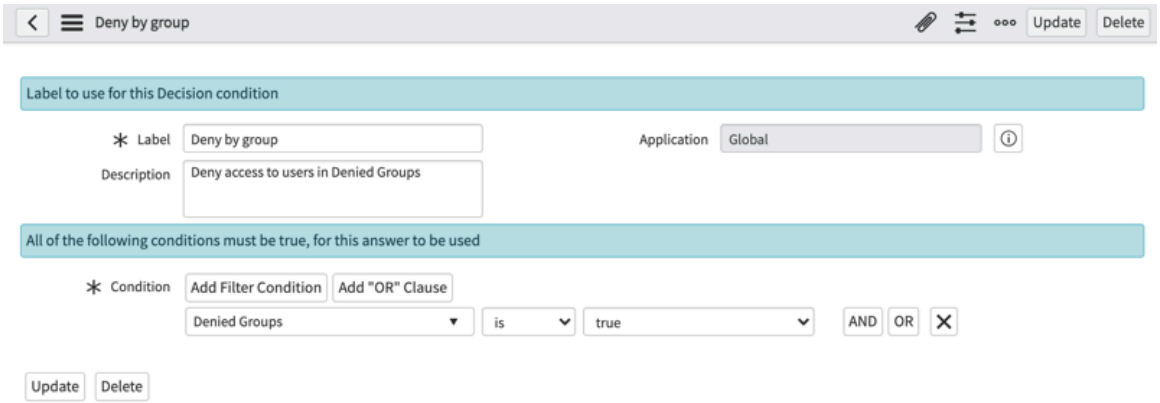
Procedimento

1. Navegar até **Todos** > **Autenticação adaptável** > **Políticas de autenticação** > **Todas as políticas**.
2. Na lista **Políticas**, clique em **Novo**.
3. No campo **Nome**, insira um nome para seu registro.
   Por exemplo, `Negado pelo grupo`.
4. No campo **Descrição**, insira uma descrição resumida.
   Por exemplo, `Grupos de usuários têm acesso negado à instância`.
5. Clique com o botão direito no cabeçalho do formulário e clique em **Salvar**.
   Depois de salvas, as listas de **Entradas de política** e **Condições de política** serão exibidas no formulário.
6. Na lista **Entradas de política**, clique em **Editar**.
7. No coletor de lista, adicione à sua política os critérios de filtro criados nas etapas anteriores.



8. Clique em **Salvar**.
   A instância salva a entrada de política e exibe o registro de política novamente.
9. Na lista **Condições de política**, clique em **Novo**.
10. No campo **Rótulo**, crie um rótulo para esta condição, por exemplo, `Negado pelo grupo`.
11. No campo **Descrição**, insira uma descrição resumida.
    Por exemplo, `Acesso negado aos usuários em grupos negados`.
12. No campo **Condição**, selecione os critérios de filtro criados nas etapas anteriores e selecione **é** e **verdadeiro** para concluir a condição.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



13. Clique em **Salvar**.

Como configurar um contexto de política

Configure o Contexto da política de pós-autenticação para usar sua nova política. Quando configurada, sua instância nega acesso a usuários dentro do grupo definido no registro de critérios de filtro.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. **Autenticação adaptável** > **Contextos da política de autenticação** > **Contexto de pós-autenticação**.
   Você deve usar o **Contexto de pós-autenticação** porque a política usada neste tutorial deve avaliar em que grupo um usuário está. Essas informações só estarão disponíveis depois que suas credenciais forem inseridas.
2. No campo **Política padrão**, selecione `Política de negação`.
   Essa seleção concede acesso aos usuários por padrão e só nega o acesso quando as condições da política forem avaliadas como verdadeiras.
3. No campo **Política de negação**, selecione a política criada nas etapas anteriores.
4. Clique em **Atualizar** para salvar o registro de contexto da política.

Autenticação adaptável para aplicativos para celular confiáveis

Acesse sua ServiceNow a partir de redes não confiáveis usando Aplicativo Now Mobile.

Autenticação adaptável para aplicativos para celular confiáveis

A Autenticação adaptável para aplicativos para celular confiáveis permite que os usuários acessem a instância ServiceNow usando Aplicativo Now Mobile. A instância está protegida por um limite de rede IP confiável.

A seguir estão alguns dos cenários em que você precisa de acesso à instância ao estar fora da rede.

Como funcionário, você precisa acessar o Aplicativo Now Mobile e a Central de serviços ao funcionário (portal) de fora da rede. O filtro do aplicativo Trusted Mobile permite que você identifique a solicitação de entrada originada de um Aplicativo Now Mobile confiável que está vinculado a uma conta de usuário.

Como administrador, você pode configurar a política. Ela permite que os usuários registrem seus dispositivos móveis e acessem a instância em uma rede confiável.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Como usuário, você pode registrar seu dispositivo móvel verificando o QR exibido na instância. Após o registro, você pode fazer login em sua instância a partir de Aplicativo Now Mobile ao usar suas credenciais.

Nota: Para registrar o dispositivo móvel, você precisa estar em uma rede confiável. Após o registro, você também pode fazer login na instância a partir de outras redes.

Recursos

Como administrador, você pode usar os seguintes recursos:

- Configuração de políticas usando critérios de filtro de aplicativos confiáveis.
- Criação de condições de política com um novo critério de filtro para aplicativos para celular confiáveis.
- Compatibilidade a todos os métodos de login no aplicativo para celular confiável para os usuários (login local, SAML, OIDC e MFA).
- Revogação de um dispositivo confiável.
- Adição de eventos de segurança para todas as ações de registro ou revogação do dispositivo. Os eventos podem ser usados para notificar o usuário.
- Compatibilidade a eventos de segurança para falhas de assinatura, falhas de validação de cookie, tokens inválidos, cabeçalhos inválidos ou parâmetros de consulta.
- Controle do número máximo de dispositivos registrados.
- Impedimento de um novo registro de dispositivo, a menos que o usuário remova um dispositivo emparelhado existente.
- Captura da última vez em que um dispositivo foi usado.

Como ativar o aplicativo Trusted Mobile

Ative a autenticação adaptável com o aplicativo Trusted Mobile usando a política de autenticação e as Condições do filtro.

Antes de Iniciar

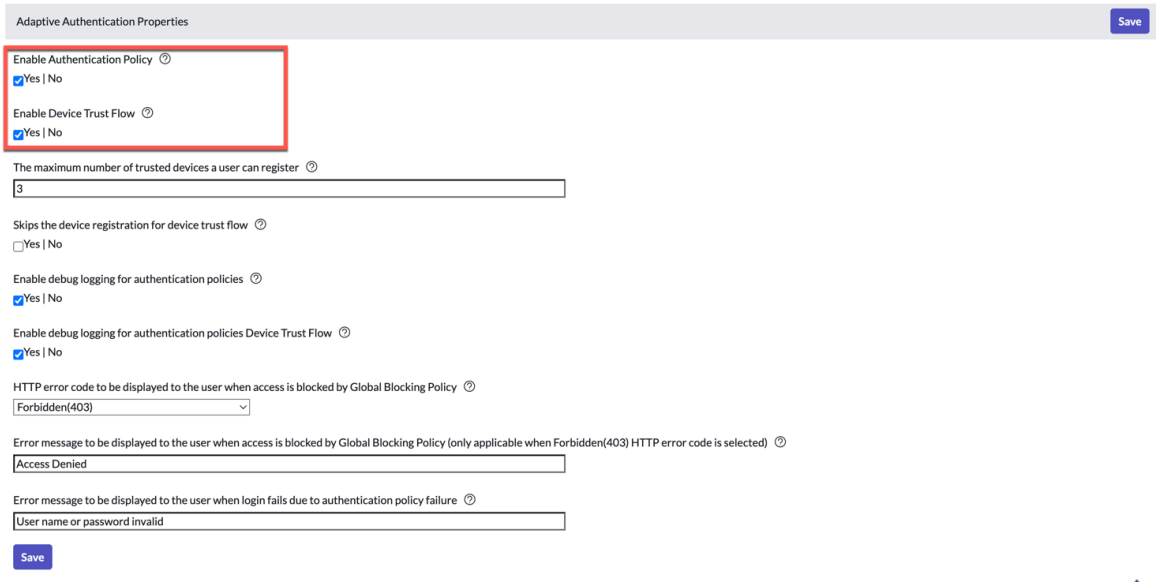
Verifique se o plug-in Adaptive Authentication (*com.snc.adaptive_authentication*) está instalado.

Função necessária: administrador

Procedimento

1. Navegar até **Todos** > **Autenticação adaptável** > **Políticas de autenticação** > **Propriedades**.
2. Na página Propriedades de autenticação adaptável, habilite as seguintes propriedades:
   - Habilitar a Política de autenticação (*glide.authenticate.auth.policy.enabled*)
   - Habilitar Fluxo de confiança do dispositivo (*glide.authenticate.preauth.allow.trusted.device*)

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Nota: Para desabilitar a propriedade de fluxo de confiança do dispositivo, você deve remover as condições com um filtro para dispositivo móvel confiável. Caso contrário, uma mensagem de erro será exibida para remover as condições.

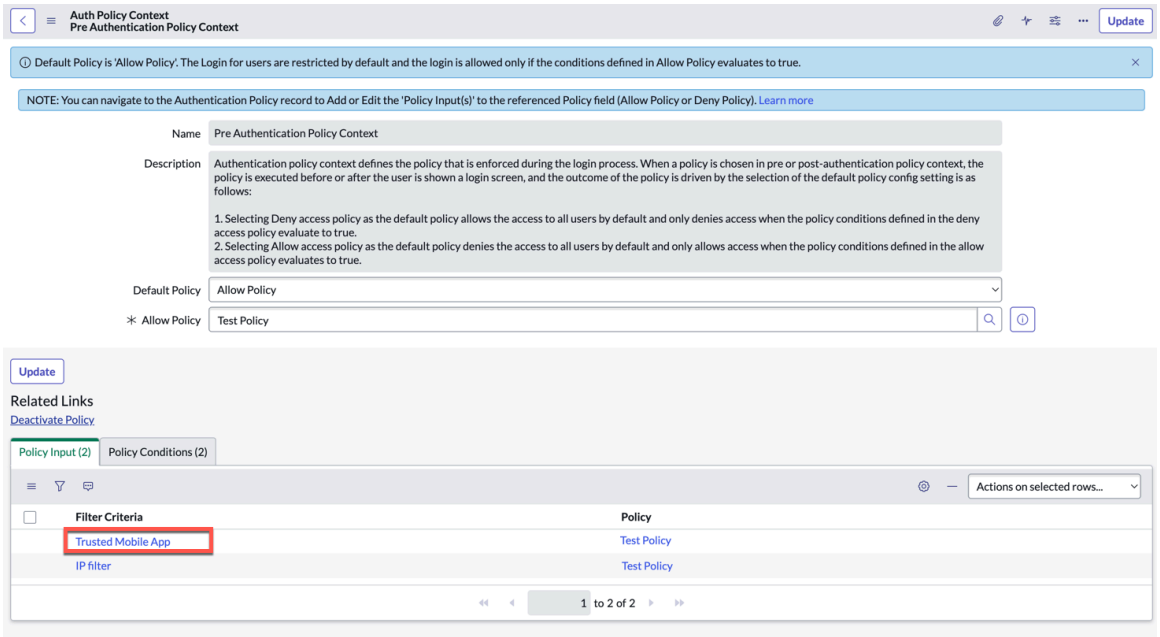
3. Navegue até **Todos** > **Autenticação adaptável** > **Contextos da política de autenticação** > **Contexto de pré-autenticação**.
4. Defina as condições no contexto de pré-autenticação.
   Para obter mais informações, consulte Contexto de pré-autenticação.

   Nota: Por padrão, a condição da política é **Política de negação**. Você pode mudar para **Política de permissão**. Essas políticas são diretamente opostas.

   - Com a **Política de permissão**, todos os usuários têm acesso negado por padrão, só permitindo o acesso quando as condições da política de permissão de acesso são verdadeiras.
   - Com a **Política de negação**, todos os usuários têm acesso permitido por padrão, só negando o acesso quando as condições da política de negação de acesso são verdadeiras.

   Na Entrada de política, o **aplicativo para celular Trusted** é uma entrada de política para o aplicativo para celular confiável.

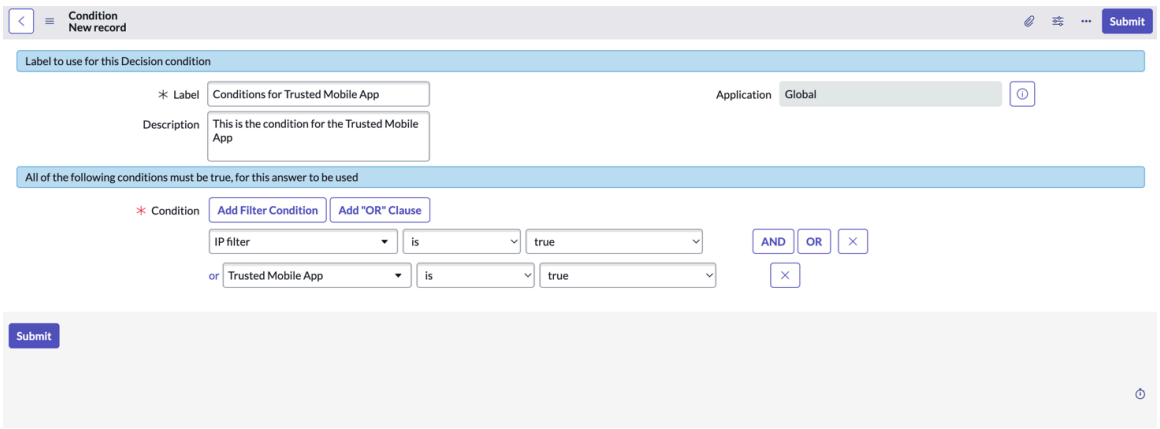
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Nas Condições de política, crie a condição clicando em **Novo**.
6. No formulário, preencha os seguintes campos.

Formulário de Condição do filtro

Campo	Descrição
Rótulo	Nome da condição
Descrição	Descrição da condição
Aplicação	Escopo da aplicação para este registro.
Condição	Condições baseadas em AND e OR. Como a Política de autenticação é a **Política de permissão**, a condição para o aplicativo Trusted Mobile é definida como verdadeira no exemplo mostrado na imagem.



7. Clique em **Enviar**.

Resultados

A entrada de política e as condições de filtro são criadas para o recurso Dispositivo confiável. Os usuários podem prosseguir com o uso do recurso Dispositivo confiável para

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

acessar a instância ServiceNow de redes não confiáveis usando o Aplicativo Now Mobile. Para obter mais informações, consulte Como registrar um dispositivo confiável.

Como registrar um dispositivo confiável

Registre um dispositivo confiável para acessar a instância ServiceNow fora da rede.

Antes de Iniciar

Você precisa estar na rede confiável para executar o registro do dispositivo confiável.

Função necessária: nenhuma

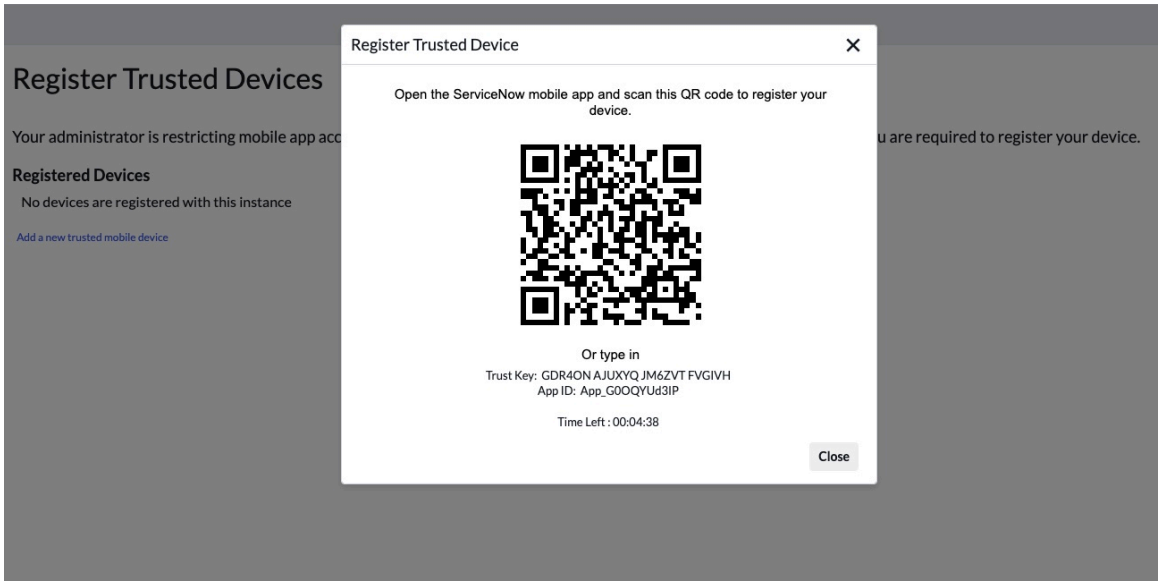
Procedimento

1. Navegue até uma das seguintes opções de menu:
   - Em Now Platform, navegue até **Todos** > **Autoatendimento** > **Meu perfil**.

     Nota: Você também pode acessar seu perfil clicando no nome de usuário no cabeçalho da instância.

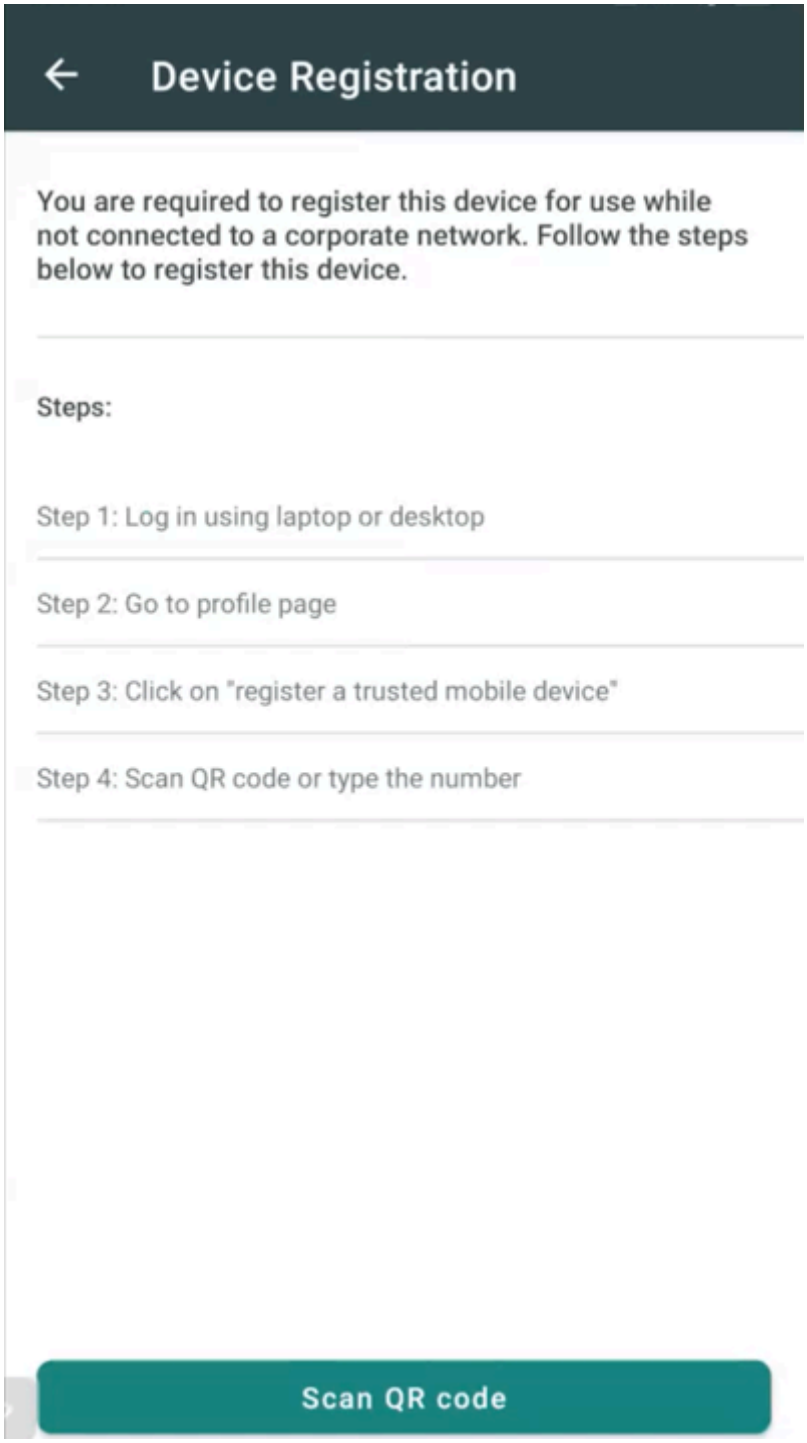
   - Em Now Support, clique no perfil e selecione **Dispositivo confiável**.
2. Em seu perfil de usuário, clique em **Registrar um dispositivo móvel confiável** na seção Links relacionados.
   A página Registrar dispositivos confiáveis será exibida.
3. Registre um novo dispositivo clicando em **Adicionar um novo dispositivo móvel confiável**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Na tela Registro do dispositivo no aplicativo para celular do ServiceNow, toque no botão **Verificar código QR** e verifique o código QR exibido em seu laptop ou desktop.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

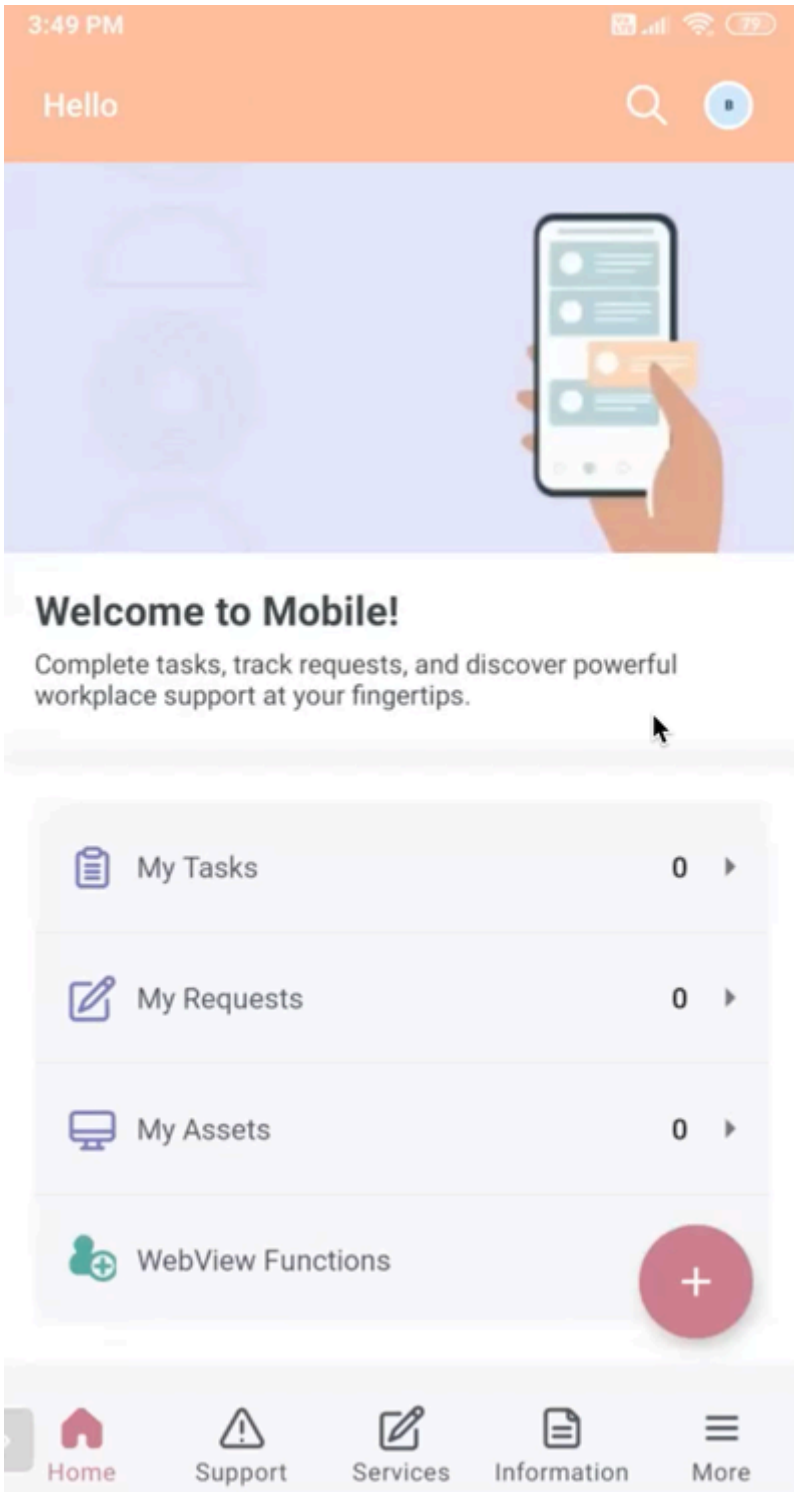


O processo de registro será concluído e você será solicitado a acessar a página de login para concluir a autenticação.

5. Especifique suas credenciais e faça login em Aplicativo Now Mobile.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A tela inicial do dispositivo móvel é exibida.



Resultados
Na página Registrar dispositivos confiáveis do seu laptop ou desktop, o dispositivo registrado será exibido. Você pode usar o se quiser remover o dispositivo registrado da página.

O que Fazer Depois
Navegue até **Todos** > **Autenticação adaptável** > **Confiança em dispositivos** > **Registro de dispositivos** para visualizar todos os detalhes do dispositivo registrado.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Como gerenciar seu dispositivo confiável

Gerencie seu dispositivo confiável na página de registro de dispositivo confiável.

Antes de Iniciar

Função necessária: nenhuma

Procedimento

1. Navegue até uma das seguintes opções de menu:
   - Em Now Platform, navegue até **Todos** > **Autoatendimento** > **Meu perfil**.

     Nota: Você também pode acessar seu perfil clicando no nome de usuário no cabeçalho da instância.

   - Em Now Support, clique no perfil e selecione **Dispositivo confiável**.
2. Em seu perfil de usuário, clique em **Registrar dispositivo confiável** na seção Links relacionados.
   A página Registrar dispositivos confiáveis será exibida.
3. Na página Registrar dispositivos confiáveis, remova o dispositivo clicando no ícone .

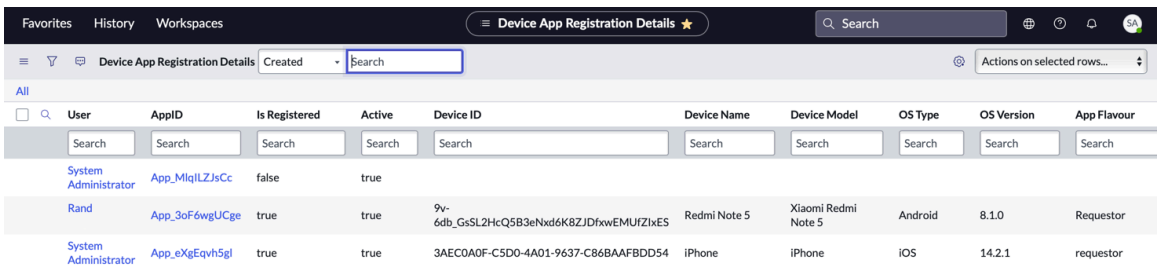
   Nota: O dispositivo móvel excluído deve ser registrado novamente para acessar a instância.

Detalhes do registro dos dispositivos registrados

Exiba os detalhes dos dispositivos registrados em sua instância ServiceNow.

Para visualizar todos os detalhes do dispositivo registrado na sua instância, navegue até **Todos** > **Autenticação adaptável** > **Confiança em dispositivos** > **Registro de dispositivos**.

Use o filtro para identificar o dispositivo. Clique no campo **AppID** para saber mais sobre o dispositivo registrado.

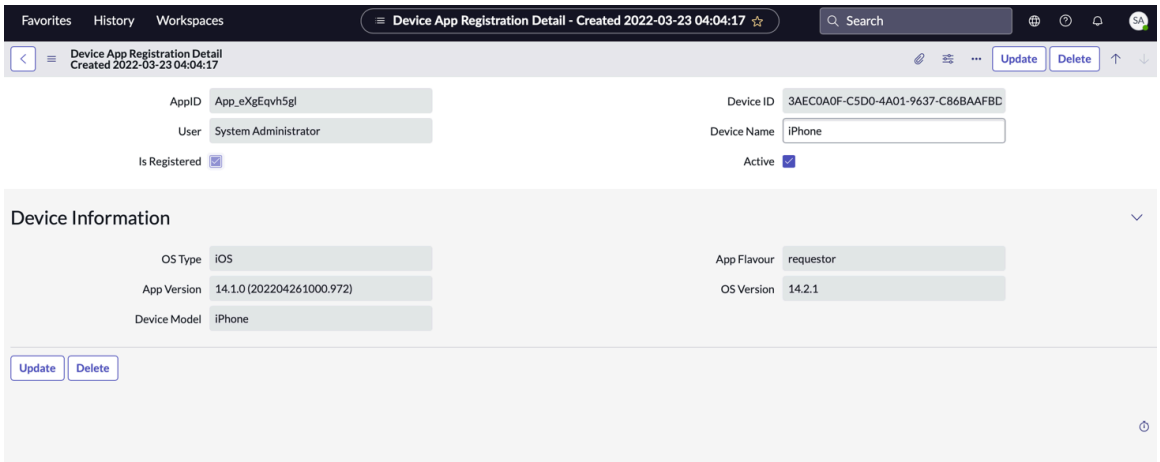


Os seguintes detalhes são exibidos para o dispositivo:

- AppID
- ID do Dispositivo
- Usuário
- Nome do Dispositivo

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Informações do dispositivo, como:
  - Tipo de SO
  - Variante do aplicativo
  - Versão do Aplicativo
  - Versão do SO
  - Modelo do Dispositivo



Solução de problemas do aplicativo para celular Trusted

Analise esses cenários de solução de problemas para resolver questões com o aplicativo Trusted Mobile.

As seções a seguir descrevem alguns cenários de solução de problemas e maneiras de solucionar problemas.

Diferença de tempo entre a instância e o dispositivo móvel (distorção do relógio)

Se houver uma distorção do relógio, você poderá ajustar ou redefinir o relógio do seu dispositivo móvel para usar o Dispositivo confiável.

Expiração do código QR em cinco minutos

O código QR do recurso Dispositivo confiável expira em cinco minutos. Nesse caso, você pode clicar para obter um novo código QR.

Nota: A expiração do código QR pode ser estendida. Para estender sua expiração, entre em contato com o administrador.

A propriedade do sistema foi alterada

Se a propriedade do sistema foi alterada, verifique o registro com base na propriedade do sistema para a credencial válida que pode ser usada para login.

Máximo de dispositivos registrados

Se o número máximo de registros de dispositivo for atingido, remova o dispositivo existente ou entre em contato com o administrador para alterar a contagem máxima de dispositivos.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Autenticação de API

Configurações de autenticação de API.

A autenticação baseada em API em ServiceNow® valida a identidade de um usuário que acessa uma instância e, em seguida, autoriza o usuário a recursos que correspondem à função do usuário ou à função de trabalho ao fazer uma chamada de API para a instância ServiceNow®.

A seguir estão os tipos de autenticação de API em ServiceNow®:

- Autenticação baseada em certificados
- OAuth
- Autenticação baseada em token

Autenticação baseada em certificados

A autenticação baseada em certificados permite autenticar mutuamente solicitações de API de entrada usando certificados de uma autoridade de certificação (CA) confiável.

Autenticação baseada em certificados para serviços Web de entrada

Autentique solicitações de entrada para SOAP e REST APIs de ServiceNow. Para configurar a autenticação mútua para serviços Web de entrada, consulte Como configurar autenticação baseada em certificados.

OAuth

A autenticação baseada em OAuth valida a identidade do cliente que tenta estabelecer uma relação de confiança no sistema usando um protocolo de autenticação.

OAuth 2.0 - Open Authorization é o protocolo padrão do setor para autorização, que se concentra na simplicidade do desenvolvedor do cliente enquanto fornece fluxos de autorização específicos para aplicações da Web, aplicações de desktop e dispositivos móveis.

Entrada

Crie um endpoint para clientes externos que desejam acessar sua instância. Isso cria um registro de aplicação cliente OAuth e gera um ID e segredo do cliente de que o cliente precisa para acessar os recursos restritos na instância. Para mais informações, consulte Entrada de OAuth.

Autenticação baseada em token

Autenticação baseada em token para configuração de REST APIs de entrada usando chave de API ou HMAC.

Ofereça suporte a tokens de API para endpoints de REST API para ServiceNow® para a autenticação de usuário.

A autenticação baseada em token para a configuração de REST APIs de entrada pode ser realizada na instância ServiceNow® com a Chave de API ou o token HMAC.

Chave de API e autenticação de HMAC para REST APIs de entrada

Ofereça suporte a tokens de API para endpoints de REST API para que o nome de usuário e a senha ServiceNow® não fiquem visíveis na URL do webhook.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Habilite a autenticação baseada em chave de API para autenticar a URL do webhook de entrada com segurança.

Para usar a Chave de API e a Autenticação de HMAC, instale (Plug-in: `com.glide.tokenbased_auth`) na instância ServiceNow®.

Aviso: Use a solicitação **POST** ao enviar informações confidenciais para o servidor.

A instalação da Chave de API e da Autenticação HMAC tem dependências nos seguintes plug-ins:

- Plug-in Escopo de autenticação da REST API (`com.glide.rest.auth.scope`)
- Plug-in Política de acesso de REST API (`com.glide.rest.policy`)
- Escopo de autenticação (`com.glide.auth.scope`)

Benefícios

A Chave de API e a Autenticação de HMAC para REST APIs de entrada permitem:

- Especificar a chave de API ou o token HMAC para autenticação de REST API.
- Associar uma conta de usuário à chave de API ou ao token HMAC.
- Capacidade de especificar um token como parâmetro de consulta ou cabeçalho na chamada de REST API.
- Associar o escopo de autenticação às configurações da chave de API ou token HMAC, de modo que as chaves de API só possam ser usadas para invocar APIs associadas a escopos específicos.
- Associar uma configuração de chave de API ou token HMAC a um perfil de autenticação que pode ser usado em políticas de acesso de API.

Ativar chave de API e autenticação de HMAC

Você pode ativar o plug-in Chave de API e autenticação de HMAC (`com.glide.tokenbased_auth`) em sua instância ServiceNow®.

Antes de Iniciar
Função necessária: administrador

Procedimento

1. Navegue até **Todos** > **Aplicações do sistema** > **Todas as aplicações disponíveis** > **Todas**.
2. Encontre o plug-in Chave de API e autenticação de HMAC (`com.glide.auth.mutual`) usando os critérios de filtro e a barra de pesquisa.

   Pesquise o plug-in pelo nome ou ID. Se não conseguir encontrar um plug-in, talvez seja necessário solicitá-lo ao pessoal ServiceNow.
3. Selecione **Instalar** para iniciar o processo de instalação.

   Nota: Quando a separação de domínio e o administrador delegado estão habilitados em uma instância, o usuário administrativo deve estar no domínio **global.** Caso contrário, será exibido o seguinte erro: `A instalação da aplicação não está disponível porque há outra operação em execução: ativação de plug-in para <plugin name>.`

   Você verá uma mensagem após a conclusão da instalação.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configurar chave de API - Autenticação baseada em token

Configure uma chave de API para oferecer suporte à autenticação de endpoints de REST API.

Antes de Iniciar

Função necessária: administrador

Plug-in necessário: chave de API e autenticação HMAC (`com.glide.tokenbased_auth`)

Procedimento

1. Crie um perfil de autenticação de entrada.

   a. Navegue até **Todos** > **Serviços Web do sistema** > **Políticas de acesso de API** > **Perfis de autenticação de entrada**.

   b. Selecione **Novo**.
   O sistema exibe a mensagem `Que tipo de perfil de autenticação?`

   c. Selecione **Criar perfis de autenticação da chave de API**.

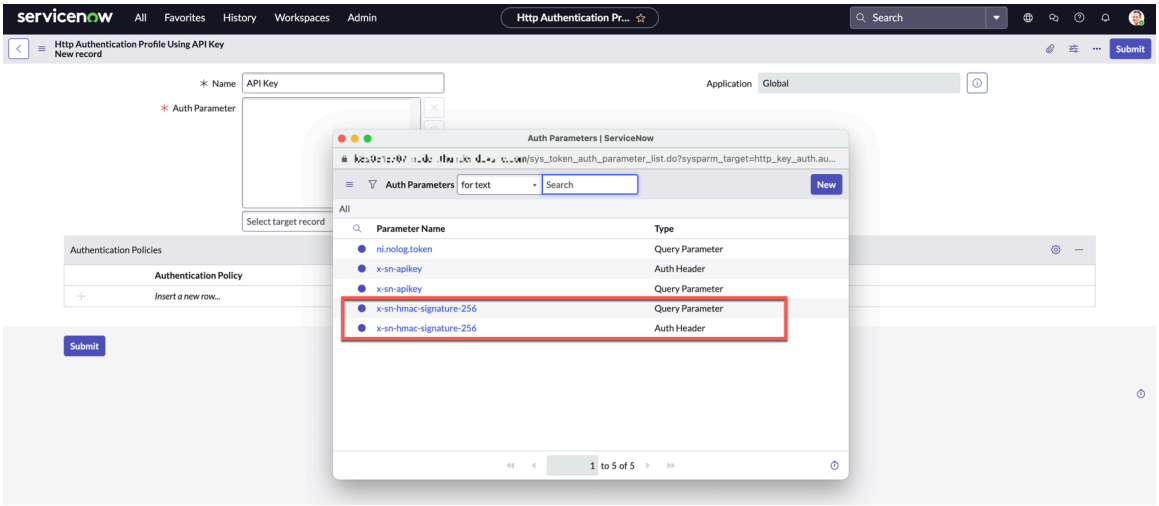
   d. No formulário, preencha os campos.

Perfis de autenticação da chave de API

Campo	Descrição
Nome	Nome para identificar a política de autenticação.
Aplicação	Escopo da política de autenticação.
Parâmetro de autenticação	Selecione o parâmetro de autenticação para a solicitação de autenticação. Você pode selecionar as opções padrão ou criar um novo parâmetro de autenticação: ▪ x-sn-apikey: cabeçalho de autenticação ▪ x-sn-apikey: cabeçalho do parâmetro de consulta

Nota: A opção selecionada deve ser definida na chamada REST como parte do cabeçalho de autenticação ou do parâmetro de consulta.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



e. Envie o formulário.

2. Crie uma chave de REST API.

a. Navegue até **Todos** > **Serviços Web do sistema** > **Políticas de acesso de API** > **Chave de REST API**.

b. Selecione **Novo**.

c. No formulário, preencha os campos:

Chave de API

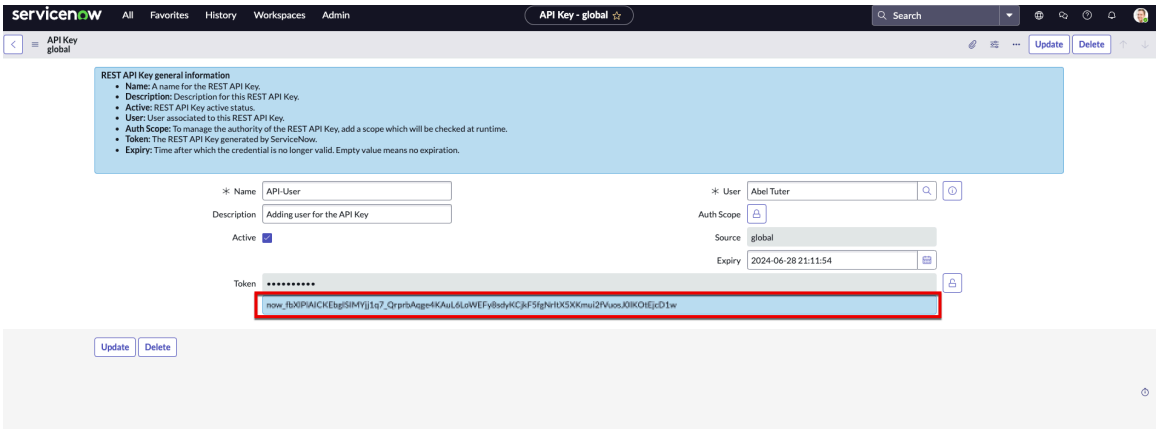
Campo	Descrição
Nome	Nome para identificar a chave de REST API
Descrição	Descrição da chave de REST API.
Ativo	Status da chave de REST API.
Usuário	Usuário associado à chave de REST API. Use o ícone de pesquisa para selecionar o usuário.
Escopo de autenticação	Opção para adicionar escopo de autenticação para gerenciar a autoridade da chave de REST API.
Token	A chave de REST API gerada pela Now Platform. Copie a chave para usar como parte da chamada de REST API no Cabeçalho ou no Parâmetro de consulta.
Vencimento	Prazo após o qual a credencial não é mais válida. Um valor vazio significa que não há vencimento.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: Para obter mais informações sobre a expiração do token, consulte Como limpar o vencimento de tokens.

d. Envie o formulário.

e. Abra o registro que foi criado para exibir o token gerado por Now Platform para o usuário.



3. Crie uma política de acesso de REST API.

a. Navegar até **Todos** > **Serviços Web do sistema** > **Políticas de acesso de REST API**.

b. Selecione **Novo**.

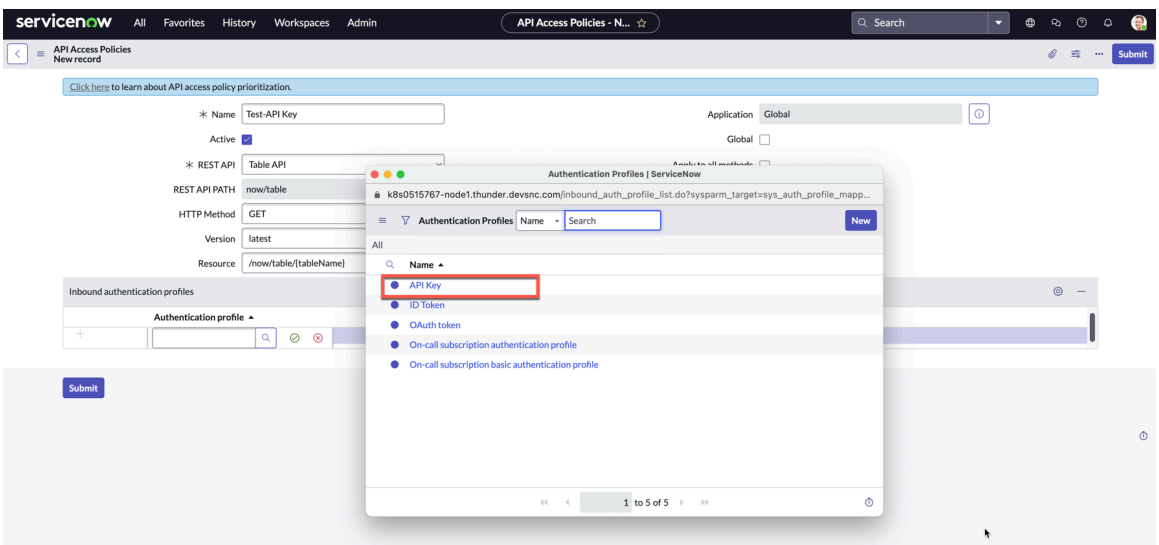
c. No formulário, preencha os campos.

Políticas de acesso de API

Campo	Descrição
Nome	Nome exclusivo da política de acesso de API.
Ativo	Opção para ativar a política de acesso de API.
REST API	A REST API à qual a política de acesso é aplicada. Por exemplo, **API de anexos**.
REST API PATH	Caminho da API da REST API. Esse campo é preenchido automaticamente com base na REST API selecionada. Por exemplo, **now/attachment**.
Método HTTP	Método usado para interagir com a API. Esse campo é preenchido automaticamente com base na REST API selecionada.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Versão	Versão da API. Por exemplo, **v1**. Esse campo é preenchido automaticamente com base na REST API selecionada. **Nota:** Se você quiser criar uma política de autenticação para todas as versões de uma REST API, deverá criar políticas individuais para cada versão.
Recurso	Recurso secundário da REST API. Esse campo é preenchido automaticamente com base na REST API selecionada. Por exemplo, **/now/attachment**.
Aplicação	Escopo da aplicação.
Global	Habilite este campo para aplicar a política de autenticação a todos os métodos, versões e recursos para a API. **Nota:** A autenticação baseada em token não é permitida na política da REST API global.
Aplicar a todos os métodos	Habilite este campo para aplicar a política de autenticação para a API a todos os métodos, versões e recursos para a API.
Aplicar a todos os recursos	Habilite este campo para aplicar a política de autenticação para a API a todas as versões.
Aplicar a todas as versões	Habilite este campo para aplicar a política de autenticação para a API a todos os recursos.



© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

d. Adicione o perfil de autenticação de API que foi criado.

e. Envie o formulário.

Você pode enviar a chamada de REST API com o x-sn-apikey (token) que foi gerado por Now Platform durante a criação da chave de API no cabeçalho ou no parâmetro de consulta com base na configuração para autenticação.

Aviso: Use a solicitação **POST** ao enviar informações confidenciais para o servidor.

Configurar HMAC - Autenticação baseada em token

Configure o HMAC para oferecer suporte à autenticação de endpoints de REST API.

Antes de Iniciar

Função necessária: administrador

Plug-in necessário: chave de API e autenticação HMAC (`com.glide.tokenbased_auth`)

Procedimento

1. Crie uma configuração HMAC.

   a. Navegue até **Todos** > **Serviços Web do sistema** > **Políticas de acesso de APIs** > **Configuração de HMAC**.

   b. Selecione **Novo**.

   Nota: Você também pode usar a **Codificação HMAC SHA256 Base64 padrão** que é criada durante a instalação do plug-in.

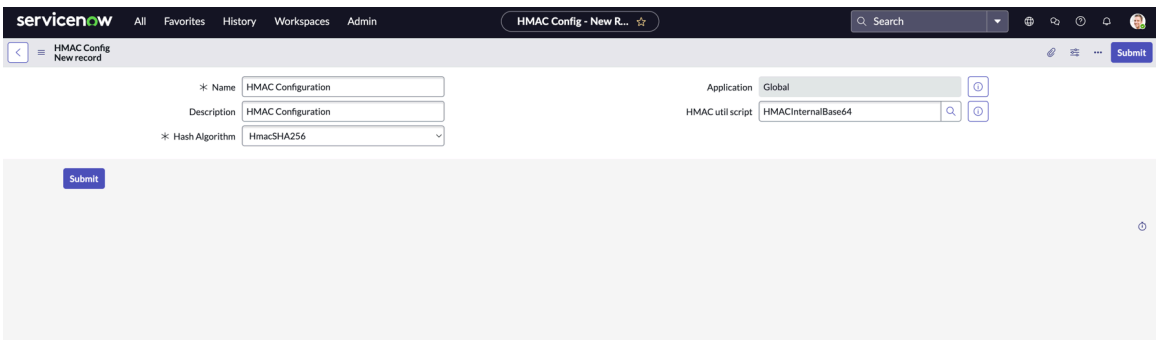
   c. No formulário, preencha os campos:

   Configuração do HMAC

Campo	Descrição
Nome	Nome da configuração do HMAC.
Aplicação	Escopo da configuração.
Descrição	Descrição detalhada da configuração.
Algoritmo de hash	Escolha o Algoritmo de hash. Opções disponíveis: ▪ HmacSHA256 ▪ HmacSHA384 ▪ HmacSHA512
Script do utilitário do HMAC	Script de utilitário para HMAC.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: Se você validar a autenticação HMAC usando o corpo da solicitação, o carimbo de data/hora e o segredo sem ID de chave, faça o seguinte: ▪ Crie uma inclusão de script personalizada como script do utilitário HMAC ▪ Use esse utilitário de inclusão de script para interpretar o carimbo de data/hora da aprovação e o corpo da solicitação. Para cada segredo compartilhado criado na instância da ServiceNow®, há um ID de chave. É necessário configurar o ID da chave como o ID de chave padrão no perfil de autenticação HMAC.



d. Envie o registro.

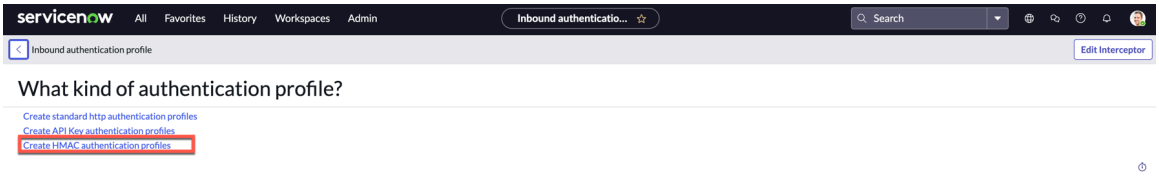
2. Crie um perfil de autenticação de entrada.

a. Navegue até **Todos** > **Serviços Web do sistema** > **Políticas de acesso de API** > **Perfis de autenticação de entrada**.

b. Selecione **Novo**.
O sistema exibe a mensagem `Que tipo de perfil de autenticação?`

c. Selecione **Criar perfis de autenticação de HMAC**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



d. No formulário, preencha os campos.

Perfis de autenticação de HMAC

Campo	Descrição
Nome	Nome para identificar a política de autenticação.
Aplicação	Escopo da política de autenticação.
Configuração do HMAC	Selecione a configuração de HMAC que você criou.
Parâmetro de autenticação	Selecione o parâmetro de autenticação para a solicitação de autenticação. Você pode selecionar as opções padrão ou criar um novo parâmetro de autenticação: ▪ x-sn-hmac-signature-256: cabeçalho de autenticação ▪ x-sn-hmac-signature-256: parâmetro de consulta
ID de chave padrão do segredo compartilhado	As informações de token que podem ser atualizadas neste campo para usar o HMAC.

Nota: A opção selecionada deve ser definida na chamada REST como parte do cabeçalho de autenticação ou do parâmetro de consulta.

e. Envie o formulário.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Crie um segredo do HMAC.

   a. Navegue até **Todos** > **Serviços Web do sistema** > **Políticas de acesso de API** > **Segredo do HMAC da REST API**.

   b. Selecione **Novo**.

   c. No formulário, preencha os campos:

Segredo do HMAC da REST API

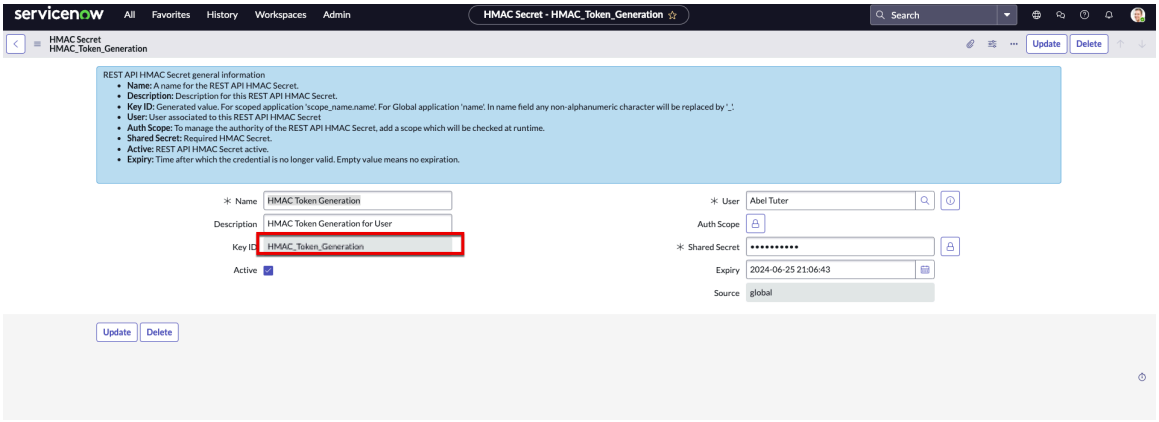
Campo	Descrição
Nome	Nome para identificar o segredo do HMAC da REST API.
Descrição	Descrição do segredo do HMAC da REST API.
Ativo	Status do segredo do HMAC da REST API.
Usuário	Usuário associado ao segredo do HMAC da REST API. Use o ícone de pesquisa para selecionar o usuário.
ID da chave	ID da chave que deve ser enviada como parte da chamada REST. O ID da chave é gerado após o envio do formulário.
Segredo compartilhado	Segredos compartilhados do usuário. Por exemplo, a senha.
Origem	Origem do registro.
Vencimento	Prazo após o qual a credencial não é mais válida. Um valor vazio significa que não há vencimento. **Nota:** Para obter mais informações sobre a expiração do token, consulte Como limpar o vencimento de tokens.

   d. Envie o formulário.

   e. Abra o registro que foi criado.

   Encontre o ID da chave gerado pela Now Platform para o usuário.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Nota: Você pode adicionar o ID da chave que foi gerado durante o ID da chave no perfil de autenticação criado para o HMAC se não quiser especificar o parâmetro de autenticação ou de consulta para a chamada de API.

4. Crie uma política de acesso de REST API.

a. Navegue até **Todos** > **Serviços Web do sistema** > **Políticas de acesso de REST API**.

b. Selecione **Novo**.

c. No formulário, preencha os campos.

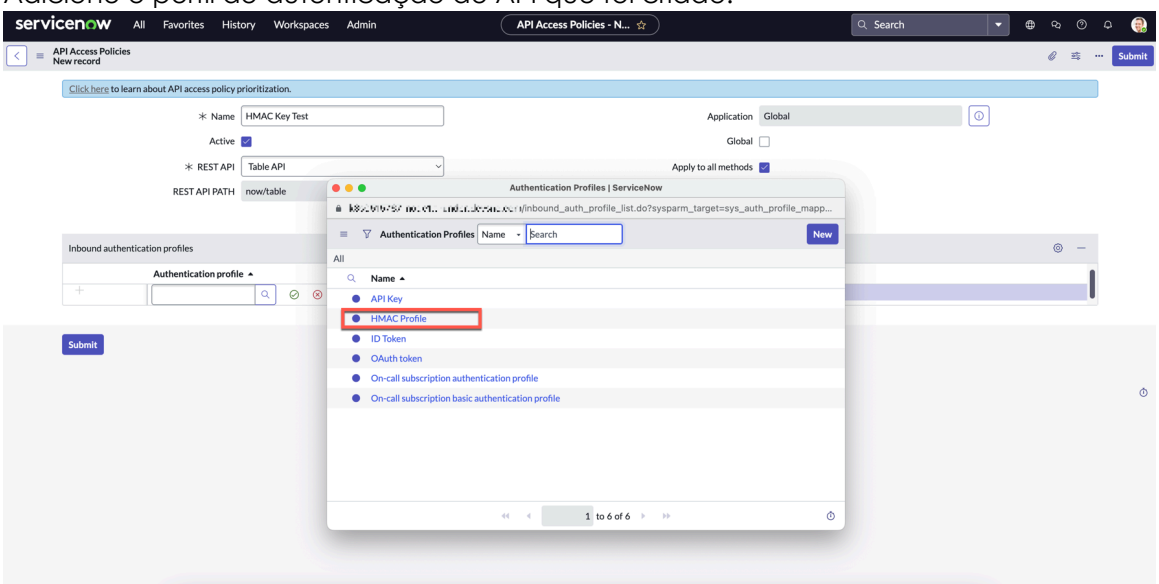
Políticas de acesso de API

Campo	Descrição
Nome	Nome exclusivo da política de acesso de API.
Ativo	Opção para ativar a política de acesso de API.
REST API	A REST API à qual a política de acesso é aplicada. Por exemplo, **API de anexos**.
REST API PATH	Caminho da API da REST API. Esse campo é preenchido automaticamente com base na REST API selecionada. Por exemplo, **now/attachment**.
Método HTTP	Método usado para interagir com a API. Esse campo é preenchido automaticamente com base na REST API selecionada.
Versão	Versão da API. Por exemplo, **v1**. Esse campo é preenchido automaticamente com base na REST API selecionada.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: Se você quiser criar uma política de autenticação para todas as versões de uma REST API, deverá criar políticas individuais para cada versão.
Recurso	Recurso secundário da REST API. Esse campo é preenchido automaticamente com base na REST API selecionada. Por exemplo, **/now/attachment**.
Aplicação	Escopo da aplicação.
Global	Habilite este campo para aplicar a política de autenticação a todos os métodos, versões e recursos para a API. **Nota:** A autenticação baseada em token não é permitida na política da REST API global.
Aplicar a todos os métodos	Habilite este campo para aplicar a política de autenticação para a API a todos os métodos, versões e recursos para a API.
Aplicar a todos os recursos	Habilite este campo para aplicar a política de autenticação para a API a todas as versões.
Aplicar a todas as versões	Habilite este campo para aplicar a política de autenticação para a API a todos os recursos.

d. Adicione o perfil de autenticação de API que foi criado.



e. Envie o formulário.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você pode enviar a chamada de REST API:

- Com a x-sn-hmac-signature-256 gerada por ServiceNow® durante a criação da chave de API no cabeçalho ou no parâmetro de consulta com base na configuração para autenticação.
- Com o Script de pré-solicitação, junto ao Segredo compartilhado especificado como parte da solicitação.

Aviso: Use a solicitação **POST** ao enviar informações confidenciais para o servidor.

Como limpar o vencimento de tokens

Detalhes sobre como limpar o vencimento de tokens usando diferentes propriedades do sistema.

Depois que a chave de API ou o segredo do HMAC expiram, a retenção dos detalhes ocorre durante sete dias. Depois desse período, um trabalho agendado `Limpar credenciais vencidas de autenticação de token` exclui as chaves de API ou os segredos do HMAC vencidos. É possível configurar esse comportamento e controlar a exclusão usando as seguintes propriedades:

- **com.snc.platform.security.token.auth.cleanup**: use essa propriedade se quiser excluir chaves de API e tokens HMAC vencidos. Por padrão, `verdadeiro`.
- **com.snc.platfrom.security.token.auth.days.expired.api_key.is.kept**: defina o valor com base em seus requisitos para determinar o número de dias pelos quais você deseja manter o token de `API` vencido no sistema. Por padrão, 7.
- **com.snc.platfrom.security.token.auth.days.expired.hmac_key.is.kept**: defina o valor com base em seus requisitos para determinar o número de dias pelos quais você deseja manter o token `HMAC` vencido no sistema. Por padrão, 7.

Para navegar até a propriedade de vencimento de tokens, digite `sys.trigger.list` na barra de navegação e pesquise as propriedades abaixo. Mude o vencimento com base em seus requisitos.

Política de acesso de API

A política de acesso de API define as permissões e a duração do acesso a uma API.

A política de acesso de API permite que você restrinja o acesso às ServiceNow® APIs de entrada com base no tipo de autenticação e nos critérios de filtro especificados da política de acesso.

Confira abaixo o suporte à política de autenticação em três níveis para sessões não interativas:

- **REST API**: o administrador pode definir uma política global de autenticação ou uma política de autenticação específica da API.
- **SOAP API**: o administrador pode definir uma política global de autenticação ou uma política de autenticação específica da API.
- **Processador de exportação/sistema**: o administrador pode definir cinco perfis de autenticação baseados no sistema, que podem ser usados para aplicar o perfil de autenticação à política de autenticação da API dos processadores ou à política de autenticação específica do processador.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Se você adicionar uma política global de autenticação, ela será aplicada a todas as REST APIs, SOAP APIs ou processadores de exportação/sistema.

Confira os plug-ins instalados automaticamente para políticas de API e escopo de autenticação:

- com.glide.rest.policy
- com.glide.soap.policy
- com.glide.processor.policy
- com.glide.rest.auth.scope

Você pode configurar a Política de bloqueio global padrão ou criar uma política de acesso de API personalizada de acordo com seus requisitos de segurança. É possível aplicar critérios de filtro que contenham condições ou consultas do filtro usadas como entradas para uma política de autenticação.

As políticas de acesso de API a seguir são compatíveis com ServiceNow®:

- Políticas de acesso de REST API
- Políticas de acesso de SOAP API

Para obter informações sobre as políticas relacionadas aos processadores de exportação, consulte Política de acesso para Processadores de sistema/exportação.

Políticas de acesso de REST API

As políticas de acesso de REST API permitem que você restrinja o acesso aos REST APIs de entrada com base no tipo de autenticação e nos critérios de filtro especificados da política de acesso.

Uma REST API, também conhecida como RESTful API, é um tipo de interface de programação de aplicação (API) que adere às diretrizes do estilo de arquitetura REST. As REST APIs fornecem um alto grau de flexibilidade, tornando-as prevalentes em toda a Web.

Os critérios de filtro contém condições ou consultas do filtro que são usadas como entradas de política para uma política de autenticação.

Você pode configurar a Política de bloqueio global padrão ou criar uma política de acesso de API personalizada de acordo com seus requisitos de segurança. Por exemplo, você pode criar uma política de acesso de API personalizada que permite somente o tipo de autenticação OAuth 2.0 de um intervalo especificado de endereços IP. Solicitações de autenticação de outros tipos de autenticação e solicitações de acesso de endereços IP diferentes dos endereços IP especificados são negadas.

Como ativar a política de acesso de REST API

Você pode ativar o plug-in REST API Access Policy (com.glide.rest.policy) se tiver a função de administrador. A aplicação inclui dados de demonstração e instala aplicações e plug-ins relacionados ServiceNow® Store se eles ainda não estiverem instalados.

Antes de Iniciar

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

Os itens a seguir são instalados com a Política de acesso de REST API:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Plug-ins: com.glide.auth.profile, com.snc.adaptive_authentication, com.snc.platform.security.oauth
- Tabelas: sys_api_access_policy, sys_auth_profile_mapping, auth_policy_mapping, inbound_auth_profile, std_http_auth.

Para obter mais informações, consulte Autenticação adaptável.

Procedimento

1. Navegue até **Todos** > **Aplicações do sistema** > **Todas as aplicações disponíveis** > **Todas**.
2. Encontre o plug-in REST API Access Policy plugin (com.glide.rest.policy) usando os critérios de filtro e a barra de pesquisa.

   Pesquise o plug-in pelo nome ou ID. Se não conseguir encontrar um plug-in, talvez seja necessário solicitá-lo ao pessoal ServiceNow.

3. Selecione **Instalar** para iniciar o processo de instalação.

   Nota: Quando a separação de domínio e o administrador delegado estão habilitados em uma instância, o usuário administrativo deve estar no domínio **global**. Caso contrário, será exibido o seguinte erro: `A instalação da aplicação não está disponível porque há outra operação em execução: ativação de plug-in para <plugin name>.`

   Você verá uma mensagem após a conclusão da instalação.

Como criar um perfil de autenticação

Crie um perfil de autenticação e adicione uma ou mais políticas de autenticação ao perfil. Você também pode configurar os perfis de autenticação **Token de ID** e **Token OAuth** que estão disponíveis por padrão.

Antes de Iniciar

Função necessária: administrador

Nota: Você pode aplicar políticas de autenticação, intervalo de IPs, com base em função, com base em usuário e muito mais com autenticação mútua e autenticação personalizada.

Procedimento

1. Navegue até **Todos** > **Serviços Web do sistema** > **Políticas de acesso de API** > **Perfis de autenticação de entrada**.
2. Selecione **"Novo"**.
   O sistema exibe a mensagem. `Que tipo de perfil de autenticação?`
3. Selecione **Criar perfis de autenticação HTTP padrão**.
4. No formulário, preencha os seguintes campos.

Formulário de perfil de autenticação padrão

Campo	Descrição
Nome	Nome para identificar a política de autenticação.
Descrição	Descrição da política de autenticação.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Ativo	Opção para ativar a política de autenticação.
Aplicação	Escopo da política de autenticação.
Tipo	Tipo de autenticação disponível. Você pode selecionar **Autenticação básica**, **Token de ID**, **Autenticação baseada em certificados** ou **OAuth**.
Entidade OAuth	Perfil de entidade OAuth. Esse campo aparece somente quando **Token de ID** ou **OAuth** é selecionado em **Tipo**.

5. Clique duas vezes em **Inserir uma nova linha**.
6. Selecione uma política de autenticação na lista e selecione o ícone de salvar .

Nota: Não selecione "Política de permissão de acesso" ou "Política de negação de acesso". Essas políticas são destinadas somente a logins dos usuários.

Você pode adicionar uma ou mais políticas de autenticação a um perfil de autenticação.

Nota:

Cabeçalho de autenticação [WWW-Authenticate].

Quando a Política de acesso de REST API estiver ativa, o cabeçalho de autenticação exibirá o perfil de autenticação mapeado mais recentemente. Caso você queira que o servidor exiba todos os esquemas de autenticação, use a propriedade `glide.security.response.authenticate.header.auth_profile.first_scheme_only` e a defina como **falsa**. A resposta é retornada com vários cabeçalhos. Por exemplo:

```
< WWW-Authenticate: BEARER realm="Service-now"
< WWW-Authenticate: BASIC realm="Service-now"
```

Como criar a política de acesso de REST API

Crie uma política de acesso de API e mapeie um perfil de autenticação para restringir o tipo de autenticação de uma REST API. Por exemplo, você pode criar uma política de acesso de API que permita somente a autenticação de token de ID para uma REST API.

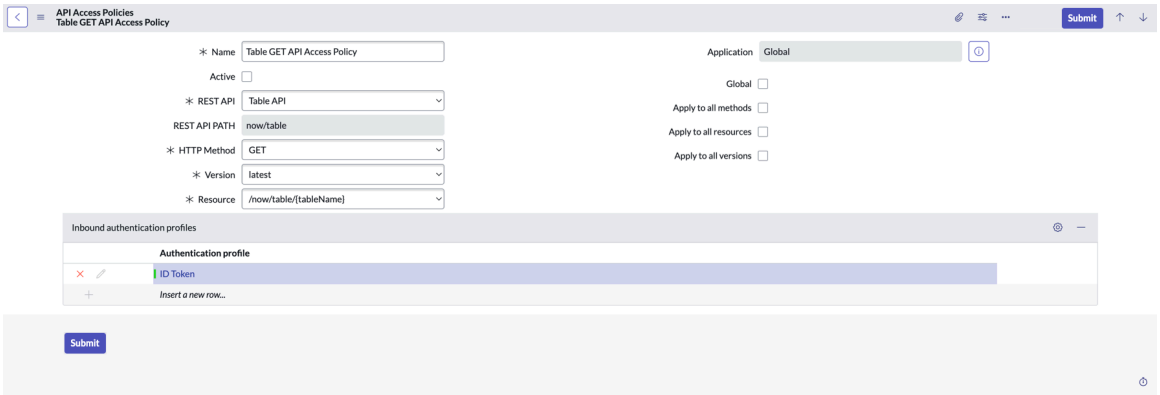
Antes de Iniciar

- Função necessária: administrador
- Certifique-se de criar um perfil de autenticação. Para obter mais informações, consulte Como criar um perfil de autenticação.

Procedimento

1. Navegar até **Todos** > **Serviços Web do sistema** > **Políticas de acesso de REST API**.
2. Clique em **Nova**.
3. No formulário, preencha os seguintes campos.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Políticas de acesso de API

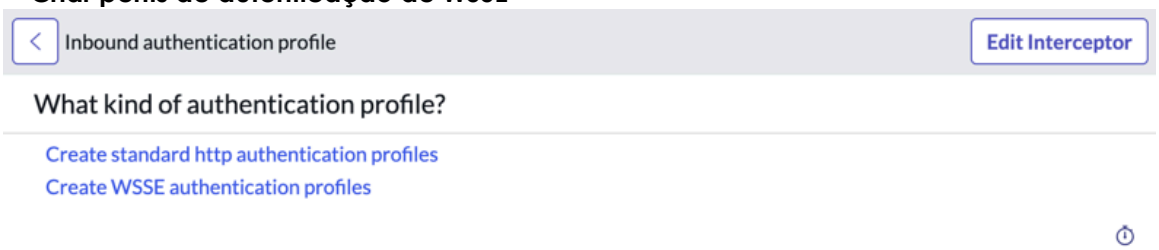
Campo	Descrição
Nome	Nome exclusivo da política de acesso de API.
Ativo	Opção para ativar a política de acesso de API.
REST API	A REST API à qual a política de acesso é aplicada. Por exemplo, **API de anexos**.
REST API PATH	Caminho da API da REST API. Esse campo é preenchido automaticamente com base na REST API selecionada. Por exemplo, **now/attachment**.
Método HTTP	Método usado para interagir com a API. Esse campo é preenchido automaticamente com base na REST API selecionada.
Versão	Versão da API. Por exemplo, **v1**. Esse campo é preenchido automaticamente com base na REST API selecionada. **Nota:** Se você quiser criar uma política de autenticação para todas as versões de uma REST API, deverá criar políticas individuais para cada versão.
Recurso	Recurso secundário da REST API. Esse campo é preenchido automaticamente com base na REST API selecionada. Por exemplo, **/now/attachment**.
Aplicação	Escopo da aplicação.
Global	Habilita a aplicação da política de autenticação a todos os métodos, versões e recursos para a API.
Aplicar a todos os métodos	Habilita a aplicação da política de autenticação para a API a todos os métodos, versões e recursos para a API.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Aplicar a todos os recursos	Habilita a aplicação da política de autenticação para a API a todas as versões.
Aplicar a todas as versões	Habilita a aplicação da política de autenticação para a API a todos os recursos.

Nota: Para entender mais sobre a priorização da política de acesso de API, consulte Priorização da política de acesso de API.

4. Clique duas vezes em **Inserir uma nova linha**.
5. Selecione um perfil de autenticação de entrada na lista e clique no ícone de salvar . Por exemplo, você pode adicionar **Autenticação básica**, **Token de ID**, **Autenticação baseada em certificados**, **OAuth** ou **Autenticação de WSSE**.
   a. Para adicionar um ou mais perfis de autenticação de entrada, clique em **Novo** para criar um novo perfil.
   b. Selecione **Que tipo de perfis de autenticação?**.
      - **Criar perfis de autenticação HTTP padrão**
      - **Criar perfis de autenticação de WSSE**



   c. Depois de criar o perfil de autenticação, salve o registro.
6. Clique em **Enviar** para enviar a política de acesso de REST API.

Priorização da política de acesso de API

Saiba mais sobre a lógica de priorização de política se houver várias políticas de acesso de API configuradas para sua instância ServiceNow®.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

As políticas de acesso de API são priorizadas com base no tipo de política de REST API definida na sua instância ServiceNow®.

A abordagem é definir pesos diferentes para cada parte da API, como método, recurso e versão.

A política de API é priorizada primeiramente para não global e, em seguida, global. Em outras palavras, uma política de acesso não global sempre substituirá uma política de acesso de API global.

A lógica de priorização é a seguinte:

Priorização

Campos	Prioridade	Lógica da priorização
Método, recurso e versão	1	Se os 3 campos corresponderem à política, então essa política terá a primeira prioridade.
Método + recurso	2	Se os 2 campos corresponderem à política, então essa política terá a primeira prioridade.
Recurso + versão	3	Se os 2 campos juntamente com o campo **Aplicar a todos os métodos** corresponderem à política, então essa política terá a terceira prioridade.
Recurso	4	Se o campo juntamente com o campo **Aplicar a todos os métodos** corresponderem à política, então essa política terá a quarta prioridade.
Método + versão	5	Se os 2 campos juntamente com o campo **Aplicar a todos os recursos** corresponderem à política, então essa política terá a quinta prioridade.
Método	6	Se o campo juntamente com o campo **Aplicar a todos os recursos** corresponderem à política, então essa política terá a quinta prioridade.
Versão	7	Se o campo juntamente com os campos **Aplicar a todos os métodos** e **Aplicar a todas as versões** corresponderem à política,

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Priorização

Campos	Prioridade	Lógica da priorização
		então essa política terá a sétima prioridade.
Global e Aplicar a todos os métodos	8	Se o campo **Global** for `verdadeiro` e o campo **Aplicar a todos os métodos** for `falso`, essa política terá a oitava prioridade.
Global e Aplicar a todos os métodos	9	Se o campo **Global** for `verdadeiro` e o campo **Aplicar a todos os métodos** for `verdadeiro`, essa política terá a nona prioridade.

Escopo de autenticação da REST API

Suporte ao escopo de autenticação para REST API.

Antes da versão Xanadu, cada token de acesso ou token OIDC era vinculado ao escopo da conta do usuário que tinha acesso total às REST APIs do usuário. Na versão Xanadu, para fornecer acesso somente às REST APIs específicas, foram introduzidos os escopos de token OAuth.

Quando uma entidade OAuth é vinculada a um escopo de autenticação, o token é emitido ou gerenciado por essa entidade OAuth e só pode ser usado para acessar as REST APIs (uma mesma entidade OAuth pode ser vinculada a vários escopos de autenticação). Para a nova entidade OAuth, o escopo de autenticação padrão está vazio. Você deve vincular manualmente o escopo de autenticação com a entidade OAuth.

Nota:

- Depois que o escopo de autenticação da REST API for habilitado e adicionado ao escopo de autenticação para a REST API, todos os tokens OAuth existentes não poderão mais acessar esta API, a menos que o administrador adicione esse escopo de autenticação à entidade OAuth correspondente.
- O administrador é responsável por garantir que a "oauth_entity" tenha o escopo de autenticação correto após vincular o escopo de autenticação à REST API.
- Os tokens de acesso OAuth emitidos pela ServiceNow são compatíveis com o escopo de autenticação.
- O token OIDC que não é emitido pela ServiceNow é validado pela ServiceNow.
- O token OIDC tem o escopo do IDP quando você precisa de um token de ID. Aqui, o escopo de autenticação é para ServiceNow em vez de terceiros (IdP).

Configurações do escopo da REST API

Para configurar o escopo da REST API, execute as seguintes tarefas:

- Crie um escopo de autenticação
- Vincule o escopo de autenticação com a REST API
- Vincule o escopo de autenticação à entidade OAuth

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Execute o fluxo OAuth para obter o token de acesso OAuth
- Use o token de acesso OAuth para fazer a chamada da API

Como ativar o plug-in "REST API Auth Scope"

Você pode ativar o plug-in "REST API Auth Scope" (com.glide.rest.auth.scope) para vincular a entidade OAuth aos escopos de autenticação.

Antes de Iniciar
Instale os seguintes plug-ins:

- OAuth 2.0
- REST API Provider
- Escopo de autenticação
- REST API Scope

Nota: O plug-in *REST API Scope* é adicionado como parte da versão Tokyo.

Função necessária: administrador

Procedimento

1. Navegue até **Todos** > **Aplicações do sistema** > **Todas as aplicações disponíveis** > **Todas**.
2. Encontre o plug-in "REST API auth Scope" (*com.glide.rest.auth.scope*) usando os critérios de filtro e a barra de pesquisa.

   Pesquise o plug-in pelo nome ou ID. Se não conseguir encontrar um plug-in, talvez seja necessário solicitá-lo ao pessoal ServiceNow.

3. Selecione **Instalar** para iniciar o processo de instalação.

   Nota: Quando a separação de domínio e o administrador delegado estão habilitados em uma instância, o usuário administrativo deve estar no domínio **global**. Caso contrário, será exibido o seguinte erro: `A instalação da aplicação não está disponível porque há outra operação em execução: ativação de plug-in para <plugin name>.`

   Você verá uma mensagem após a conclusão da instalação.

Propriedades e tabelas do escopo de autenticação da REST API

O plug-in "REST API Auth Scope" (com.glide.rest.auth.scope) inclui as seguintes propriedades do sistema, tabelas e scripts.

Propriedades do escopo de autenticação da REST API

O escopo de autenticação da REST API adiciona as seguintes propriedades do sistema.

Propriedades

Nome	Descrição
com.glide.rest.api.auth.scope.check.enable	Esta propriedade é usada para desativar a verificação do escopo de autenticação no nível de plataforma.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Propriedades

Nome	Descrição
	Se estiver definida como falsa, a verificação do escopo de autenticação será ignorada durante o tempo de execução, independentemente de estar vinculada ou não à REST API. Por padrão, esta propriedade é definida como verdadeira. Ela é usada quando você deseja reverter para o comportamento da versão anterior.
com.glide.oauth.token.scope.useraccount	Essa propriedade é usada somente quando o escopo de autenticação *useraccount* é excluído e adicionado de volta manualmente pelo usuário final. Nesse caso, o ID do sistema para *useraccount* é alterado. É necessário atualizar essa propriedade para o novo "sys_id". Durante o tempo de execução, o ID do sistema do escopo de autenticação é usado em vez do nome do escopo de autenticação.

Tabelas do escopo de autenticação da REST API

O escopo de autenticação da REST API tem as seguintes tabelas.

Tabelas

Nome	Descrição
Escopo de autenticação (sys_auth_scope)	Essa tabela define o escopo de autenticação que pode ser vinculado à REST API e à entidade OAuth. O nome do escopo de autenticação deve ser exclusivo e global.
Escopo de autenticação da REST API (sys_api_access_scope)	Essa tabela vincula a REST API ao escopo de autenticação.

Como configurar o escopo de autenticação da REST API

Vincule a entidade OAuth a um escopo de autenticação para gerenciar o token para acessar as REST APIs que estão vinculadas ao escopo de autenticação.

Antes de Iniciar

Instale os seguintes plug-ins:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- OAuth 2.0
- REST API Provider
- Escopo de autenticação
- REST API Auth Scope

Nota: O plug-in *REST API Auth Scope* é adicionado como parte da versão Tokyo.

Função necessária: administrador

Procedimento

1. Navegue até **Todos** > **Escopos de autenticação de API** > **Escopo de autenticação da REST API**.
   A página Escopos de autenticação da REST API é exibida.
2. Para configurar um novo Escopo de autenticação da REST API, clique em **Novo**.
3. No formulário, preencha os campos.

Escopo de autenticação da REST API

Nome	Um nome exclusivo que identifica o Escopo de autenticação da REST API.
Ativo	Marque a caixa de seleção para ativar a configuração.
Aplicação	Escopo da aplicação de somente leitura.
REST API	A REST API à qual o escopo de autenticação é aplicado. Por exemplo, a API da tabela.
Escopo de autenticação	Selecione o escopo de autenticação no ícone de pesquisa.
REST API PATH	Caminho da API da REST API. Esse campo é preenchido automaticamente com base na REST API selecionada. Por exemplo, "now/table".
Método HTTP	Método usado para interagir com a API. Selecione o método na lista suspensa. Você pode desabilitar manualmente o campo **Aplicar escopo de autenticação a todos os métodos HTTP nesta API** no formulário para selecionar o método.
Versão da REST API	Versão da API. Por exemplo, v1. Esse campo é preenchido automaticamente com base na REST API selecionada. Você pode desabilitar manualmente o campo **Aplicar escopo de autenticação a todas as versões nesta API** no formulário para selecionar a versão.

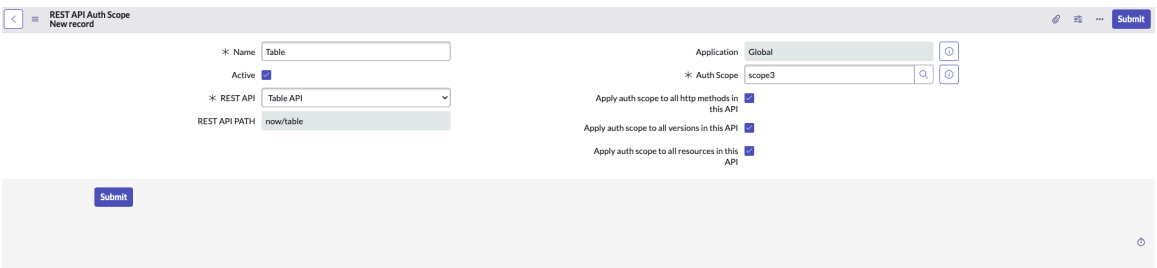
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Recurso	Recurso secundário da REST API. Esse campo é preenchido automaticamente com base na REST API selecionada. Por exemplo, "/now/table". Você pode desabilitar manualmente o campo **Aplicar escopo de autenticação a todos os recursos nesta API** no formulário para selecionar os recursos.
Aplicar escopo de autenticação a todos os métodos HTTP nesta API	Quando habilitado, aplica o escopo de autenticação a todos os métodos HTTP na API.
Aplicar escopo de autenticação a todas as versões nesta API	Quando habilitado, aplica o escopo de autenticação a todas as versões na API.
Aplicar escopo de autenticação a todos os recursos nesta API	Quando habilitado, aplica o escopo de autenticação a todos os recursos na API.

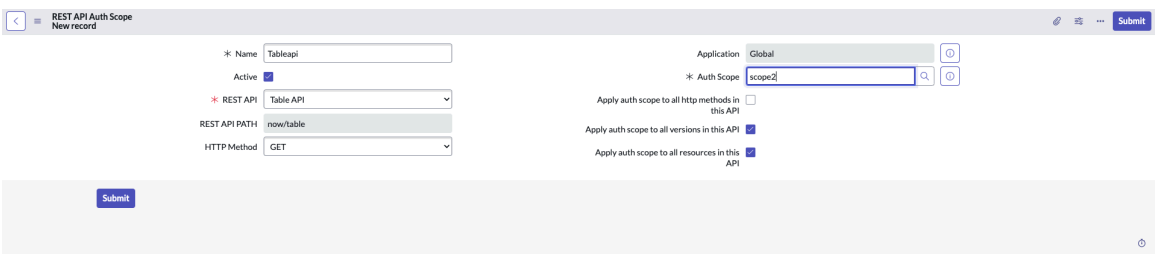
4. Clique em **Enviar**.
   Com base na REST API e no escopo de autenticação selecionados, as APIs recuperam informações específicas do escopo.

Example: Considere criar três escopos de autenticação da REST API para a API da tabela

O primeiro escopo de autenticação é mapeado para a **API da tabela** com todos os métodos HTTP, versões e recursos habilitados.

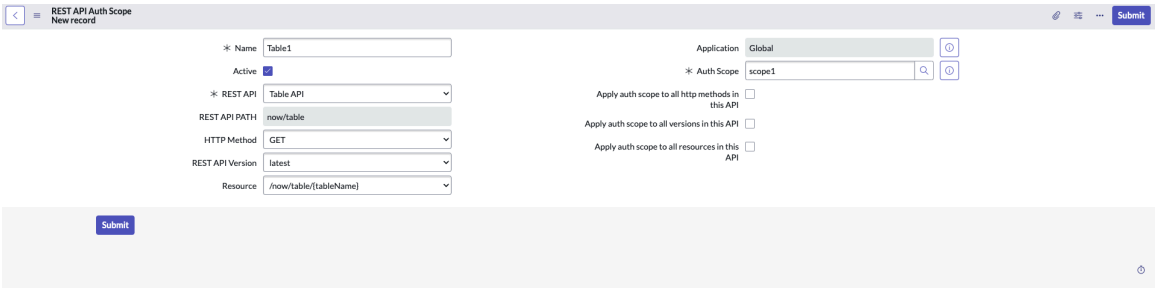


O segundo escopo de autenticação é mapeado para a **API da tabela** com todas as versões e recursos habilitados. Mas, neste exemplo, escolhe-se o método **GET** no método HTTP.



O terceiro escopo de autenticação é mapeado para a **API da tabela** sem os métodos HTTP, versões e recursos habilitados. Você escolherá manualmente o método HTTP, a versão e o recurso. Neste exemplo, o método HTTP é **GET**, a versão da REST API é a **mais recente** e o recurso é `/now/table/{tableName}`.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Se todos esses escopos de autenticação forem criados, você poderá usar o método **GET** com todos os três escopos, mas para os métodos **POST**, **PUT**, **DELETE**ou **PATCH**, somente o **escopo 3** poderá ser usado.

Solução de problemas do escopo da REST API

Ações de solução de problemas podem ajudar a resolver problemas comuns durante a configuração ou execução do escopo da REST API.

Solução de problemas

Problema	Ação
A REST API está vinculada ao escopo de autenticação. No entanto, no tempo de execução, não há verificação de escopo de autenticação mesmo usando a autenticação de token do portador.	• Certifique-se de que o registro "sys_api_access_policy" esteja ativo. O tempo de execução ignora registros inativos. • Verifique se a propriedade *com.glide.rest.api.auth.scope.check.enable* está definida como falsa. • Verifique se o token OAuth tem escopo de autenticação `useraccount`.
A REST API está vinculada a *auth_scope1*, mas o token de acesso que tem *auth_scope2* também pode acessá-la.	• Verifique se este registro está ativo. • Verifique este REST e se há outros registros que tenham as mesmas APIs, mas métodos, versões ou recursos diferentes.
A REST API está vinculada ao escopo de autenticação. No entanto, no tempo de execução, não há verificação de escopo de autenticação para *basicAuth* e *mutualAuth*.	Isso é esperado, já que o escopo de autenticação da REST API se aplica somente ao token de acesso OAuth ou ao token OIDC. Ele não se aplica à BasicAuth, cookie de sessão e autenticação baseada em certificados.
A chamada de REST API retorna 403 ao usar o token de acesso OAuth.	Verifique a mensagem de erro "Escopo de acesso de API necessário ausente". Se encontrado, a verificação do escopo de autenticação falha para esta REST API
A `useraccount` predefinida foi excluída e não há certeza de que será restaurada.	Exporte `useraccount` como `xml` da outra instância e importe-a ou crie uma `useraccount` e modifique a propriedade do sistema

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Solução de problemas

Problema	Ação
	glide.oauth.token.scope.useraccount para o registro "sys_id" recém-criado.

Perguntas frequentes

A seguir estão algumas das perguntas frequentes ao usar o escopo de autenticação da REST API:

Um mesmo token OAuth pode ser vinculado a vários escopos de autenticação?

Sim, uma mesma `oauth_entity` pode ser vinculada a vários escopos de autenticação. Cada token OAuth emitido por essa `oauth_entity` tem os mesmos escopos de autenticação.

Tokens OAuth diferentes com escopos de autenticação diferentes podem acessar a mesma REST API?

Sim, a mesma REST API pode ser acessada por diferentes escopos de autenticação. Desde que um escopo de autenticação seja correspondido, o escopo de autenticação retornará os resultados.

O token de acesso OAuth com escopo de autenticação `useraccount` pode acessar REST APIs?

Sim, `useraccount` tem acesso total ao escopo de autenticação.

O escopo de OAuth do token de acesso OAuth pode ser alterado dinamicamente?

Sim, o escopo de autenticação não está codificado com o token de acesso na tabela `oauth_credential`. Em vez disso, durante o tempo de execução o escopo de autenticação é obtido da `oauth_entity` vinculada.

O token OAuth pode manter os mesmos escopos de autenticação após a atualização?

Sim, o escopo de autenticação não mudará após a atualização do token, a menos que o `oauth_admin` modifique o escopo de autenticação vinculado a `oauth_entity`.

O registro de escopo de autenticação `useraccount` predefinido foi excluído. Um novo escopo de autenticação com o nome `useraccount` pode ser criado?

Não é possível criar um novo escopo de autenticação com a mesma `useraccount`. No tempo de execução, ele usa o `sys_id` em vez do nome para fazer a verificação do escopo de autenticação. Modifique a propriedade do sistema *glide.oauth.token.scope.useraccount* para o registro `sys_id` recém-criado.

Se o administrador modificar o escopo de autenticação vinculado a `oauth_entity`, todos os tokens de acesso OAuth existentes emitidos por esta entidade OAuth também serão alterados?

Sim, o escopo de autenticação não está diretamente vinculado ao token de acesso OAuth. Ele é obtido da `oauth_entity` durante o tempo de execução.

Diferentes tokens de acesso OAuth emitidos pela mesma `oauth_entity` podem ter diferentes escopos de autenticação?

Não, todos os acessos ao token são emitidos pela mesma `oauth_entity` e sempre têm os mesmos escopos de autenticação.

Um usuário pode definir diferentes escopos de autenticação para um endpoint específico?

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Não, há uma verificação de restrição exclusiva para um endpoint de REST API específico. No entanto, para o mesmo endpoint de REST API, ele pode ter mais de um escopo de autenticação correspondente.

A verificação de escopo de autenticação também é usada para BasicAuth?

Não, a verificação do escopo de autenticação é apenas para token de acesso OAuth e token OIDC, não é aplicado para *basicAuth* e *mutualAuth*

Políticas de acesso de SOAP API

As políticas de acesso de SOAP API permitem que você restrinja o acesso aos SOAP APIs de entrada com base no tipo de autenticação e nos critérios de filtro especificados da política de acesso.

As políticas de acesso de SOAP API permitem que você aplique o perfil de autenticação de entrada e as políticas de acesso de API ao SOAP de entrada e às SOAP APIs de script.

Você pode aproveitar políticas de acesso de API ServiceNow, como intervalo de IPs e restrições baseadas em função, para permitir ou proibir chamadas de SOAP API de entrada com base na autenticação.

Como administrador, você pode executar as seguintes ações para aplicar as políticas.

- Ative os plug-ins SOAP API Access Policy e Authentication Profile. Para obter mais informações, consulte Como ativar a política de acesso de SOAP API.
- Crie políticas de acesso de SOAP API e associe essas políticas a um perfil de autenticação. Para obter mais informações, consulte Como criar a política de acesso de SOAP API e Como criar um perfil de autenticação.

  Nota: As políticas são aplicáveis à API da tabela SOAP ou à SOAP API de script, além do `HTTP` padrão e do perfil de autenticação `WSSE`.

- Crie políticas de autenticação, como intervalo de IPs, restrições baseadas em função e associe essa política ao perfil de autenticação. Para obter mais informações, consulte Como criar uma política de autenticação de API.

Como ativar a política de acesso de SOAP API

Para a política de acesso de SOAP API, instale o plug-in SOAP API Access Policy (`com.glide.soap.policy`).

Antes de Iniciar

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

O item a seguir é instalado com o plug-in SOAP API Access Policy: Política de acesso ao processador (`com.glide.processor.policy`)

Plug-in dependente: Perfil de autenticação (`com.glide.auth.profile`)

Procedimento

1. Navegue até **Todos** > **Aplicações do sistema** > **Todas as aplicações disponíveis** > **Todas**.
2. Encontre o plug-in SOAP API Access Policy (`com.glide.soap.policy`) usando os critérios de filtro e a barra de pesquisa.

   Pesquise o plug-in pelo nome ou ID. Se não conseguir encontrar um plug-in, talvez seja necessário solicitá-lo ao pessoal ServiceNow.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Selecione **Instalar** para iniciar o processo de instalação.

   Nota: Quando a separação de domínio e o administrador delegado estão habilitados em uma instância, o usuário administrativo deve estar no domínio **global.** Caso contrário, será exibido o seguinte erro: `A instalação da aplicação não está disponível porque há outra operação em execução: ativação de plug-in para <plugin name>.`

   Você verá uma mensagem após a conclusão da instalação.

Como criar um perfil de autenticação

Crie um perfil de autenticação e adicione uma ou mais políticas de autenticação ao perfil. Você também pode configurar os perfis de autenticação **Token de ID** e **Token OAuth** que estão disponíveis por padrão.

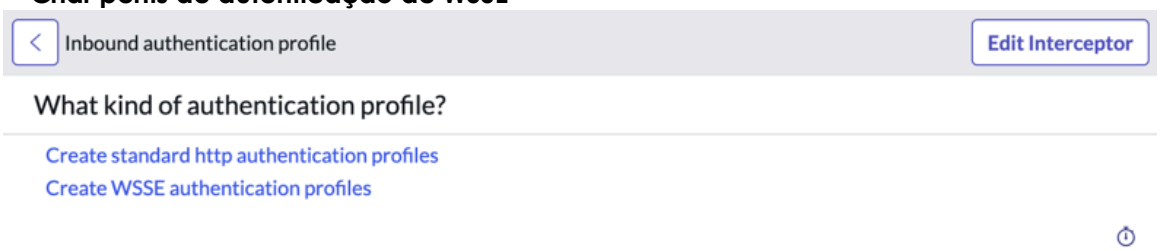
Antes de Iniciar

Função necessária: administrador

Nota: Você pode aplicar políticas de autenticação, intervalo de IPs, com base em função, com base em usuário e muito mais com autenticação mútua e autenticação personalizada.

Procedimento

1. Navegue até **Todos** > **Serviços Web do sistema** > **Políticas de acesso de API** > **Perfis de autenticação de entrada**.
2. Selecione **"Novo"**.
   O sistema exibe a mensagem. `Que tipo de perfil de autenticação?`
3. Selecione **Que tipo de perfis de autenticação?**.
   - **Criar perfis de autenticação HTTP padrão**
   - **Criar perfis de autenticação de WSSE**



4. No formulário, preencha os seguintes campos.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formulário de perfil de autenticação padrão

Campo	Descrição
Nome	Nome para identificar a política de autenticação.
Descrição	Descrição da política de autenticação.
Ativo	Opção para ativar a política de autenticação.
Aplicação	Escopo da política de autenticação.
Tipo	Tipo de autenticação disponível. Você pode selecionar **Autenticação básica**, **Token de ID**, **Autenticação baseada em certificados**, **OAuth** ou **WSSE** (no caso de perfil de autenticação WSSE).
Entidade OAuth	Perfil de entidade OAuth. Esse campo aparece somente quando **Token de ID** ou **OAuth** é selecionado em **Tipo**.

5. Clique duas vezes em **Inserir uma nova linha**.
6. Selecione uma política de autenticação na lista e selecione o ícone de salvar .

Nota: Não selecione **Política de permissão de acesso** ou **Política de negação de acesso**. Essas políticas são destinadas somente a logins dos usuários.

Você pode adicionar uma ou mais políticas de autenticação a um perfil de autenticação.

Quando há uma mudança no perfil de autenticação, o cabeçalho de autorização retorna um valor específico das mudanças feitas naquele momento. Para que todos os esquemas de autenticação sejam retornados no cabeçalho "WWW-Authenticate", você deve ativar `glide.security.response.authenticate.header.auth_profile.first_scheme_only` como **falso**. A resposta é retornada com vários cabeçalhos. Por exemplo:

```
< WWW-Authenticate: BEARER realm="Service-now"
< WWW-Authenticate: BASIC realm="Service-now"
```

Como criar a política de acesso de SOAP API

Crie uma política de acesso de API e mapeie um perfil de autenticação para restringir o tipo de autenticação de uma SOAP API. Por exemplo, você pode criar uma política de acesso de API que permita somente a autenticação de token de ID para uma SOAP API.

Antes de Iniciar

- Certifique-se de criar um perfil de autenticação. Para obter mais informações, consulte Como criar um perfil de autenticação.
- Função necessária: admin

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

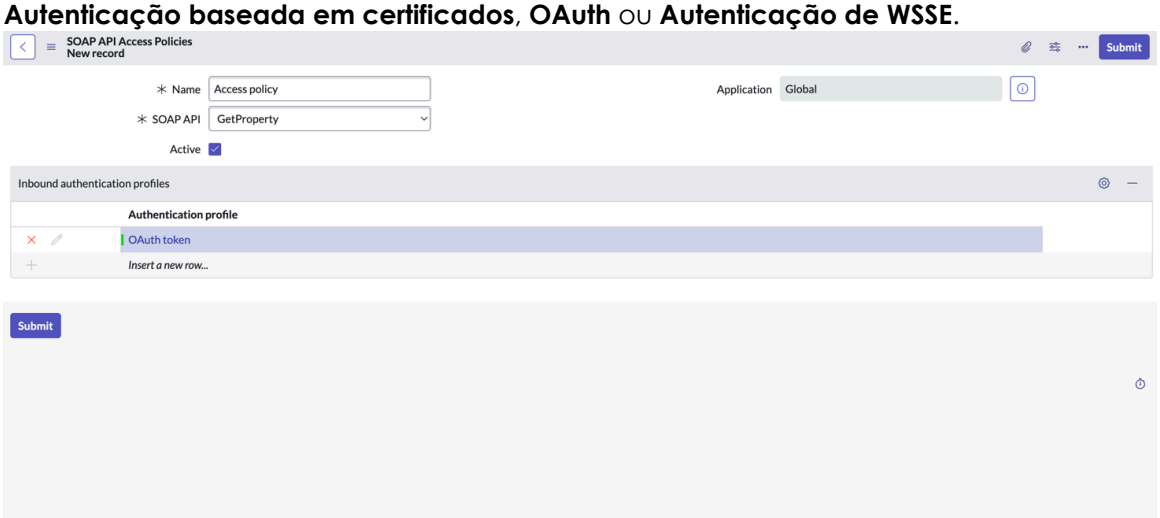
Procedimento

1. Navegue até **Todos** > **Serviços Web do sistema** > **Políticas de acesso de API** > **Políticas de acesso de SOAP API**.
2. Clique em **Nova**.
3. No formulário, preencha os campos.

Formulário Políticas de acesso de API

Campo	Descrição
Nome	Nome exclusivo da política de acesso de API.
SOAP API	SOAP API à qual a política de acesso é aplicada. Por exemplo, **API GetProperty**.
Aplicação	Escopo do aplicativo.
Ativo	Opção para ativar a política de acesso de API.

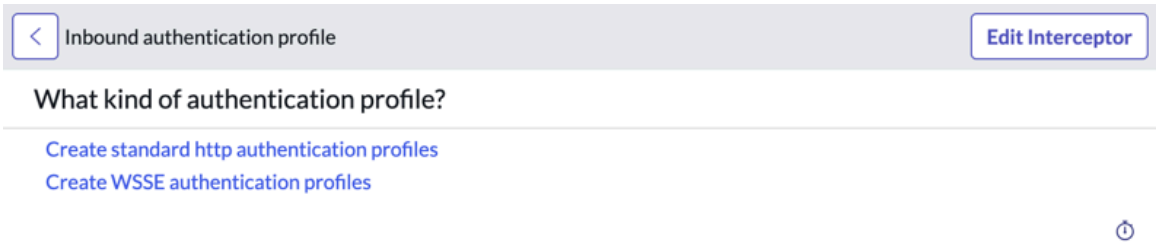
4. Na seção Autenticação de entrada, clique duas vezes em **Inserir uma nova linha**.
5. Selecione um perfil de autenticação de entrada na lista e clique no ícone de salvar . Por exemplo, você pode adicionar **Autenticação básica**, **Token de ID**, **Autenticação baseada em certificados**, **OAuth** ou **Autenticação de WSSE**.



   a. Para adicionar um ou mais perfis de autenticação de entrada, clique em **Novo** para criar um novo perfil.

   b. Selecione **Que tipo de perfis de autenticação?**.
      - **Criar perfis de autenticação HTTP padrão**
      - **Criar perfis de autenticação de WSSE**

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

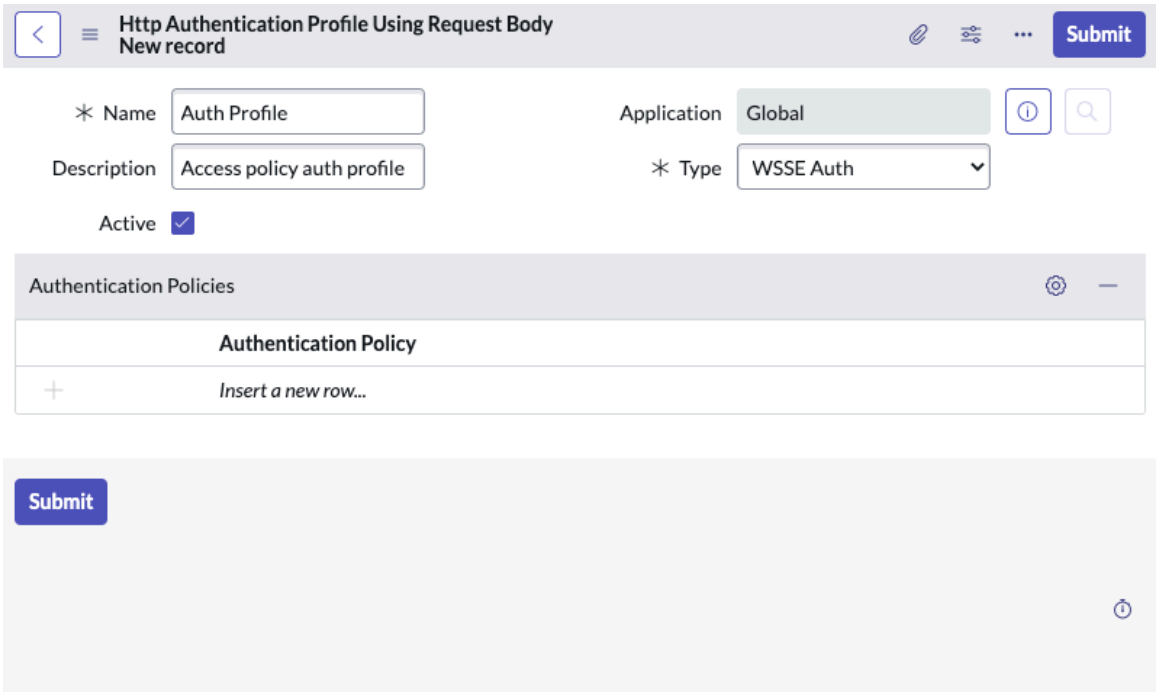


c. Para criar um perfil de autenticação WSSE, preencha os seguintes campos no formulário.

Perfil de autenticação WSSE

Campo	Descrição
Nome	Nome exclusivo da política de acesso de API.
Descrição	Descrição do perfil de autenticação.
Aplicação	Escopo do aplicativo.
Ativo	Opção para ativar a política de acesso de API.
Tipo	Autenticação WSSE como perfil de autenticação WSSE (segurança na Web).

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



d. Depois de criar o perfil de autenticação, salve o registro.

6. Clique em **Enviar** para enviar a política de acesso de SOAP API.

Criar uma política de acesso a API global para proteger as SOAP APIs

Crie uma política única de acesso a API global para proteger todas as SOAP APIs.

Antes de Iniciar

- Função necessária: admin
- Instale o plug-in **Política de Acesso do Processador** (`com.glide.processor.policy`)
- Certifique-se de criar um perfil de autenticação. Para obter mais informações, consulte Como criar um perfil de autenticação.

As etapas a seguir descrevem como criar uma política única de acesso global para proteger todas as SOAP APIs.

Nota: As políticas definidas nos níveis individuais da SOAP API substituem a política de acesso global no nível do **SOAPProcessor**.

Procedimento

1. Navegue até **Todos** > **Segurança do sistema** > **Políticas de acesso ao processo**.

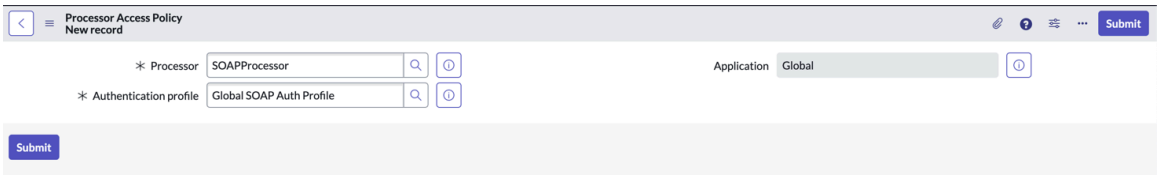
2. No formulário, preencha os campos.

Formulário de política de acesso de processo

Campo	Descrição
Processador	Nome para identificar a política de autenticação. Por exemplo, selecione **SOAPProcessor** (perfil de autenticação).

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Aplicação	Escopo da política de autenticação. Padrão: global
Perfil de autenticação	Tipo de perfil de autenticação. Selecione **Perfil de autenticação SOAP global**.



3. Selecione **Enviar**.

Critérios de filtro para APIs

Os critérios de filtro contém condições ou consultas do filtro que são usadas como entradas de política para uma política de autenticação. As entradas de política são usadas para agrupar um ou mais critérios de filtro e definir as condições da política de autenticação. Por exemplo, um critério de filtro IP define um endereço IP no formato Roteamento entre domínios sem classe (CIDR) ou um intervalo de endereços IP.

Você pode criar critérios de filtro com base no endereço IP do usuário, na função e no grupo de usuários ao qual eles pertencem.

Nota: Você também usa os critérios de filtro criados a partir do módulo **Autenticação adaptável**. Para obter mais informações, consulte Autenticação adaptável.

Você pode criar critérios de filtro para APIs usando o mesmo processo dos critérios de filtro para autenticação adaptável. Para obter detalhes, consulte Critérios de filtro.

Informações relacionadas

- Como criar critérios de filtro por IP
- Como criar critérios de filtro por função
- Como criar critérios de filtro por grupo

Políticas de autenticação de API

As políticas de autenticação avaliam as solicitações de autenticação com base nas condições de política especificadas e permitem ou negam o acesso, dependendo dos critérios correspondentes.

Você pode usar a política de bloqueio global interna ou criar uma política de autenticação de acordo com seus requisitos de segurança. A Política de bloqueio global nega as solicitações de autenticação de usuários e APIs com base nos critérios de filtro especificados.

Nota: Não use ou modifique a Política de permissão de acesso e a Política de negação de acesso. Essas políticas são destinadas somente a logins dos usuários.

Como criar uma política de autenticação de API

As políticas de autenticação permitem que você aplique restrições de acesso nas APIs com base nos critérios de filtro especificados.

Antes de Iniciar
Função necessária: administrador

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

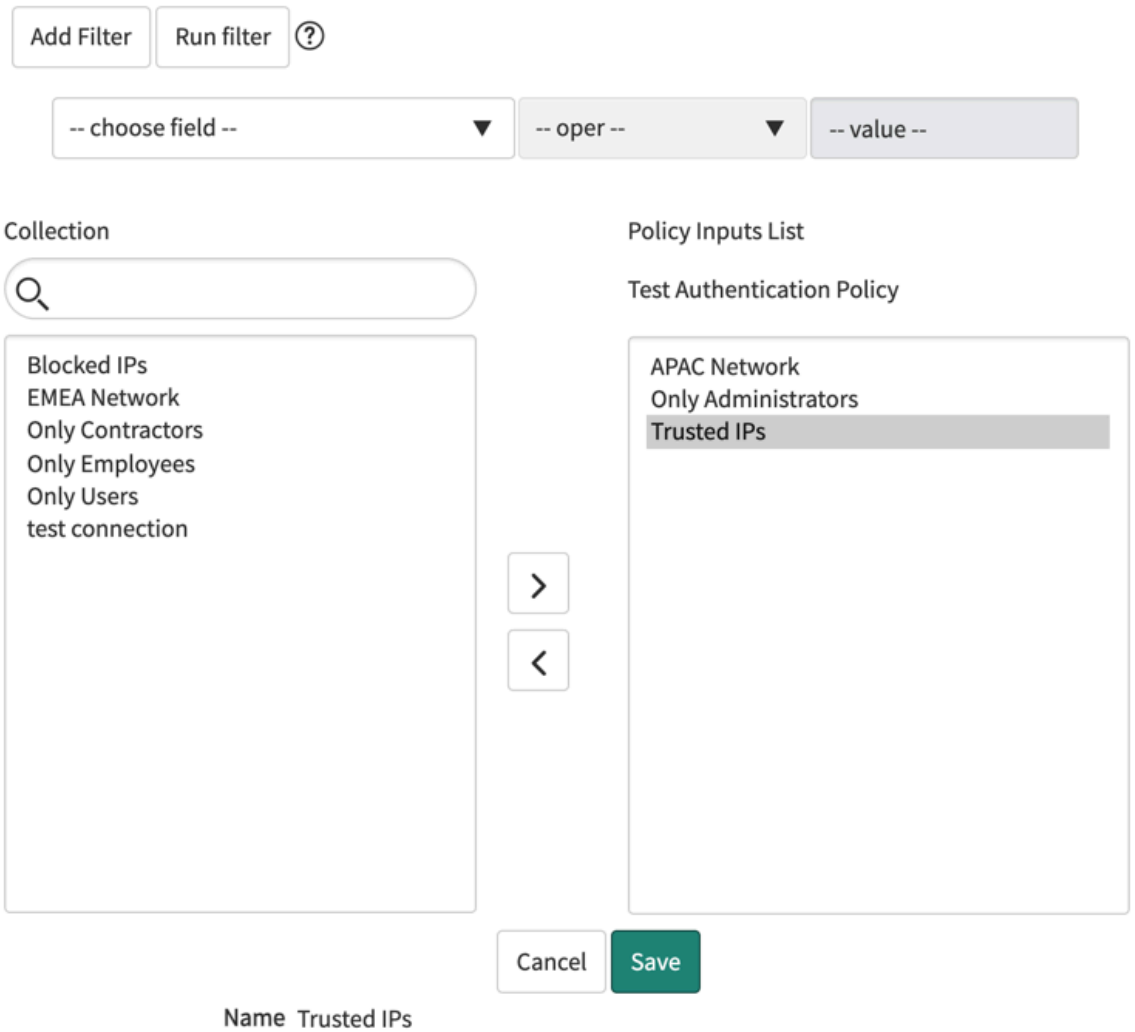
Procedimento

1. Navegue até **Todos** > **Serviços Web do sistema** > **Política de autenticação de API**.
2. Clique em **Nova**.
3. No formulário, preencha os seguintes campos.

Formulário de política

Campo	Descrição
Nome	Nome para identificar a política.
Descrição	Descrição resumida da política.
Aplicação	Escopo da aplicação.

4. Clique com o botão direito no cabeçalho do formulário e selecione **Salvar**.
5. Na guia Entradas de política, selecione **Editar** para adicionar os critérios de filtro existentes. Você também pode criar uma nova entrada de política. Para obter mais informações, consulte Criar inputs de política.
6. Mova um ou mais critérios de filtro da lista Coleção para a Lista de entradas de política.



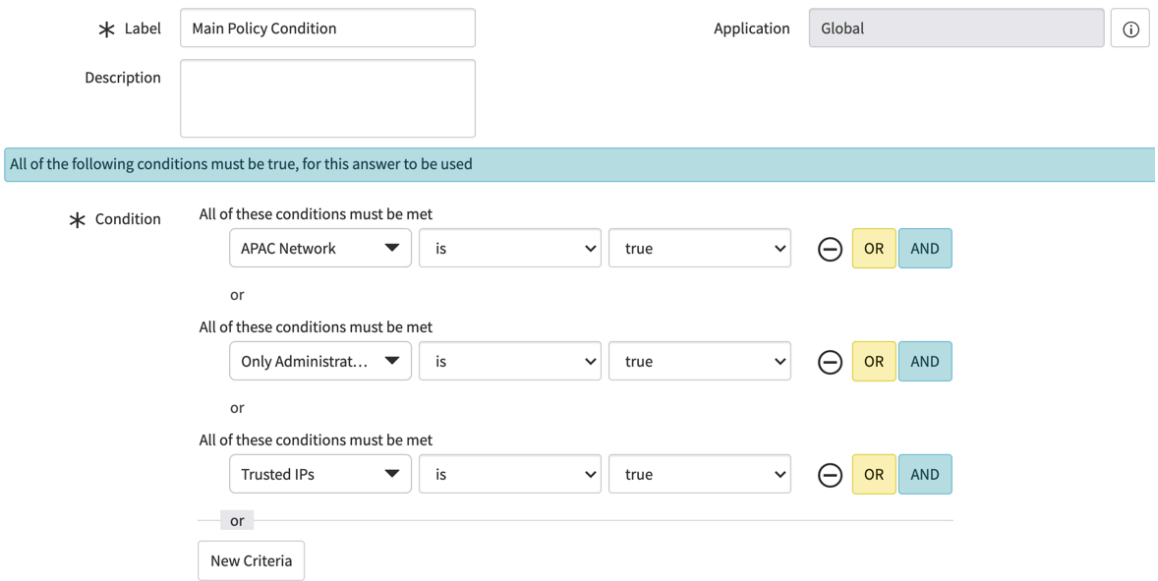
7. Selecione **Salvar**.
8. Na guia Condições da política, selecione **Nova**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

9. No formulário, preencha os seguintes campos.

Formulário de condições

Campo	Descrição
Rótulo	Nome da condição da política.
Descrição	Descrição resumida da condição da política.
Aplicação	Escopo da aplicação.
Condição	Uma ou mais condições combinadas com o filtro **OR**.



10. Selecione **Enviar**.

Como configurar a política de bloqueio global para APIs

A política de bloqueio global nega as solicitações de autenticação de usuários e APIs com base nas condições de política especificadas. Esta política pode ser usada como uma alternativa ao Controle de acesso de endereços IP.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Navegue até **Todos** > **Serviços Web do sistema** > **Políticas de acesso de API** > **Política de bloqueio global**.
2. Na guia **Entradas de política**, clique em **Editar**.
3. Selecione um ou mais critérios de filtro na lista **Coleção** e mova-os para a lista **Política de bloqueio global**.
   Você também pode adicionar outros filtros.
4. Na guia **Condições da política**, clique em **Novo**.
5. No formulário, preencha os seguintes campos:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formulário de condições

Campo	Descrição
Rótulo	Nome para identificar a condição.
Descrição	Descrição da condição.
Condição	Combinação lógica de várias entradas de política (critérios de filtro) para avaliar solicitações de autenticação. Por exemplo, você pode criar condições que permitem somente prestadores de serviços de uma lista de endereços IP confiáveis.

Política de acesso para Processadores de sistema/exportação

Capacidade dos Processadores de sistema/exportação de aproveitar a política de acesso do processador para proteger todos os endpoints de exportação.

Capacidade de proteger todos os endpoints de exportação e aplicar o perfil de autenticação de entrada e as políticas de acesso do processador em um nível global ou em um nível de instância.

Nota:

- Processadores não públicos, incluindo os processadores de exportação como CSV, PDF etc., são compatíveis com as políticas de acesso.
- Os processadores de script também são compatíveis com as políticas de acesso.

Amostras de casos de uso

- O administrador pode bloquear o processador RSS se não tiver a intenção de usá-lo, aproveitando a política de acesso de API.
- O administrador pode criar um perfil de autenticação com autenticação básica e associar uma política de autenticação que sempre seja avaliada como falsa.

  Por exemplo, crie critérios IP com um intervalo de `0.0.0.0` a `255.255.255.255` (adicione também o espaço de endereço Ipv6) e adicione a condição de política com o operador falso. Dessa forma, as condições da política sempre serão avaliadas como falsas e a política de acesso de API bloqueará o acesso, independentemente da origem da solicitação.

- Permissão de acesso ao processador somente de uma rede confiável.

Como ativar a política de acesso do processador

Para o processador, instale o plug-in Processor Access Policy (`com.glide.processor.policy`).

Antes de Iniciar
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa
Os itens a seguir são instalados com o plug-in Processor Access Policy:

- Propriedade do sistema: com.glide.auth.profile.supported.processor.list
- Módulo na navegação: políticas de acesso do processador

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegue até **Todos** > **Aplicações do sistema** > **Todas as aplicações disponíveis** > **Todas**.
2. Encontre o plug-in Processor Access Policy (`com.glide.processor.policy`) usando os critérios de filtro e a barra de pesquisa.

   Pesquise o plug-in pelo nome ou ID. Se não conseguir encontrar um plug-in, talvez seja necessário solicitá-lo ao pessoal ServiceNow.

3. Selecione **Instalar** para iniciar o processo de instalação.

   Nota: Quando a separação de domínio e o administrador delegado estão habilitados em uma instância, o usuário administrativo deve estar no domínio **global**. Caso contrário, será exibido o seguinte erro: `A instalação da aplicação não está disponível porque há outra operação em execução: ativação de plug-in para <plugin name>.`

   Você verá uma mensagem após a conclusão da instalação.

O que Fazer Depois

.
Configure o perfil de autenticação para os processadores. Para obter mais informações, consulte Como configurar o perfil de autenticação para processador.

Como configurar o perfil de autenticação para processador

Aplique o perfil de autenticação para os processadores de exportação.

Antes de Iniciar

Função necessária: administrador

Plug-in necessário: Processor Access Policy (`com.glide.processor.policy`)

Procedimento

1. Navegue até **Todos** > **Segurança do sistema** > **Políticas de acesso ao processo**.
2. Para adicionar perfil de autenticação ao processador, clique em **Novo**.
3. No formulário, preencha os seguintes campos.

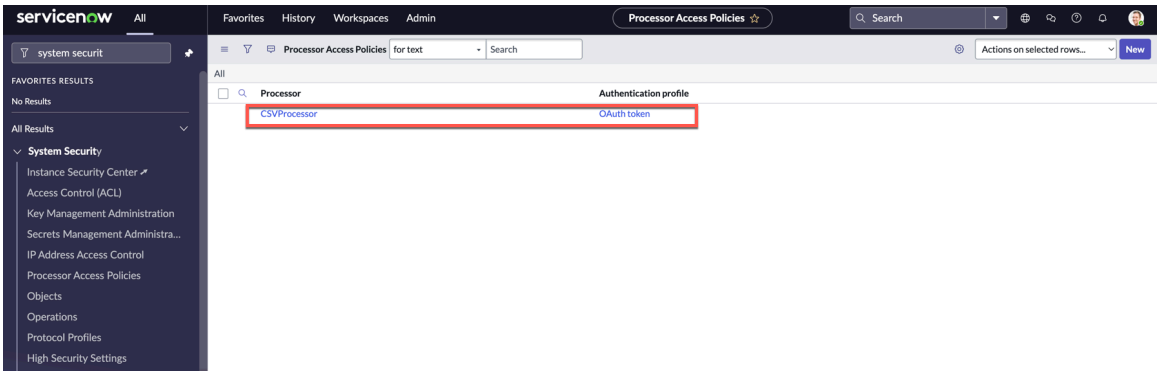
Formulário de política de acesso de processo

Campo	Descrição
Processador	Nome para identificar a política de autenticação. **Nota:** Processadores públicos não são compatíveis. Se um processador não compatível for selecionado, um erro será exibido durante o envio do processador.
Aplicação	Escopo da política de autenticação. Padrão: global
Perfil de autenticação	Tipo de perfil de autenticação. Você pode selecionar **token de ID** ou **token OAuth**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Clique em **Enviar**.
   O perfil de autenticação é aplicado ao processador.

   Por exemplo, o perfil de autenticação OAuth está configurado para o processador CSV. Nesse caso, você precisa usar o token de acesso OAuth para a exportação usando CSV como uma opção de exportação.



Autenticação baseada em certificados

A autenticação baseada em certificados permite autenticar mutuamente logins dos usuários ou solicitações de API de entrada usando certificados de uma autoridade de certificação (CA) confiável.

Nota: A autenticação baseada em certificados não é compatível com o local e a instância habilitada para edge encryption.

Autenticação baseada em certificados para logins de interface do usuário

Permite que os usuários finais usem os cartões PIV (Personal Identity Verification) ou CAC (Common Access Card) para fazer login em Now Platform ou em Portal de serviços em vez de usar um nome de usuário e uma senha. Para configurar a autenticação mútua para logins de interface do usuário, consulte Como configurar autenticação baseada em certificados.

Depois que a autenticação baseada em certificados for configurada, os usuários finais podem finalizar a configuração e fazer login. Consulte Faça login usando a autenticação baseada em certificados.

Autenticação baseada em certificados para serviços Web de entrada

Autentique solicitações de entrada para SOAP e REST APIs de ServiceNow. Para configurar a autenticação mútua para serviços Web de entrada, consulte Como configurar autenticação baseada em certificados.

Como configurar autenticação baseada em certificados

Configure a autenticação mútua para logins baseados na interface do usuário ou serviços da Web de entrada.

Antes de Iniciar

Função necessária: administrador

Verifique se sua instância está usando um balanceador de carga ADCv2. Para obter mais informações, consulte o artigo de conhecimento da migração do ADCv2. Se sua instância não estiver usando o balanceador de carga ADCv2, entre em contato com Now Support.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

Configure a autenticação baseada em certificados para:

- Permitir que os usuários finais façam login com segurança em Now Platform ou em Portal de serviços usando cartões PIV ou CAC. Depois que a autenticação baseada em certificados for habilitada, você poderá registrar automaticamente o certificado PEM ou um administrador poderá mapear o certificado para você. Consulte Faça login usando a autenticação baseada em certificados.
- Habilitar a autenticação mútua para serviços da Web de entrada. Depois que a autenticação baseada em certificados é configurada, o sistema usa os certificados fornecidos para autenticar mutuamente as solicitações de acesso às REST e SOAP APIs de ServiceNow.

Como ativar o plug-in Autenticação baseada em certificado

Você pode ativar o plug-in Autenticação baseada em certificado (com.glide.auth.mutual) para Now Platform se tiver a função de administrador.

Antes de Iniciar
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa
As tabelas a seguir são instaladas com o plug-in Autenticação baseada em certificado:

- sys_user_certificate
- sys_ca_certificate
- sys_ca_certificate_api_track

Procedimento

1. Navegue até **Todos** > **Aplicações do sistema** > **Todas as aplicações disponíveis** > **Todas**.
2. Encontre o plug-in Autenticação baseada em certificado (com.glide.auth.mutual) usando os critérios de filtro e a barra de pesquisa.

   Pesquise o plug-in pelo nome ou ID. Se não conseguir encontrar um plug-in, talvez seja necessário solicitá-lo ao pessoal ServiceNow.

3. Selecione **Instalar** para iniciar o processo de instalação.

   Nota: Quando a separação de domínio e o administrador delegado estão habilitados em uma instância, o usuário administrativo deve estar no domínio **global**. Caso contrário, será exibido o seguinte erro: `A instalação da aplicação não está disponível porque há outra operação em execução: ativação de plug-in para <plugin name>.`

   Você verá uma mensagem após a conclusão da instalação.

Como registrar o certificado CA

Registre certificados raiz ou certificados intermediários para disponibilizá-los para autenticação.

Antes de Iniciar
Função necessária: administrador

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegue até **Todos** > **Autenticação baseada em certificados** > **Cadeias de certificados de CA**.
2. Clique em **Nova**.
3. No formulário, preencha os campos:

Formulário de certificado de CA de autenticação mútua

Campo	Descrição
Nome	Nome para identificar o certificado.
Notificação de expiração	Opção para avisar os usuários quando um certificado está prestes a expirar.
Notificar no vencimento	Lista de usuários a serem notificados quando o certificado expirar.
Aviso emitido antes do vencimento (em dias)	Número de dias em que uma notificação é enviada aos usuários antes que um certificado expire.
Ativo	Opção para ativar o certificado do cliente.
Formato	PEM
Tipo	Tipo de certificado. As opções incluem: ◦ **Certificado de CA**: o certificado de CA raiz. Também pode incluir certificados intermediários na cadeia. Os certificados de CA são sincronizados automaticamente com o balanceador de carga. Use esta opção sempre que possível para evitar a perda de um certificado necessário na cadeia. ◦ **Certificado intermediário**: um certificado intermediário na cadeia de certificação. Este certificado permanece somente na instância e não é sincronizado com o balanceador de carga. Use esta opção somente se você precisar adicionar um certificado intermediário a uma cadeia existente.
Descrição resumida	Descrição resumida do certificado de cliente do usuário.

Nota: Durante o carregamento do certificado, os campos de somente leitura **Válido de**, **Expira emDias até o vencimento**, **Emissor**e **Assunto**, e os campos **Cadeia de certificados** e **Certificado PEM** são extraídos e preenchidos automaticamente.

4. Clique em **Enviar**.
5. Opcional: Clique em **Validar armazenamentos/certificados** para validar o certificado.

Como mapear um certificado PEM para usuário

Mapeie certificados PEM para usuários para permitir que eles façam login usando cartões PIV ou CAC ou para autenticar solicitações de entrada. Você pode mapear vários certificados PEM para um usuário.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

- Função necessária: administrador
- Verifique se você tem o certificado de Correio eletrônico com privacidade aprimorada (Privacy Enhanced Mail, PEM) do usuário.

Nota: Após mapear o certificado PEM para a configuração do usuário, a "verificação do certificado" falhará. Isso ocorre porque o certificado PEM não está armazenado.

Procedimento

1. Navegue até **Todos** > **Autenticação baseada em certificados** > **Mapeamento de certificado para usuário** e clique em **Novo**.
2. No formulário, preencha os seguintes campos:

Formulário do certificado de cliente do usuário

Campo	Descrição
Nome	Nome do certificado de cliente do usuário.
Notificação de expiração	Opção para avisar os usuários quando um certificado está prestes a expirar.
Aviso emitido antes do vencimento (em dias)	Número de dias em que uma notificação é enviada aos usuários antes que um certificado expire.
Notificar no vencimento	Lista de usuários a serem notificados quando o certificado expirar.
Ativo	Opção para ativar o certificado do cliente.
Usuário	Usuário mapeado para o certificado do cliente. O sistema recebe o certificado do cliente da solicitação de entrada ou do registro do certificado e, em seguida, usa o usuário designado neste campo para iniciar uma sessão para executar a solicitação.
Descrição resumida	Descrição resumida do certificado de cliente do usuário.
Formato	O formato Correio eletrônico com privacidade aprimorada (PEM) é um certificado de Regras de codificação distintas (DER) codificado em base 64.
Tipo	Certificado do cliente Este campo é somente leitura.

Nota: Durante o carregamento do certificado, os campos somente leitura **Válido de**, **Expira em**, **Dias até o vencimento**, **Emissor**e **Assunto** são extraídos e preenchidos automaticamente.

3. Clique no ícone de anexos e carregue o certificado.
4. Clique em **Enviar**.
   O certificado será validado e mapeado para o usuário especificado se o certificado for de uma autoridade de certificação (CA) confiável.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Como configurar as propriedades da autenticação baseada em certificados

Use as propriedades do sistema para habilitar ou desabilitar recursos da autenticação baseada em certificados.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Navegue até **Todos** > **Autenticação baseada em certificados** > **Propriedades**.
2. No formulário, preencha os campos:

Formulário de propriedades da autenticação baseada em certificados

Propriedade	Descrição
Habilitar autenticação baseada em certificado	Opção para habilitar a autenticação baseada em certificados para logins de interface do usuário e serviços da Web de entrada. Padrão: verdadeiro
Mostrar a opção "Login com PIV/CAC" na tela de login	Exibe a opção **Login com cartão PIV/CAC** na tela de login. Permite que os usuários façam login usando a autenticação baseada em certificados ao usar a interface do usuário. Padrão: falso
Habilitar redirecionamento automático para login baseado em certificados	Determina se o usuário deve clicar em **Login com cartão PIV/CAC** depois de selecionar um certificado registrado e inserir seu PIN. Ative para fazer login automaticamente do usuário depois que ele selecionar um certificado de cliente registrado e inserir seu PIN. Desative para solicitar que o usuário clique em **Login com cartão PIV/CAC** depois de selecionar um certificado de cliente registrado e inserir seu PIN. Padrão: falso

Faça login usando a autenticação baseada em certificados

Depois que o administrador configurar a autenticação baseada em certificados, será possível registrar o certificado do cliente e fazer login usando seu cartão PIV (Personal Identity Verification) ou CAC (Common Access Card).

Registre o certificado do cliente para seu cartão PIV ou CAC

Antes de fazer login na Now Platform usando seu cartão PIV ou CAC, será necessário registrar o certificado de cliente do seu cartão PIV ou CAC. Se conseguir registrar o certificado do cliente, entre em contato com o administrador. O administrador também pode registrar o certificado do cliente do seu cartão PIV ou CAC.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

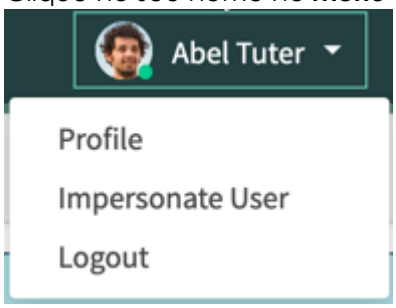
- Certifique-se de que a autenticação baseada em certificados esteja habilitada.
- Verifique se um leitor de cartão está conectado ao computador e se o cartão PIV ou CAC está inserido.
- Função necessária: nenhuma

Por Que e Quando Desempenhar Esta Tarefa

Se precisar de um administrador para registrar seu certificado de cliente, consulte Como mapear um certificado PEM para usuário.

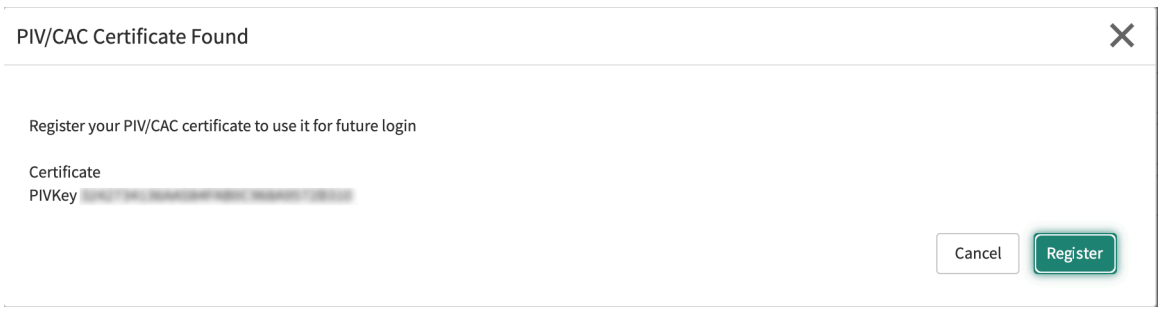
Procedimento

1. Faça login na Now Platform usando seu nome de usuário e senha.
2. Clique no seu nome no **Menu do usuário** e selecione **Perfil**.



3. Em **Links relacionados**, clique em **Registrar certificado de cliente**.

   A seguinte mensagem será exibida se um certificado válido estiver disponível:

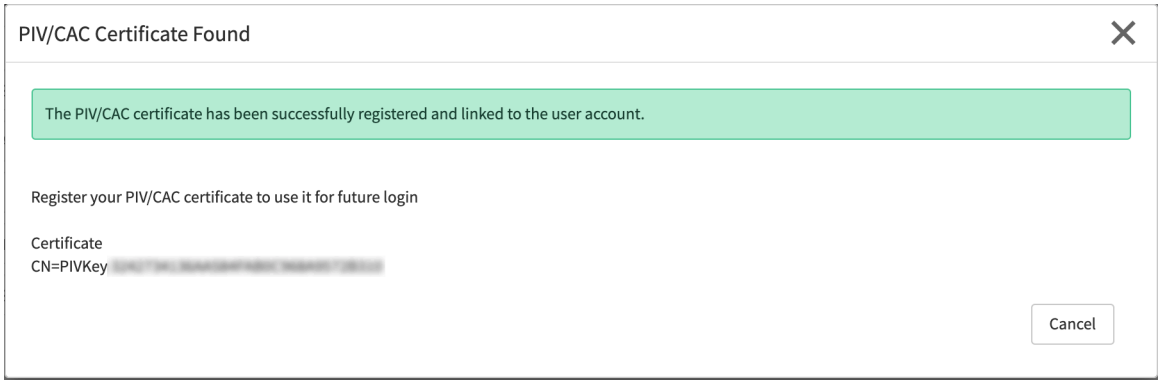


4. Clique em **Registrar**.

   A seguinte mensagem será exibida depois que o registro for bem-sucedido:

   ```
   O certificado PIV/CAC foi registrado e vinculado à conta do usuário com sucesso.
   ```

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Na próxima vez em que fizer login na Now Platform, você poderá usar seu cartão PIV ou CAC. Para obter mais informações, consulte Faça login em Now Platform usando o cartão PIV ou CAC.

Faça login em Now Platform usando o cartão PIV ou CAC

É possível fazer login com seu cartão PIV ou CAC em vez do nome de usuário e senha quando a autenticação baseada em certificados estiver habilitada em Now Platform.

Antes de Iniciar

- Função necessária: nenhuma
- Certifique-se de que a autenticação baseada em certificados esteja habilitada.
- Certifique-se de que um leitor de cartão PIV ou CAC esteja conectado ao seu computador.
- Certifique-se de que um certificado de cliente do seu cartão PIV ou CAC esteja mapeado até você. Para obter mais informações, consulte Como registrar o certificado CA.

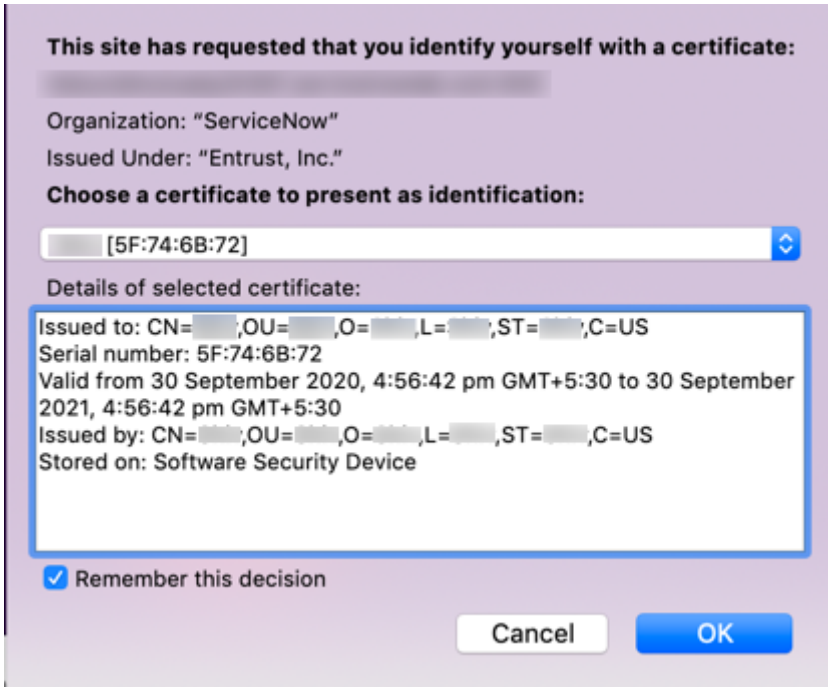
Procedimento

1. Insira seu cartão PIV ou CAC no leitor de cartão.
2. Navegue até sua instância em um navegador.
   O navegador solicita um PIN para o cartão PIV ou CAC.
3. Insira o PIN do seu cartão PIV ou CAC no prompt do navegador.

   Nota: Se esquecer o PIN, entre em contato com o administrador.

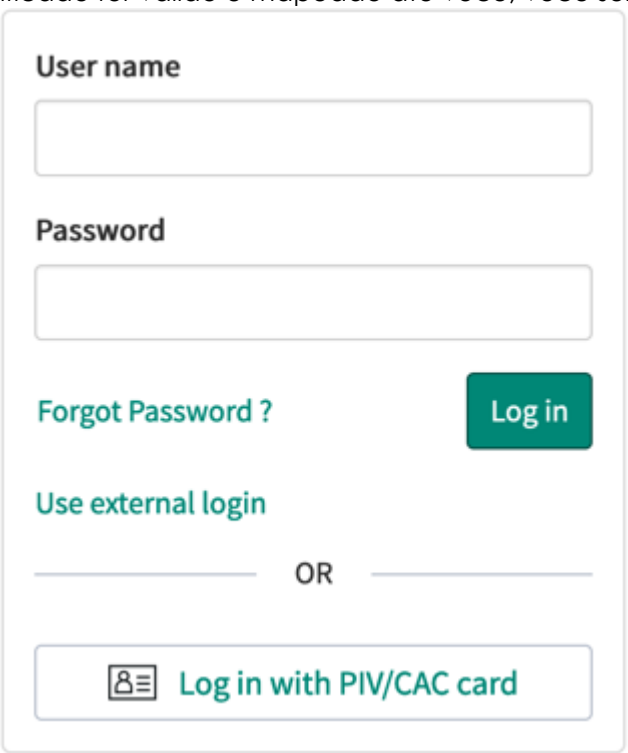
4. Se um PIN correto for inserido, o navegador exibirá um aviso para selecionar um certificado.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Selecione um certificado no prompt do navegador.

   Se o certificado for válido e mapeado até você, você será redirecionado para a página de login.



6. Clique no botão **Fazer login com cartão PIV/CAC**.

   Para fazer logout da Now Platform, remova o PIV ou CAC do leitor de cartão e feche o navegador.

Gerenciamento de certificados de clientes

Exiba e exclua certificados de cliente associados à sua conta.

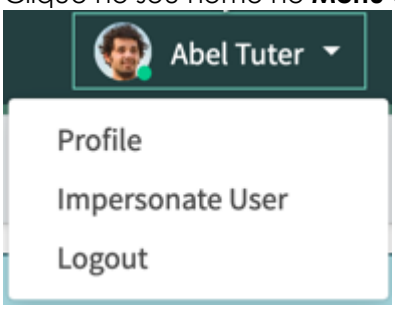
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

- Certifique-se de que a autenticação baseada em certificados esteja habilitada.
- Função necessária: nenhuma

Procedimento

1. Faça login à Now Platform usando seu nome de usuário e senha.
2. Clique no seu nome no **Menu do usuário** e selecione **Perfil**.



3. Em **Links relacionados**, clique em **Gerenciar certificados de clientes**.
   A tabela certificados de cliente do usuário [sys_user_certificate] é aberta e exibe os certificados associados à sua conta.
4. Exiba ou exclua os certificados associados à sua conta.

Associação de URLs personalizadas para sua instância

É possível habilitar sua instância ServiceNow para ser acessível a partir de Uma URL personalizada ou da marca da empresa.

Visão geral da URL personalizada

É possível usar URLs personalizadas para permitir que a instância ServiceNow seja acessível a partir de um ou mais URLs personalizadas ou de marca da empresa.

URLs personalizadas podem ser associados a um portal específico. Por exemplo, o administrador pode definir `http://support.acme.com` para o portal CSM e `http://hr.acme.com` para o portal de RH. Nessa situação, é necessário redirecionar os usuários para diferentes IdPs para autenticação com base na URL personalizada que estão acessando.

Importante:

- Não crie uma URL personalizada com mais de 100 domínios por instância.
- Você deve excluir o registro de URL personalizada da instância de ServiceNow primeiro, depois excluir todas as entradas de servidor de nomes de domínio (DNS) do servidor DNS.
- Qualquer exclusão de entrada DNS do Servidor DNS antes da exclusão do registro de URL personalizada da instância de ServiceNow resultaria no bloqueio da exclusão de outros registros de URL personalizada correspondentes de ServiceNow.

Em Tokyo, é possível permitir que os usuários redirecionem automaticamente para IdPs especificados definidos no registro de URL personalizada.

Nota: URLs personalizadas não estão disponíveis para clientes no local ou instâncias de desenvolvedor. Além disso, o URL deve ser voltado para o público.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Somente o proprietário do domínio de nível superior (TLD) ou qualquer subdomínio pode configurar a URL personalizada para um subdomínio DNS. Por exemplo, sua instância pode ter o seguinte URL designado e URLs personalizadas adicionais:

Exemplo de URL personalizada

URLs de exemplo	Uso
`https://acme.service-now.com`	O nome do domínio inicial da Acme que acompanha a instância ServiceNow.
`https://support.acme.com`	Uma URL personalizada que se associa à sua instância ServiceNow. Este URL é conhecido como um alias (CNAME) do nome do domínio inicial.
`https://US-support.acme.com`	Uma URL personalizada secundário associado a um portal de serviços em sua instância. Sua instância pode oferecer suporte a vários URLs personalizadas para o mesmo portal de serviços.

Considerações para URLs personalizadas fora da sua instância

Antes de associar Uma URL personalizada, é preciso ter (ou comprar) um URL por meio de um provedor de domínio. Também há configurações específicas necessárias antes de criar e associar Uma URL personalizada à sua instância.

Configurações de URL personalizadas

Itens de configuração	Descrição
Defina o CNAME com o provedor	O registro CNAME deve ser definido como o URL da instância ServiceNow.
Determine seu status de VIP dedicado	O status de VIP.

Nota: Ao excluir ou atualizar registros CNAME que apontam para sua instância, é necessário seguir esta sequência para evitar registros pendentes na instância. Primeiro, exclua os registros CNAME da sua instância e, em seguida, remova ou atualize a configuração CNAME no seu provedor DNS.

Ativação de URLs personalizadas

Habilite a configuração de URLs personalizadas em sua instância ServiceNow. Você pode ativar o plug-in URL personalizadas (com.snc.customurl) se tiver a função de administrador.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Navegue até **Todos** > **Definição do sistema** > **Plug-ins**.
2. Encontre e clique no plug-in **URL personalizada**.

Nota: Não selecione o plug-in **URL personalizada - Interna**, que é um componente interno das APIs de URL personalizada com script.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. No registro de URL personalizada, clique no link relacionado **Ativar/Reparar** .
4. Na janela Ativação do plug-in, clique em **Ativar**.
   Quando a janela Ativação do plug-in for reaberta com uma mensagem de que o plug-in está ativado, clique em **Fechar e recarregar formulário** para permanecer neste formulário.
5. Na lista relacionada Arquivos de plug-in, localize a seguinte propriedade e altere o valor da configuração:

Opção	Descrição
glide.customurl.enabled	Para habilitar URLs personalizadas, defina o valor como **Verdadeiro**. Por padrão, esta propriedade é definida como **Falso**, o que significa que você não pode associar uma URL personalizada. **Nota:** Para desabilitar esse recurso, defina essa propriedade novamente como **Falso**.

6. Clique em **Atualizar**.

Definição de Uma URL personalizada como o URL da instância

Adicione Uma URL personalizada à configuração da sua instância para ser usado em vez do URL ServiceNow.

Antes de Iniciar

Função necessária: administrador
É preciso ativar o plug-in URL personalizada e ter comprado ou registrado um URL antes de adicionar a URL personalizada à sua instância.

Procedimento

1. Navegue até **Todos** > **URL personalizada** > **URL personalizadas**.
2. Você deve:
   - Clicar em **Novo** para associar um novo nome do domínio à sua instância.
   - Selecionar Uma URL personalizada já configurado para ser definido como o URL da sua instância.
3. Preencha os campos se necessário:

Campos de URL personalizada

Campo	Descrição
Nome do domínio	Nome do domínio totalmente qualificado (FQDN) da URL personalizada. O FQDN é um redirecionamento CNAME criado no registro do servidor de nomes para o domínio personalizado.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: Por exemplo, no servidor de nomes para acme.com, é possível criar uma entrada: `support.acme.com 300 IN CNAME acme.servicenow.com`
É URL da instância	Marque a caixa para habilitar este URL personalizada para todos os URLs de saída. Somente Uma URL personalizada ativo pode ser o URL da instância. Para habilitar esta configuração para Uma URL personalizada, clique em **Definir como URL da instância** no registro do URL. Todos os URLs personalizados anteriores são removidos.
Status	Status do registro da URL personalizada. Se o status for **Ativo**, a URL personalizada estará provisionado e pronto para uso.
Portal de serviços	O portal de serviços a ser usado para o redirecionamento de usuários para sua instância usando a URL personalizada.
Provedor de identidade	O provedor de identidade para a URL personalizada permite que você permita que os usuários redirecionem automaticamente para IdPs especificados definidos no registro de URL personalizada.

Uma URL personalizada deve ser ativado em sua instância em até seis horas.

Nota:

- Você deve excluir o registro de URL personalizada da instância de ServiceNow primeiro, depois excluir todas as entradas de servidor de nomes de domínio (DNS) do servidor DNS.
- Qualquer exclusão de entrada DNS do Servidor DNS antes da exclusão do registro de URL personalizada da instância de ServiceNow resultaria no bloqueio da exclusão de outros registros de URL personalizada correspondentes de ServiceNow.

URL personalizada com provedor de identidade

Defina seu URL personalizada com o provedor de identidade para permitir que o usuário faça login com seu IdP.

Antes de Iniciar

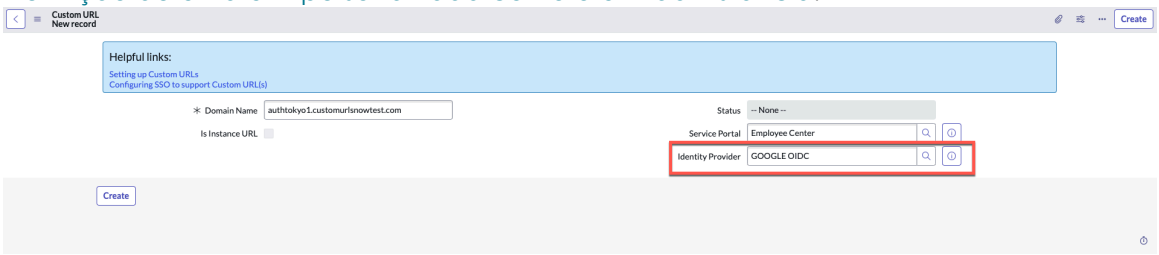
Função necessária: administrador

Procedimento

1. Navegue até **Todos** > **URL personalizada** > **URL personalizadas**.
2. Clique em **Novo**.

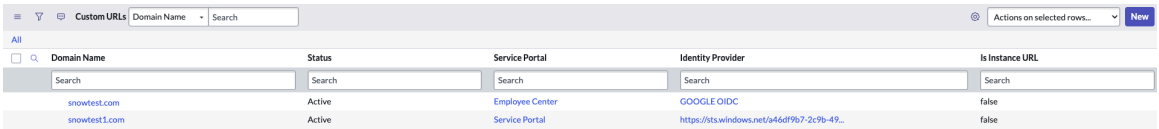
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Forneça os detalhes do IdP no campo **Provedor de identidade**.
   Para obter informações sobre outros campos, consulte Definição de Uma URL personalizada como o URL da instância.



4. Clique em **Criar**.

   O registro é criado e exibido na página da URL personalizada.



   Quando a URL personalizada é acessado, o usuário é redirecionado para o provedor de identidade configurado. Nesse caso, ao acessar o `snowtest.com`, o usuário é conduzido até a **Central do funcionário**e, em seguida, redirecionado para o Google provedor de identidade.

   Nota:

   - Se o campo Portal de serviços estiver vazio e o campo Provedor de identidade estiver definido, quando acessar a URL personalizada, o usuário será conduzido diretamente para o provedor de identidade configurado.
   - Se Portal de serviços e o campo Provedor de identidade estiverem definidos, quando acessar a URL personalizada com o Portal de serviços definido, o usuário será conduzido até o provedor de identidade configurado.
   - Se Portal de serviços e o campo Provedor de identidade estiverem definidos, quando acessar a URL personalizada com o portal diferente não definido, o usuário será conduzido para o provedor de identidade de redirecionamento automático se configurado na instância.

5. Use as credenciais para fazer login na aplicação.

Informações do trabalho do datacenter da URL personalizada

Cada URL personalizada associada à sua instância tem um trabalho de datacenter da ServiceNow correspondente que é executado e mostra informações de URL pertinentes à sua instância conforme descrito na tabela.

Campo Trabalho	Descrição
ID do trabalho	ID exclusivo do trabalho que verifica o domínio da URL personalizada.
Última execução em	Data e hora da última execução do trabalho.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo Trabalho	Descrição
Carga	Lista de domínios/URLs personalizadas enviados ao datacenter para o provisionamento de CERT
Contagem de pesquisas	Número de vezes que os resultados foram pesquisados para este trabalho.
Resultado	Verifica e valida cada domínio ou URL personalizada enviados em uma carga.
Status	Status do trabalho do datacenter.

Como gerar metadados de SP para instalações de URL personalizada de SAML/SSO

Uma instalação de SAML ou SSO precisa dos metadados de SP gerados para o IdP antes que a instância da URL personalizada seja gerada.

Antes de Iniciar

Função necessária: administrador
O IdP precisa de metadados do SP para que a instância seja autenticada e encaminhe solicitações.

Nota: Adicionar o URL do serviço de asserção ao consumidor (URL de login do SP) pode ser diferente para cada IdP (Azure, ADFS ou Okta).

Procedimento

1. Escolha o plug-in SSO instalado:

Opção	Descrição
SSO Multiprovedor	Navegue até **SSO de vários provedores** > **Provedores de identidade**. Escolha um IdP e clique no botão **Gerar metadados**. A integração gera automaticamente os metadados do SP da instância a partir das configurações de propriedade do sistema.
SAML 2 SSO	Navegue até **SAML 2 Single Sign-on** > **Metadados**. A integração gera automaticamente os metadados do SP da instância a partir das configurações de propriedade do sistema.

2. Copie os metadados do SP na caixa de texto.

Por exemplo:

```
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
 entityID="https://yourinstance.service-now.com">
  <SPSSODescriptor AuthnRequestsSigned="false"
 WantAssertionsSigned="true"
 protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
  <SingleLogoutService
 Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
 Location="https://yourinstance.service-now.com/navpage.do" />
```

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

```
 <NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddres
s</NameIDFormat>
  <AssertionConsumerService isDefault="true" index="0"
 Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
 Location="https://yourinstance.service-now.com/navpage.do" />
  <AssertionConsumerService index="1"
 Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
 Location="https://yourinstance.service-now.com/consumer.do"/>
 </SPSSODescriptor>
</EntityDescriptor>
```

3. Forneça os metadados do SP da instância para o IdP.
   Por exemplo, SSOCircle permite que um usuário forneça os metadados do SP online.
4. Opcional: Para configurar URLs personalizados no Azure:
   a. Navegue até **Registros de apps**.
   b. Selecione **Todos os apps** no menu.
   c. Selecione o **app ServiceNow**.
   d. Clique em "Configurações" para configurar a URL.
5. Opcional: Para configurar URLs personalizadas no Okta:
   a. Crie duas aplicações do diretório universal Okta da ServiceNow.
   b. Uma aplicação Okta para a URL da instância "service-now.com".
   c. Uma aplicação Okta para a URL personalizada.

   Nota:
   - Desabilite a opção **Desabilitar autenticação forçada** na configuração do Okta para que a **Testar conexão** seja executada.
   - Para testar o registro do provedor de identidade associado ao URL base, faça login na instância com a URL base.
   - Para testar o provedor de identidade associado à URL personalizada, faça login na instância com a URL personalizada.
6. Opcional: Para usar a autenticação OAuth, configure o URL de redirecionamento como todos os URLs personalizados registrados na configuração do endpoint da aplicação OAuth para as aplicações de cliente externos.
   O URL de redirecionamento é sinônimo do URL de retorno de chamada para o qual o servidor de autorização faz o redirecionamento.
7. Opcional: Para usar o serviço Google reCAPTCHA, configure um par de chaves de API.

Erros e correções de URL personalizada

Uma lista de erros comuns e correções associadas para uma configuração ou configuração de URL personalizada.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Erros durante a configuração

Mensagem de erro	Correção
Não é possível criar Uma URL personalizada. Tente novamente mais tarde.	Pode haver um problema fora do seu controle que interfira na criação da URL personalizada. Faça a execução em um horário diferente antes de entrar em contato com o suporte. **Nota:** Em geral, são necessários 30 minutos para criar Uma URL personalizada. Se levar mais tempo, entre em contato com https://support.servicenow.com/now?draw=case.
Não foi possível enviar sua nova solicitação da URL personalizada porque há outra solicitação para a sua instância em andamento.	Verifique o status dos trabalhos de URL personalizada antes de enviar uma nova solicitação.
Você deve limpar as seguintes propriedades antes que o URL da instância possa ser definido: Glide Proxy, Glide Servlet.	
O provisionamento de <custom_domain> ainda está em andamento. Este processo pode levar até X horas. O administrador da instância receberá uma notificação quando este processo for concluído.	Depois que o provisionamento em uma instância for iniciado para Uma URL personalizada, será preciso aguardar a conclusão do processo antes que o status mude.
<custom_domain> agora está definido como o novo URL da instância. <base.service-now.com> ainda está em serviço, mas todos os novos URLs, como nas notificações, usarão <custom_domain>.	Somente um URL pode ser designado como o URL da instância. Os outros URLs associados à sua instância podem estar ativos, mas somente o URL da instância pode usar notificações.
a URL personalizada <custom_domain> está definido para ser removido imediatamente da configuração da instância e revertido para <base.service-now.com>. <custom_domain> dá continuidade a uma associação a esta instância desde que o registro CNAME esteja definido no seu DNS.	Esta mensagem confirma que você pretende mudar a URL personalizada. Ao aceitar esta confirmação, você inicia a mudança do URL para sua instância. Qualquer URL na sua lista de nomes de domínio, como Uma URL personalizada, pode estar ativo, a menos que você o remova do registro CNAME no seu provedor.
Não é possível modificar glide.servlet.uri. Esta propriedade é definida pelo URL personalizada.	
Não é possível modificar glide.proxy.host. Esta propriedade é definida pelo URL personalizada.	
O registro CNAME para <custom_domain> não aponta para <base.service-now.com>.	A configuração no lado do provedor de URL não está correta. Verifique sua configuração no registro CNAME.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mensagem de erro	Correção
Registro CNAME ausente para <custom_domain>.	O registro CNAME deve ser configurado no seu provedor de URL antes que a URL personalizada possa ser definido para sua instância.

Saídas de instalação

Saídas de instalação são personalizações que saem do Java para chamar um script antes de retornar ao Java.

Nota: A funcionalidade descrita aqui requer a função de **administrador**.

Saídas de instalação disponíveis

Navegue até **Definição do Sistema** > **Saídas de instalação**. Alguns nomes de saída da instalação (Login, Logout, ValidatePassword, ExternalAuthentication) são reservados e não podem ser alterados. Outras saídas de instalação podem substituí-las por um script personalizado que substitui o script na saída de instalação padrão.

As seguintes saídas de instalação estão disponíveis no sistema de base:

Saída de instalação	Descrição
Login	Usa um par de nome de usuário e senha e autentica com o objeto de usuário
Logout	Conduz o usuário à página de boas-vindas ao fazer o logout; pode ser substituído por LogoutRedirect
LogoutRedirect	Leva o usuário a um URL especificado após o logout
ExternalAuthentication	Autentica usando cabeçalho, parâmetro ou cookie; pode ser substituída por DigestSingleSignOn e PGPSingleSignOn
DigestSingleSignOn	Autentica usando cabeçalho, parâmetro ou cookie e descriptografa a codificação Digest
PGPSingleSignOn	Autentica usando cabeçalho, parâmetro ou cookie e descriptografa a codificação PGP
ValidatePassword	Ativa por padrão, começando com a versão Helsinki; permite que os clientes definam sua própria validação de senha; pode ser substituída por ValidatePasswordStronger
ValidatePasswordStronger	A senha deve ter pelo menos 8 caracteres e conter um dígito, uma letra maiúscula e uma letra minúscula.
GetIntegrationSessionTimeout	Implementa o comportamento de tempo limite da sessão de integração padrão.

Modificações de login

A modificação a seguir da saída de instalação de **Login** define o valor de tempo limite de cada sessão do usuário conforme o usuário faz login. Neste exemplo específico, se o nome de usuário for *admin*, a sessão será definida como tempo limite em 30 segundos.

```
gs.include("PrototypeServer");
```

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

```
var Login = Class.create();
Login.prototype = {
 initialize : function() {
 },

        process : function() {
          // the request is passed in as a global
          var userName = request.getParameter("user_name");
          var userPassword = request.getParameter("user_password");

          var authed = GlideUser.authenticate(userName, userPassword);
          if (authed) {
             //
 ********************************************************
             // customization - if the userName == admin, set the session
             // timeout to be 30 seconds. You can implement your own
             // session timeout algorithm here by checking to see if a
 user
             // belongs to a certain group or has a certain role.
             // Values of setMaxInactiveInterval exceeding 1440 minutes
 are
             // treated as one day (1440 minutes).

           if (userName == "admin") {
               request.getSession().setMaxInactiveInterval(30);
             }
             //
 ********************************************************
             return GlideUser.getUser(userName);
          }

          this.loginFailed();

          return "login.failed";
        },

        loginFailed : function() {
          var message = GlideSysMessage.format("login_invalid");
          var gSession = GlideSession.get();
          gSession.addErrorMessage(message);

          var userName = request.getParameter("user_name");
          EventManager.queue("login.failed", "", userName, "");
       }

}
```

O tempo limite da sessão também pode ser definido de acordo com o endereço IP.

```
gs.include("PrototypeServer");

var Login = Class.create();
Login.prototype = {
 initialize : function() {
 },

        process : function() {
```

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

```
         // the request is passed in as a global
         var userName = request.getParameter("user_name");
         var userPassword = request.getParameter("user_password");

         var authed = GlideUser.authenticate(userName, userPassword);
         if (authed) {

         //
*************************************************************
         // customization - if the user is logging in from a particular
IP
         // range starting with XXX.XXX you can implement your own
         // session timeout algorithm here by checking the login IP
         //
         // Values of setMaxInactiveInterval exceeding 1440 minutes are
         // treated as one day (1440 minutes).

         var clientIP = gs.getSession().getClientIP().toString();

         // if client IP starts with specified range
         if (clientIP.indexOf('XXX.XXX') == 0) {
            // set to 10 hours
            request.getSession().setMaxInactiveInterval(60 * 60 * 10);
         }
         //
*************************************************************

            return GlideUser.getUser(userName);
         }

         this.loginFailed();

         return "login.failed";
       },

       loginFailed : function() {
         var message = GlideSysMessage.format("login_invalid");
         var gSession = GlideSession.get();
         gSession.addErrorMessage(message);

         var userName = request.getParameter("user_name");
         EventManager.queue("login.failed", "", userName, "");
      }

}
```

Informações relacionadas

Impor senhas fortes

Autenticação baseada no intervalo de IP

Uma maneira de proteger uma aplicação baseada na Web é restringir o acesso com base no endereço IP.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você pode bloquear o acesso a um endereço específico ou a um intervalo de endereços que você suspeita que pertençam a indivíduos mal-intencionados. A instância permite que você controle o acesso por endereço IP.

Nota: Use a política de contexto de pré-autenticação Autenticação adaptável (AA) para aplicar autenticações e restrições baseadas em IP a recursos adicionais. Para obter mais informações, consulte Autenticação adaptável.

Observações e limitações:

- O sistema não permitirá que você se bloqueie, portanto, se tentar adicionar uma regra de modo que seu endereço atual seja bloqueado, o sistema o avisará e recusará a inserção.
- Se você estiver dentro de uma intranet corporativa, tenha muito cuidado ao configurar suas regras de IP. O endereço IP que você vê no seu próprio computador (como 10.10.10.25) geralmente não tem nenhuma relação com o endereço IP com que você realmente aparecerá na Internet. Sua empresa provavelmente usará proxies e/ou NATs em seu endereço em um conjunto previsível de endereços de saída, sobre os quais você provavelmente precisará consultar sua equipe de rede.
- Um usuário cujo acesso é restrito com base em uma regra de acesso obtém um erro 403 em seu navegador.
- Usuários restritos não usam transações, semáforos ou contagem para qualquer contagem de recursos do servidor.
- Este recurso não substitui suas regras de controle de acesso existentes se, por exemplo, você estiver executando uma VPN em nosso datacenter. É uma verificação adicional que deve ser cumprida, além de quaisquer controles de acesso que possamos ter configurado no seu PIX.
- Permita que regras sempre superem regras de negação Portanto, se um endereço for permitido (por uma regra) e negado (por uma segunda regra), ele será, de fato, permitido.
- Asteriscos e blocos CIDR não são compatíveis no momento.
- Em relação aos endereços de proxy encaminhados, as regras de permissão são aplicadas a cada endereço na cadeia e as regras de negação são aplicadas a cada endereço na cadeia se nenhuma das regras de permissão corresponder.
- A Autenticação baseada no intervalo de IP pode afetar a transferência de conjuntos de atualizações. Se o controle de acesso ao endereço IP estiver habilitado na instância de origem, adicione os endereços IP de todos os nós da aplicação que oferecem suporte à sua instância como exceções.

  Nota: Para encontrar as informações de IP da sua instância, faça login em ServiceNow - NOW Support e pesquise o item do Catálogo de serviços **Informações sobre meu IP**.

Nota: Para aprender mais sobre as propriedades *com.snc.ipauthenticator* e *glide.ip.authenticate.strict*, que restringem o acesso da instância a intervalos de IP específicos, consulte os seguintes tópicos nas Configurações de proteção de segurança da instância:

- Restringir o acesso a intervalos de IP específicos
- Restrição estrita de IP

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Controle de acesso de endereços IP

Aplique um controle de acesso IP ao tráfego de saída, tráfego de entrada ou tráfego bidirecional. O sistema só bloqueará um endereço IP se houver uma regra de negação correspondente e nenhuma regra de permissão correspondente. Por padrão, não há restrições de acesso à sua instância.

Antes de Iniciar

Função necessária: administrador

Nota: Use a política de contexto de pré-autenticação da Autenticação adaptável (AA) para impor autenticações e restrições baseadas em IP para recursos adicionais. Para obter mais informações, consulte Autenticação adaptável.

Procedimento

1. Navegue até **Todos** > **Segurança do sistema** > **Controle de acesso de endereços IP** para ver uma lista de seus controles de acesso IP.
   Pode ser necessário ativar o plug-in Autenticação baseada no intervalo de IP [com.snc.ipauthenticator].
2. Preencha o formulário.

   Nota: Para encontrar as informações de IP da sua instância, faça login em ServiceNow - NOW Support e pesquise o item do Catálogo de serviços **Informações sobre meu IP**.

Campo	Descrição
Tipo	Tipo de regra de controle de acesso a ser incluída. ◦ *Permitir*: qualquer endereço IP neste intervalo pode interagir com esta instância. ◦ *Negar*: qualquer endereço IP neste intervalo não pode interagir com esta instância, a não ser que esteja listado na regra Permitir. Além disso, ao adicionar regras de negação, você não pode negar seu próprio endereço IP público ou sua instância não atualizará uma regra de negação. **Nota:** Para oferecer suporte a manutenção, upgrades e Suporte e atendimento ao cliente, alguns IPs internos da ServiceNow não podem ser bloqueados por regras de negação.
Direção	Direção da regra de controle de acesso IP. ◦ **Entrada**: permite ou nega transações de entrada. Essas são transações iniciadas fora da sua instância. ◦ **Saída**: permite ou nega transações de saída. Essas são transações iniciadas dentro da sua instância. ◦ **Bidirecional**: permite ou nega transações de entrada e saída.
Ativo	Quando selecionado, o formulário está ativo.
Descrição	Descrição do controle de acesso.
Início do intervalo	Intervalo inicial de endereços IP a serem permitidos ou negados.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: Essas regras também afetam a transferência de conjuntos de atualizações. Para garantir que o controle de acesso de endereços IP não cause falha nos conjuntos de atualizações, adicione a instância de destino como uma exceção.
Término do intervalo	Intervalo final de endereços IP a serem permitidos ou negados. **Nota:** Para limitar o acesso somente a endereços VPN específicos, insira um Intervalo de negação de **0.0.0.0** a **255.255.255.255** no campo **Negar** e insira somente os intervalos VPN específicos permitidos.

3. Clique em **Enviar**.

Encontrar endereços IP negados

Encontre endereços IP negados nos arquivos de log do nó da instância

Antes de Iniciar
Função necessária: administrador.

Por Que e Quando Desempenhar Esta Tarefa
As entradas de log para o endereço IP bloqueado aparecem da seguinte forma: `2015-10-21 18:37:43 (175) http-30 WARNING *** WARNING *** Security restricted: Access restricted (xx.xx.xxx.xxx not authorized)`.

Nota: Os endereços IP negados são os arquivos visíveis de log do nó da instância, que não podem ser vistos nos logs do sistema.

Procedimento

1. Navegue até **Todos** > **Logs do sistema** > **Utilitários** > **Navegador de arquivos de log do nó**.
2. Pesquise os logs por critérios, como período de tempo e mensagem.
3. Você também pode baixar arquivos de log quando souber qual log está procurando, navegando até **Logs do sistema** > **Utilitários** > **Download do arquivo de log do nó**.

Integração LDAP

Uma integração LDAP permite que sua instância use seu servidor LDAP existente como origem primária de dados do usuário.

Os administradores se integram a um diretório LDAP (Lightweight Directory Access Protocol) para simplificar o processo de login do usuário e automatizar tarefas administrativas, como a criação de usuários e a atribuição de funções a eles. Uma integração LDAP permite que seu sistema use seu servidor LDAP existente como origem primária de dados do usuário. Normalmente, uma integração LDAP também faz parte de uma implementação Single Sign-on.

A integração usa as credenciais da conta de serviço LDAP para recuperar o nome diferenciado (DN) do usuário do servidor LDAP. Dado o valor de DN do usuário, a integração

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

é religada LDAP com o DN e a senha do usuário. A senha que o usuário insere está contida inteiramente na sessão HTTPS. A integração nunca armazena senhas LDAP.

A integração usa uma conexão somente leitura que nunca grava no diretório LDAP. A integração apenas consulta informações e, em seguida, atualiza seu banco de dados interno conforme necessário.

Nota: Para obter informações detalhadas sobre como configurar a integração, consulte Configuração de integração LDAP.

Nota: Se sua instância estiver usando uma integração LDAP e as configurações do Active Directory exigirem que os usuários redefinam suas senhas após o login, os usuários não poderão fazer login na instância. A instância não pode alterar a senha do Active Directory de nenhum usuário.

Recursos de integração LDAP

Os recursos de integração LDAP incluem o seguinte.

Atualização programada LDAP

Uma verificação programada do servidor LDAP geralmente é executada uma vez por noite. Ela consulta todos os atributos de registros do usuário aplicáveis e os compara com a conta em nossos servidores. Se houver uma diferença, modificaremos nosso registro de usuário com o atributo alterado. A carga imposta ao servidor LDAP durante a atualização depende de quantos registros são consultados e do número de atributos que estão sendo comparados. Recomendamos que atualizações sejam programadas fora dos horários de pico. Operações extensas de atualização podem afetar outras operações programadas, como a execução de relatórios, e devem ser planejadas de modo a minimizar conflitos.

Ouvinte LDAP

O ouvinte LDAP é a nossa versão de uma consulta persistente (ou pesquisa persistente). Emitimos uma consulta permanente para mudanças feitas no servidor LDAP e ouvimos constantemente em busca de uma resposta. Supondo que seu servidor suporte uma pesquisa persistente, todas as alterações feitas em qualquer uma das suas contas LDAP aplicáveis são retornadas ao ouvinte LDAP e enviadas para sua instância em aproximadamente 10 segundos. Esta é uma ferramenta extremamente útil que permite obter uma cópia quase em tempo real dos detalhes da conta de seus usuários, sem a necessidade de esperar pela próxima atualização agendada.

Login LDAP sob demanda

Depois que uma integração LDAP é estabelecida, a instância pode permitir que novos usuários façam login no sistema, mesmo que eles ainda não tenham uma conta. Quando um novo usuário tenta fazer login na instância, a integração verifica se ele tem uma conta. Se não encontrar uma conta de usuário existente, a integração consultará automaticamente o servidor LDAP para obter o nome de usuário inserido. Se uma conta LDAP correspondente for encontrada, a integração tentará autenticar com a senha inserida pelo usuário. Se a senha for válida, a instância criará uma conta para o usuário, preencherá a conta com todas as informações LDAP aplicáveis e fará o login do usuário na instância.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O login sob demanda usa o mapa de transformação de importação de usuário LDAP. Para obter mais informações sobre os requisitos do mapa de transformação, consulte Mapas de transformação LDAP.

Preenchimento de dados LDAP

> **Nota:** A funcionalidade descrita nesta integração não está disponível por padrão. Esta integração envolve personalização pós-implantação realizada por um administrador experiente ou ServiceNow consultores de serviços profissionais.

Uma integração com os servidores LDAP permite que você preencha de forma rápida e fácil o banco de dados da instância com registros de usuário do banco de dados LDAP existente. Para evitar inconsistências de dados, você pode criar, ignorar ou omitir os registros de entrada LDAP.

Você também pode limitar os dados importados pela integração, especificando atributos LDAP para importar somente os dados que deseja expor para uma instância. Normalmente, os atributos LDAP especificados por você se tornam parte do mapa de transformaçãoda integração. Se você não especificar nenhum atributo LDAP, a integração importará todos os atributos de objeto disponíveis do servidor LDAP. A instância armazena dados LDAP importados em tabelas de conjunto para importação temporária. Consequentemente, quanto mais atributos você importar, maior será o tempo de importação. Para obter mais informações, consulte Especificar os atributos LDAP.

Autenticação LDAP

Use a autenticação LDAP para obter acesso usando credenciais LDAP.

Quando um usuário insere credenciais de rede na página de login:

1. A instância passa as credenciais para que um servidor LDAP encontre a instância.
2. Com RDNs, ela valida a cadeia de caracteres DN do usuário. Ela somente fornece validação se pelo menos uma das configurações de OU LDAP com `table = sys_user` tiver um RDN configurado.
3. O servidor LDAP responde com uma mensagem de autorização ou negativa de autorização usada pelo sistema para determinar se o acesso deve ser concedido.

Ao fazer uma autenticação contra o servidor LDAP, os usuários acessam a plataforma com as mesmas credenciais que usam para outros recursos internos em seu domínio de rede. Além disso, é possível reutilizar qualquer senha e política de segurança existentes que já estejam em vigor. Por exemplo, o servidor LDAP pode já ter políticas de expiração de senha e bloqueio de conta.

Ao habilitar o LDAP, o sistema atualiza os registros do usuário com esses campos.

Atualizações do registro de usuário LDAP

Campo	Descrição
Origem	Identifica se o LDAP será ou não usado para validar um usuário. Se a origem iniciar com ldap, o usuário será validado via LDAP. Se a origem não iniciar com ldap, a senha no registro do usuário será usada para validar o usuário no login.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atualizações do registro de usuário LDAP

Campo	Descrição
Servidor LDAP	Identifica qual servidor LDAP autentica o usuário quando vários servidores LDAP estiverem disponíveis.

Nota: O sistema não oferece suporte à autenticação de senha LDAP por meio de um MID Server. Uma instância deve ser capaz de se conectar diretamente a um servidor LDAP para oferecer suporte à autenticação de senha.

Noções básicas sobre integração LDAP

Uma integração LDAP permite que sua instância use seu servidor LDAP existente como origem primária de dados do usuário.

Pré-requisitos de integração LDAP

- O servidor de serviços de diretório deve ser compatível com o LDAP versão 3
- O acesso à rede de entrada por firewall deve ser permitido (para o servidor LDAP)
- IP externo ou nome do servidor LDAP
- Credenciais de usuário com acesso somente leitura
- Para o LDAPS, um certificado PKI

Tempo de integração LDAP

As integrações LDAP geralmente são feitas antes que a instância entre em operação, mas podem feitas a qualquer momento.

Integridade de dados do servidor LDAP

Alguns usuários ficam preocupados com a possibilidade de um terceiro (a instância, nesse caso) fazer mudanças (gravação) no servidor LDAP. Em uma integração LDAP, a instância não grava no diretório LDAP interno. A instância consulta as informações e atualiza o banco de dados da forma adequada.

A instância não faz nenhuma mudança no servidor LDAP interno. A conta de serviço é somente leitura.

A maioria das mudanças, inclusive adições, do servidor LDAP ficam disponíveis para a instância em segundos, dependendo de quantos componentes da integração LDAP completa estão em vigor.

Para manter os registros LDAP sincronizados, programe uma verificação periódica do servidor LDAP para selecionar as mudanças.

A instância não sincroniza registros de departamento. Os usuários e as associações de grupo são mantidos atualizados pelo mecanismo de ouvinte LDAP e por uma navegação LDAP completa diária, mas a instância não exclui nenhuma dessas entradas depois que elas desaparecem do LDAP.

Se uma entrada fosse excluída, todo o histórico também seria excluído e todas as referências a ele seriam limpas ou excluídas. Itens de configuração (ICs), acordos de ANS, licenças de software, ordens de compra e entradas do Catálogo de serviços têm uma

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

referência ao departamento e, se um departamento for excluído, essas referências serão limpas. Há muitas referências a usuários, portanto, a exclusão de um usuário apagaria todo o histórico do que ele fez. Atualmente, a decisão de excluir ou não é dos clientes.

Segurança

A conexão é feita de uma única máquina que usa um endereço IP fixo por uma porta específica do firewall. A autenticação é feita com uma conta LDAP somente leitura de sua escolha. Você pode usar o LDAP padrão ou carregar o lado público de um certificado SSL instalado no diretório. Nesse caso, é possível usar o LDAPS. Para adicionar outra camada de segurança, também oferecemos a opção de um túnel VPN IPSec ponto a ponto. Fale com o gerente de conta para obter detalhes e preços.

Conexões LDAP seguras

Conexão	Descrição
MID Server	Para proteger o servidor LDAP do tráfego de rede externa, instale um MID Server na rede local e configure o sistema para se comunicar com o MID Server por um canal seguro.
LDAPS	Para estabelecer uma conexão LDAPS criptografada, carregue o lado público do certificado SSL do servidor LDAP. A integração usa o certificado para criptografar todas as comunicações entre o servidor LDAP e a instância.
VPN	Para proteger o servidor LDAP com um túnel VPN IPSec ponto a ponto criptografado, fale com o gerente de conta para obter detalhes e preços.

Os dados compartilhados em uma integração LDAP são outro aspecto de segurança. Para limitar os dados expostos à instância, especifique os atributos no mapa de transformação. Para obter mais informações, consulte Mapas de transformação LDAP.

Importação de dados LDAP para a instância

É recomendável que os atributos sejam definidos para importar somente os dados necessários. Os atributos definidos são mapeados para o banco de dados do usuário da instância.

Não podemos responder à pergunta sobre quais atributos específicos são necessários porque isso é determinado pelo escopo do projeto e pelos requisitos de negócio.

Tipos compatíveis de servidores LDAP

A instância foi integrada com sucesso com o Microsoft Active Directory, Novell, Domino (Lotus Notes) e Open LDAP. O JNDI foi usado para fazer a interface com o servidor LDAP. Desde que o servidor LDAP seja compatível com o LDAP versão 3, a integração será bem-sucedida.

Single Sign-on do LDAP

Junto com a funcionalidade de preenchimento de dados da importação LDAP, é possível usar a funcionalidade de autenticação externa compatível com a aplicação para evitar que os usuários precisem fazer logon todas as vezes.

Vários domínios LDAP

O método recomendado para lidar com vários domínios é criar um registro de servidor LDAP separado para cada domínio. Cada registro de servidor LDAP deve apontar para

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

um controlador de domínio desse domínio. Isso significa que a rede local deve permitir conexões com cada controlador de domínio.

Depois de expandir para mais de um domínio de rede, é essencial identificar atributos LDAP exclusivos para os nomes de usuário da aplicação e importar valores de aglutinação. Um atributo de aglutinação exclusivo comum para o Active Directory é objectSid. Nomes de usuário exclusivos podem variar com base no design de dados LDAP. Atributos comuns são `e-mail` ou `userPrincipalName`.

Manipulação de limites de consulta

Por padrão, o Active Directory 2000/2003 tem um limite de consulta LDAP (maxPageSize) de 1000 objetos para evitar cargas excessivas e ataques de negação de serviço. Há dois métodos para manipulação desse limite.

O método padrão é dividir a consulta para retornar menos de 1000 objetos por vez. Por exemplo, consulte somente o objeto que começa com a letra "a" e, em seguida, consulte os objetos que comecem com a letra "b". O método mais eficiente para ambientes grandes é habilitar a paginação. A paginação é compatível por padrão com todos os servidores Microsoft Active Directory. Ela divide automaticamente os resultados em vários conjuntos de resultados, portanto, não é preciso dividir a consulta em várias solicitações.

Tipo de consulta LDAP

Se uma senha LDAP for fornecida, uma "vinculação simples" será executada. Se nenhuma senha LDAP for fornecida, a palavra "nenhuma" será usada e, nesse caso, o servidor LDAP deve permitir login anônimo.

Autenticação LDAP

As credenciais de conta de serviço fornecidas para LDAP são usadas para a recuperação do DN do usuário do servidor LDAP. Com base no valor de DN do usuário, nós nos vinculamos novamente com o LDAP de acordo com o DN do usuário e a senha fornecida.

Armazenamento de senhas

A senha que o usuário insere fica totalmente contida na sessão HTTPS. A senha não fica armazenada em nenhum lugar.

Configuração da autenticação LDAP

Estes campos do registro do usuário pertencem ao LDAP:

- **Origem**: o campo Origem identifica se um usuário é validado ou não pelo LDAP. Se o campo de origem começar com "ldap", o usuário é validado pelo LDAP. Se o campo Origem não começar com "ldap", a senha do registro do usuário é usada para validar o usuário após o login.
- **Servidor LDAP**: a instância é compatível com vários servidores LDAP, portanto, o campo Servidor LDAP determina qual servidor deve ser usado para autenticar o usuário.

Requisitos para integração LDAP

Revise os requisitos para integração LDAP, incluindo um certificado PKI e um servidor de serviços de diretório compatível com LDAP.

A integração LDAP exige:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Um servidor de serviços de diretório compatível com LDAP v3
  - Permite acesso de rede de entrada por meio do firewall (para o servidor LDAP)
  - (Opcional) Aceita login anônimo
  - (Opcional) Oferece suporte à paginação para consultas extensas LDAP
- O endereço IP externo ou nome do domínio totalmente qualificado do servidor LDAP. Também é possível usar um MID Server.
- Uma conta LDAP somente leitura de sua escolha
- Para vários domínios, acesso à rede para cada controlador de domínio
- Para o LDAPS, um certificado PKI
- Para o ouvinte LDAP, um servidor Microsoft Active Directory que oferece suporte a consultas persistentes (ADNotify)

Servidores LDAP compatíveis

Usando o JNDI para estabelecer interface com o servidor LDAP, a instância foi integrada com sucesso com os seguintes servidores:

- Microsoft Active Directory
- Novell
- Domino (Lotus Notes)
- Abrir o LDAP

Limites de consulta LDAP

Por padrão, o Active Directory 2000/2003 tem um limite de consulta LDAP (maxPageSize) de 1.000 objetos para evitar cargas excessivas e ataques de negação de serviço. O sistema conta com dois métodos para lidar com esse limite.

- O método-padrão é dividir a consulta para retornar menos de 1.000 objetos por vez. Por exemplo, consulte apenas os objetos que começam com a letra A e, em seguida, os objetos com a letra B.
- O método mais eficiente para ambientes grandes é habilitar a paginação, que é compatível por padrão em todos os servidores Microsoft Active Directory. A paginação divide automaticamente os resultados em vários conjuntos de resultados para que a integração não precise dividir a consulta em várias solicitações.

Configuração de integração LDAP

Os administradores podem habilitar a integração LDAP para permitir o logon de usuários do diretório LDAP da empresa.

O LDAP normalmente usa um desses tipos de canais de comunicação.

Canais de comunicação LDAP

Conexão	Descrição	Suporte à importação LDAP?	Suporte a autenticação LDAP?
Conexão do MID Server	Por padrão, comunica-se por HTTP na porta 80. Este canal de comunicação não requer um	Sim	Não

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Canais de comunicação LDAP

Conexão	Descrição	Suporte à importação LDAP?	Suporte a autenticação LDAP?
	certificado. A conexão entre o MID Server e a instância é feita por HTTPS (porta 443). É possível usar o MID Server para importar dados pelo LDAP, mas não usar o MID Server para autenticação LDAP. Prossiga para Definir o servidor LDAP.		
Integração LDAP padrão	Por padrão, comunica-se por TCP na porta 389. Este canal de comunicação não requer um certificado. Prossiga para Definir o servidor LDAP.	Sim	Sim
Integração LDAP criptografada por SSL (LDAPS)	Por padrão, comunica-se por TCP na porta 636. Este canal de comunicação requer um certificado. Prossiga para Instalação do certificado SSL LDAP X.509 para obter e carregar o certificado.	Sim	Sim
Conexão VPN	Comunica-se por meio de um túnel IPSEC. Compre ou crie um túnel IPSEC em sua rede local. Prossiga para Definir o servidor LDAP.	Sim	Sim

Se um MID Server estiver sendo usado, ele se conectará à instância. O MID Server também se conectará ao servidor LDAP. Em ambos os casos, o MID Server inicia a conexão:

1. Primeiro, o MID Server se conecta ao servidor LDAP por LDAP na porta 389.
2. Em seguida, o MID Server inicia uma conexão criptografada HTTPS com a instância na porta 443 para fazer o envio por push dos dados para a instância.

Para obter mais informações sobre VPNs, MID Servers e LDAP, consulte Você não precisa de uma VPN Parte II na comunidade.

Instalação do certificado SSL LDAP X.509

É possível instalar um certificado X.509 para sua integração LDAP.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Compre ou gere um certificado SSL no servidor LDAP.
2. Navegue até **LDAP** > **Certificado** e clique em **Novo**.
3. Preencha os campos de formulário:

Campo	Descrição
Nome	O nome do certificado.
Notificação de expiração	Selecione essa opção para enviar uma notificação aos usuários selecionados no campo **Notificar na expiração**. Por padrão, essa opção está ativada.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Notificar no vencimento	Selecione os usuários para reativar a notificação sobre a expiração do certificado. Se nenhum usuário for selecionado, o usuário conectado será adicionado por padrão, juntamente com os dois últimos usuários conectados com a função de administrador.
Aviso emitido antes do vencimento (em dias)	O número de dias antes da expiração em que a instância envia a notificação. Insira um valor de pelo menos 20. As instâncias atualizadas para a versão Istanbul e posteriores têm esse valor definido como 20, a menos que um valor maior seja especificado.
Ativo	Uma caixa de seleção indicando que este certificado está ativo.
Formato	O formato do certificado.
Tipo	O contêiner do certificado. A instância reconhece os certificados dos armazenamentos de confiança, armazenamento de chaves Java e armazenamentos de chave PKCS#12.
Válido de	A instância adiciona a data de início da validade do certificado a esse campo automaticamente. Anexe o certificado ao registro do certificado X.509 para preencher este campo.
Expira	A instância adiciona automaticamente a esse campo a data de expiração do certificado. Anexe o certificado ao registro do certificado X.509 para preencher este campo.
Dias até o vencimento	O número calculado de dias até o vencimento.
Descrição resumida	Uma descrição para o certificado.
Emissor	A instância adiciona o emissor do certificado a esse campo automaticamente. Anexe o certificado ao registro do certificado X.509 para preencher este campo.
Assunto	A instância adiciona automaticamente a esse campo o assunto do certificado. Anexe o certificado ao registro do certificado X.509 para preencher este campo.
Certificado PEM	Insira o valor do certificado X509.

Nota: A integração atualmente não assina o certificado nas comunicações entre a instância e o IdP.

4. Clique em **Salvar**.

O que Fazer Depois

Clique em **Validar armazenamentos/certificados** para testar a confiabilidade do armazenamento e do certificado.

Definição de um servidor LDAP

Crie um novo registro de servidor LDAP na instância.

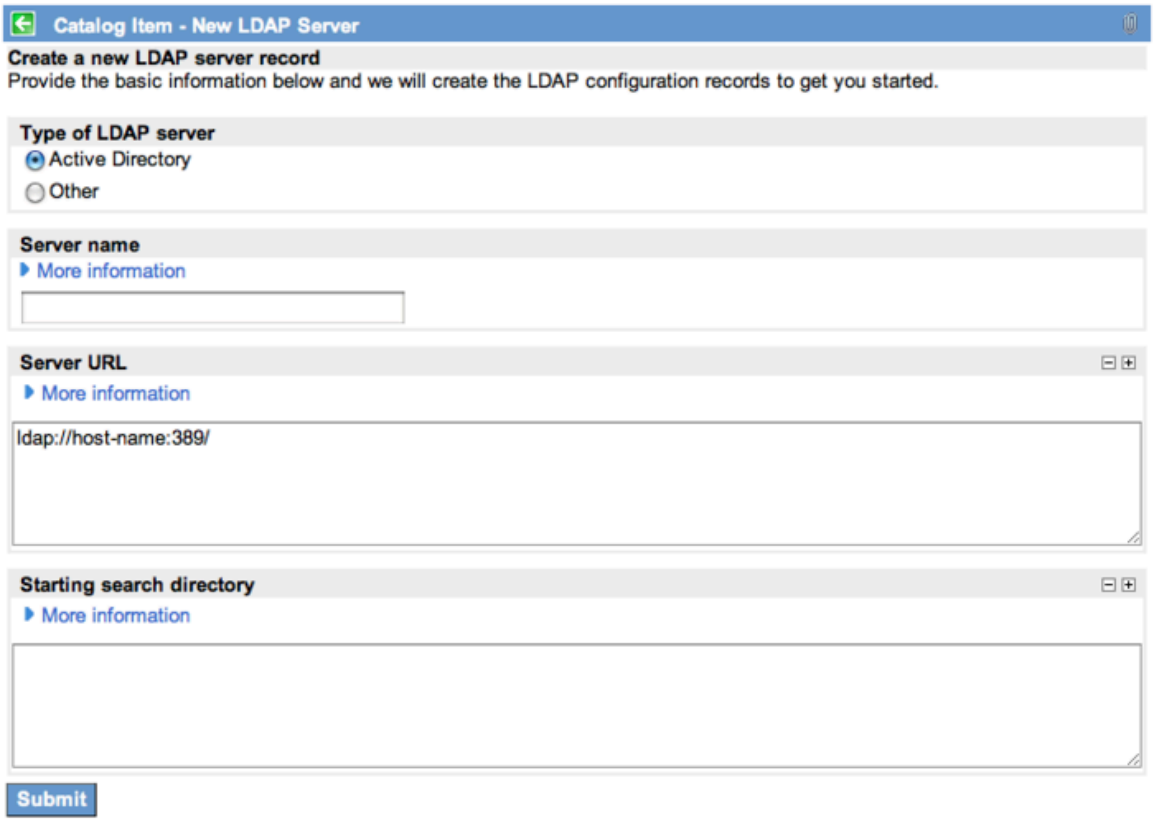
Antes de Iniciar

Função necessária: administrador

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegue até **Todos** > **Sistema LDAP** > **Criar novo servidor**.
2. Preencha os campos de formulário.



No campo **URL do servidor**, os URLs válidos de todos os servidores aparecem separados por um espaço. Os servidores são ordenados primeiro por status operacional, com os servidores listados primeiro como **Funcionais** e, em seguida, ordenados pelo valor de **Ordem** especificado. O primeiro servidor listado é o servidor LDAP primário. Os outros são servidores redundantes.

Nota: Há um pequeno atraso entre a mudança no status operacional e a exibição.

Como alternativa, é possível adicionar um servidor LDAP redundante ao navegar até um registro de servidor LDAP existente e inserir uma linha na lista integrada de URLs do servidor LDAP.

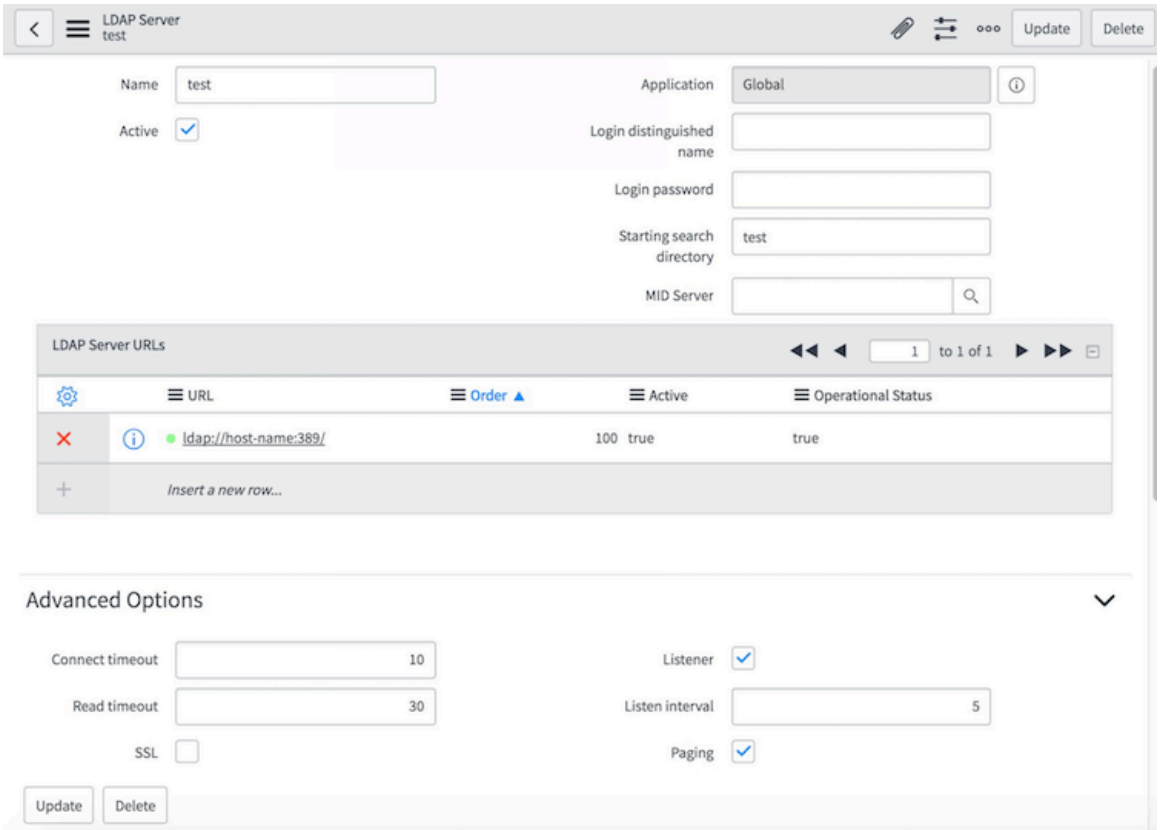
3. Clique em **Enviar**.

Nota: Você também pode modificar um registro de servidor LDAP existente navegando até **Sistema LDAP** > **Servidores LDAP** e fazendo as alterações necessárias.

4. Faça mudanças nos campos conforme necessário.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formulário do servidor LDAP



Campo	Descrição
Nome	Insira o nome do servidor.
Ativo	Marque esta caixa de seleção se o servidor estiver ativo.
URLs do servidor LDAP	Insira os URLs dos servidores LDAP primário e de backup. Os servidores são ordenados primeiro por status operacional, com os servidores listados primeiro como Funcionais e, em seguida, ordenados pelo valor de Ordem especificado. O primeiro servidor listado é o servidor LDAP primário. Os outros são servidores redundantes.
URL do servidor	Insira o URL do servidor. Configure o formulário para adicionar este campo, se necessário. É um campo somente leitura calculado que mostra a lista de servidores LDAP que também é visível no campo **URLs do servidor LDAP**, separados por um espaço e ordenados por status operacional e valores de ordem dos URLs.
Nome distinto de login	Insira o nome diferenciado (DN) do usuário que autentica a conexão LDAP. Para acessar um servidor de diretório LDAP, o nome de usuário deve estar no formato de nome diferenciado completo: `servicenow@service-now.com`
Senha de login	Insira a senha do servidor.
Diretório de	Insira o nome diferenciado relativo (RDN) do diretório de pesquisa padrão. Todas as consultas para este servidor LDAP serão iniciadas a partir deste RDN.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
pesquisa inicial	
MID Server	Selecione o MID Server que você deseja usar para se conectar ao servidor LDAP. Usar um MID Server para estabelecer uma conexão LDAP evita a necessidade de expor o servidor LDAP ao tráfego de rede externa. Ele também elimina a necessidade de estabelecer um túnel VPN entre o servidor LDAP e os datacenters ServiceNow. **Nota:** ◦ O usuário do MID Server deve ter a função user_admin para poder ler registros de configuração do servidor LDAP. ◦ Os itens a seguir não estão disponíveis com o MID Server: ▪ Autenticação LDAP ▪ Conexão SSL
Tempo limite de conexão	Se um MID Server estiver configurado, a conexão expirará após 10 segundos independentemente desta configuração. Esta configuração é codificada e não pode ser alterada.
Tempo limite de leitura	Especifique o número de segundos que a integração terá disponíveis para ler dados LDAP. A integração para de ler dados LDAP depois que a conexão excede o tempo limite de leitura. Ao habilitar uma conexão SSL, também é possível definir um valor de tempo limite de leitura com a propriedade do sistema *com.glide.ssl.read.timeout*. Se valores de tempo limite forem inseridos para este campo e a propriedade do sistema, o menor valor de tempo limite terá precedência.
SSL	Marque esta caixa de seleção para exigir que o servidor LDAP faça uma conexão criptografada por SSL. Este campo não estará disponível se um MID Server for selecionado. Se uma integração LDAPS e a porta SSL padrão for 636 forem usadas, nenhuma configuração adicional será necessária; o SSL será habilitado automaticamente. Se a integração LDAPS usar outra porta SSL, defina as propriedades de conexão SSL alternativas. **Nota:** Certifique-se de que um administrador de rede configure o firewall local para permitir que o servidor de aplicações acesse o servidor LDAP. Se o servidor LDAP estiver localizado em uma rede interna, o firewall encaminhará (ou NATs) o endereço IP do servidor de aplicações por meio do firewall na porta correta.
Ouvinte	Marque esta caixa de seleção para habilitar a integração para pesquisar periodicamente Microsoft servidores do Active Directory ou servidores LDAP que oferecem suporte ao controle de solicitação de pesquisa persistente. Além disso, se um MID Server for selecionado, a funcionalidade de ouvinte estará disponível para ele. Para obter mais informações, consulte Habilitação de um ouvinte LDAP e definição de propriedades do sistema.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Intervalo de escuta (valor de tempo limite)	Especifique o valor de tempo limite do ouvinte no número de minutos em que a integração escuta os dados LDAP com cada conexão. A integração para de escutar dados LDAP depois que a conexão excede o intervalo de escuta.
Paginação	Marque esta caixa de seleção para que o servidor LDAP divida os dados de atributo LDAP em vários conjuntos de resultados em vez de enviar várias consultas.

Nota: Se uma senha LDAP for fornecida, a integração executará uma operação de vinculação simples. Se uma senha LDAP não for fornecida, o servidor LDAP deverá permitir login anônimo ou a integração não poderá ser vinculada ao servidor LDAP.

Resultados
Quando um registro de servidor LDAP é definido como ativo, o sistema testa automaticamente todas as conexões para validá-las.
As validações incluem:

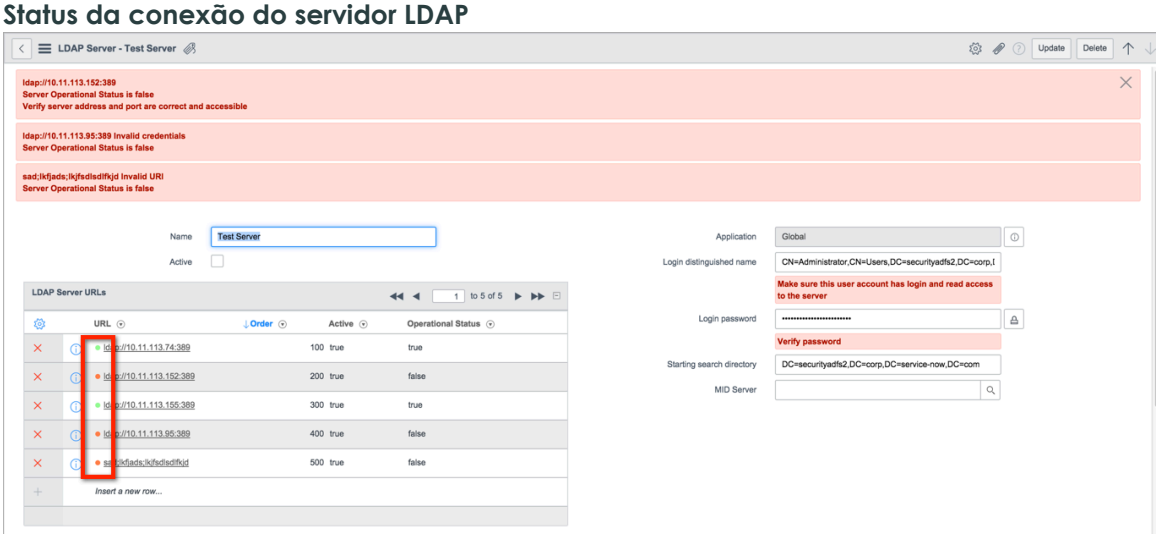
- O servidor LDAP está acessível no URL e na porta fornecida
- O URL do servidor LDAP está formatado corretamente
- As credenciais de login são válidas

A partir da versão Fuji, o sistema exibe pontos coloridos ao lado de cada URL do servidor:

Ícones de conexão do servidor LDAP

Cor	Descrição
Verde	O servidor está ativo e operacional.
Cinza	O servidor não está ativo nem operacional.
Vermelho	O servidor está ativo, mas não operacional.

Status da conexão do servidor LDAP



© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Habilitação de um ouvinte LDAP e definição de propriedades do sistema

Habilitar um ouvinte é opcional. Se habilitado, um ouvinte notificará o sistema para processar registros LDAP assim que houver um upgrade no servidor LDAP.

Antes de Iniciar

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

Um ouvinte é um processo dedicado que busca periodicamente por mudanças no servidor LDAP.

O ouvinte pode ser implantado em um servidor do Microsoft Active Directory que ofereça suporte a consultas persistentes (DNAotify) ou em um servidor LDAP que ofereça suporte ao controle de solicitação de pesquisa persistente (com OID 2.16.840.1.113730.3.4.3).

Se o servidor LDAP oferecer suporte a uma pesquisa persistente, o ouvinte LDAP reconhecerá todas as mudanças de usuário e grupo feitas em qualquer uma das contas LDAP aplicáveis e as encaminhará para sua instância em aproximadamente 10 segundos. Isso permite que a instância tenha uma cópia quase em tempo real dos detalhes da conta dos usuários sem a necessidade de aguardar a próxima atualização programada. O ouvinte LDAP somente pode sincronizar objetos que são mapeados para as tabelas de usuários [sys_users] e grupos [sys_user_group].

Nota: Se um usuário for adicionado por meio do ouvinte, mas não atender aos requisitos definidos pelo filtro da OU, a instância ignorará o registro no servidor LDAP. Se atender aos critérios, o usuário será adicionado à instância.

Para habilitar um ouvinte:

Procedimento

1. Navegue até **Todos** > **Sistema LDAP** > **Servidores LDAP**.
2. Selecione o servidor LDAP a ser configurado.
3. Marque a caixa de seleção **Ouvinte**.
4. Clique em **Atualizar**.

Nota:

O sistema somente importa registros de usuário correspondentes ao filtro OU LDAP. Registros de entrada de usuários que não atendem aos requisitos de filtro são sinalizados como inválidos e ignorados pela importação. Os administradores podem habilitar o registro em log detalhado LDAP para determinar se os registros de entrada não correspondem ao filtro OU LDAP.

5. Opcional: Navegue até a tabela Propriedades do sistema [sys_properties] e defina as propriedades do sistema do ouvinte LDAP.

Propriedades do ouvinte LDAP

Propriedade	Descrição
glide.ldap.listener.use_background_transaction	Quando verdadeiro, o ouvinte LDAP é iniciado com transação em segundo plano. Ao executar o ouvint como uma transação em segundo plano, a transaç Interromper o ouvinte LDAP da regra de cota pode a transação depois que a duração máxima for atin

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países. Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Propriedade	Descrição
	padrão, 5 minutos). Este comportamento evita que LDAP aguarde indefinidamente. **Nota:** Esta propriedade se aplica somente a conexões LDAP que não usam um MID Server. U *glide.ldap.listener.mid.use_background* para controlar o comportamento das conexões passam por um MID Server. ◦ Tipo: verdadeiro | falso ◦ Valor padrão: falso ◦ Local: adicionar à tabela [sys_properties] de prop sistema
glide.ldap.listener.mid.use_background_transaction	Quando verdadeiro, o ouvinte LDAP é iniciado com transação em segundo plano. Ao executar o ouvint como uma transação em segundo plano, a transaç Interromper o ouvinte LDAP da regra de cota pode transação de MID depois que a duração máxima é padrão, 5 minutos). Este comportamento evita que LDAP aguarde indefinidamente. **Nota:** Esta propriedade se aplica somente a conexões LDAP que usam um MID Server. Use *glide.ldap.listener.use_background_tra* para controlar o comportamento das conexões não passam por um MID Server. ◦ Tipo: verdadeiro | falso ◦ Valor padrão: falso ◦ Local: adicionar à tabela [sys_properties] de prop sistema
glide.ldap.listener.mid.one_listener	Quando verdadeiro, apenas uma única mensagem ECC é criada para iniciar ou interromper o ouvinte L de um MID Server. Quando falso, várias mensagens podem ser criadas, levando à criação de vários thre iniciar ou interromper o ouvinte LDAP. ◦ Tipo: verdadeiro | falso ◦ Valor padrão: verdadeiro ◦ Local: adicionar à tabela [sys_properties] de prop sistema

Especificar os atributos LDAP

Especifique os atributos incluídos nas consultas do servidor LDAP usando o campo **Atributos** do servidor LDAP. Isso pode melhorar o desempenho e a segurança.

Antes de Iniciar
Função necessária: administrador

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

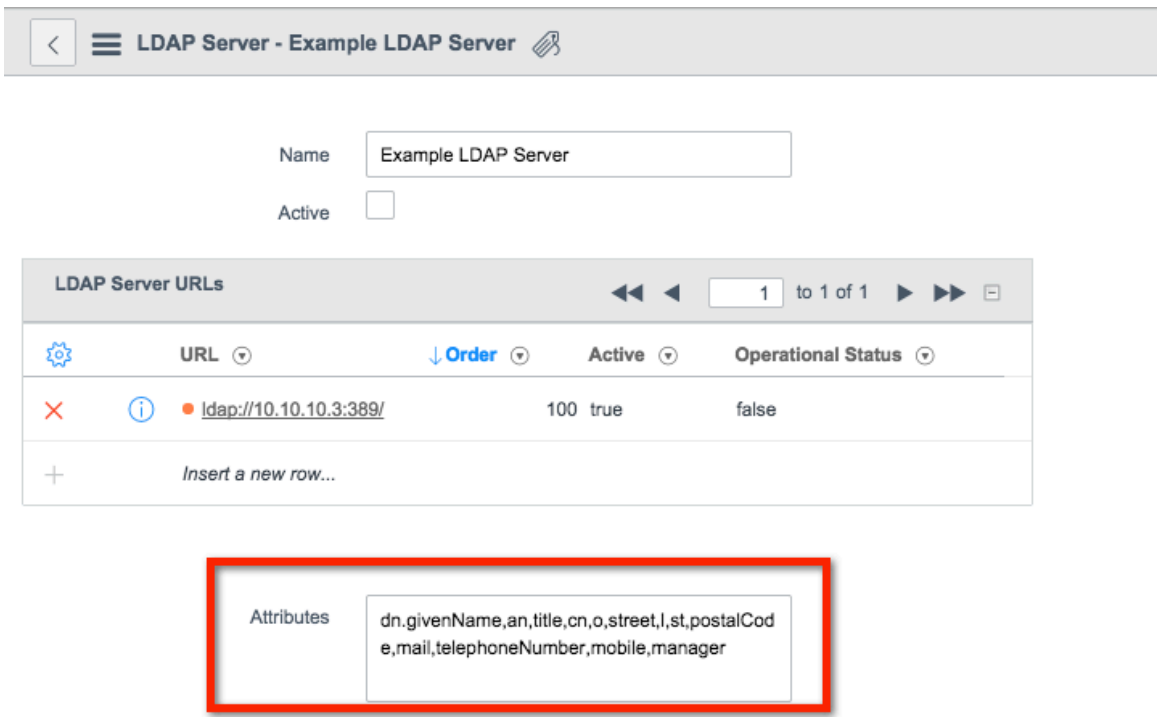
Por padrão, o sistema carrega todos os atributos de cada objeto que tem permissão para ler do servidor LDAP. Usando o campo **Atributos**, é possível especificar e limitar os atributos retornados pela consulta LDAP. Usar essa abordagem para grandes importações de LDAP pode melhorar muito a velocidade dessas importações.

Procedimento

Defina explicitamente os atributos onde for possível.

Se houver informações que você não deseja expor à instância, exclua o atributo. Se os atributos do servidor LDAP não forem especificados, as transações do usuário poderão congelar por longos períodos quando novos atributos forem adicionados a um objeto do servidor LDAP porque o sistema estará ocupado carregando dados dos novos atributos.

Nota: Para usar os scripts de pesquisa de gerente descritos em Selecionar ou Criar um mapa de transformação para dados LDAP, especifique o **gerente** e o **DN** (nome diferenciado) no campo **Atributos**. Nenhum dos atributos precisa fazer parte de um mapa de transformações.



Teste de uma conexão LDAP

A instância testa a conexão automaticamente toda vez que um usuário abre o formulário do servidor LDAP. Como alternativa, é possível testar manualmente a conexão com o servidor LDAP a partir do formulário do servidor LDAP.

Antes de Iniciar

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

Por padrão, mensagens de erro serão exibidas no formulário do servidor LDAP se houver problemas na conexão com o servidor LDAP.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Os funcionários também podem verificar a conectividade entre a instância e o servidor LDAP. Entre em contato com o suporte técnico para obter assistência na verificação da conectividade com o LDAP.

Para testar manualmente uma conexão:

Procedimento

1. Navegue até **Todos** > **Sistema LDAP** > **Servidores LDAP**.
2. Selecione o servidor LDAP a ser testado.
3. Em **Links relacionados**, clique em **Testar conexão**.
4. Em **Links relacionados**, clique em **Procurar** para verificar se a estrutura de diretórios LDAP apropriada está visível para o sistema.
5. Opcional: Se a conexão tiver sido bem-sucedida, clique em **Procurar** para exibir a estrutura de diretórios LDAP de origem visível para a instância.

   Nota: Os campos **Filtro** e **RDN** à esquerda da janela Procurar são ignorados quando você usa o campo de pesquisa à direita.

Resultados

A instância muda o status operacional dos servidores LDAP dependendo do resultado do teste de conexão.

- Se sua instância estabelecer uma conexão com um servidor que tenha um valor de **Status operacionalinativo**, o valor do **Status operacional** será alterado automaticamente para **ativo**. Esta funcionalidade é compatível com testes de conexão automáticos e manuais.
- Se uma conexão não puder ser estabelecida com um servidor que tenha um valor de **Status operacional funcional**, o valor do **Status operacional** será alterado automaticamente para I**inoperante**. Esta funcionalidade é compatível apenas com testes de conexão automáticos, não com testes manuais.

Definição de unidades organizacionais LDAP

Uma definição de unidade organizacional (OU) especifica os diretórios de origem LDAP disponíveis para a integração.

Antes de Iniciar

Função necessária: administrador.

Por Que e Quando Desempenhar Esta Tarefa

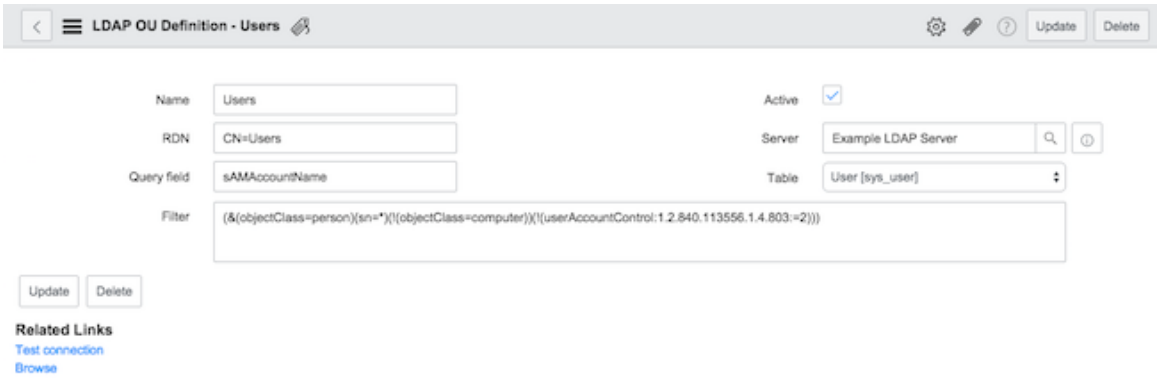
As definições da OU podem conter locais, pessoas ou grupos de usuários. Cada definição de servidor LDAP contém duas definições de OU de amostra: uma para importar grupos para o sistema e outra para usuários.

Procedimento

1. Navegue até **Todos** > **Sistema LDAP** > **Servidores LDAP**.
2. Selecione o servidor LDAP a ser configurado.
3. Na lista relacionada **Definições de OU LDAP**, selecione a definição da OU de exemplo de **Grupos** ou **Usuários**.
4. Preencha o formulário de definição de OU do LDAP (consulte a tabela).
5. Clique em **Atualizar**.
   O sistema testa a conexão com o servidor LDAP automaticamente.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

6. Em **Links relacionados**, clique em **Procurar** para exibir os registros do diretório LDAP retornados pela definição da OU.



Formulário de definição do OU

Campo	Descrição
Nome	Especifique o nome que a integração usa quando referencia este OU. O nome inserido aqui se torna um destino LDAP no registro da fonte de dados.
RDN	Especifique o nome distinto relativo do subdiretório que você deseja pesquisar. Este RDN é combinado com o diretório de início de pesquisa da definição do servidor LDAP para identificar o subdiretório que contém informações para esta unidade organizacional. Por exemplo, a definição de OU de exemplo usa o valor de RDN de `CN=Users` para pesquisar o diretório LDAP `CN=Users,DC=service-now,DC=com` e qualquer diretório abaixo deste ponto. Este campo deve corresponder a um subdiretório no seu sistema LDAP.
Campo de consulta	Especifique o nome do atributo no servidor LDAP para consultar os registros. O campo de consulta deve ser exclusivo tanto em instâncias de domínio único como de vários domínios. Para obter melhores resultados, use endereços de e-mail ou outras credenciais que identifiquem exclusivamente o usuário em uma instância de vários domínios. O Active Directory usa o atributo **sAMAccountName**. Outros servidores LDAP tendem a usar o atributo **cn**. **Nota:** O **campo de Consulta** deve ser mapeado para o campo **ID do usuário** na tabela Usuário [sys_user]. Por exemplo, se um usuário do Active Directory fizer login como `joe.example`, deverá haver um registro de usuário com um valor de **ID de usuário** de **joe.example** e um registro LDAP com um valor **sAMAccountName** de **joe.example**.
Ativo	Marque esta caixa de seleção para ativar a definição da OU e permitir que os administradores testem a importação de dados. No entanto, a integração só pode trazer dados para o sistema de definições de OU ativas.
Tabela	Especifique a tabela que recebe os dados mapeados do servidor LDAP. Para usuários, selecione **Usuário (sys_user)**e, para grupos, selecione **Grupo (sys_group)**.
Filtro	Insira uma cadeia de caracteres de filtro LDAP para selecionar registros específicos para importar da OU. Quanto mais específica for a consulta do filtro LDAP, mais eficiente será a consulta. Por exemplo, a definição de OU do LDAP de usuários usa o seguinte filtro para selecionar registros que são classificados como uma pessoa, têm um valor de atributo **sn**, não são computadores e não estão sinalizados como inativos:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	`(&(objectClass=person)(sn=*)(!(objectClass=computer)) (!(userAccountControl:1.2.840.113556.1.4.803:=2)))` Você pode encontrar uma descrição da sintaxe do filtro LDAP pesquisando a `RFC de filtros LDAP`na Internet.

Example: Exemplos de definições de unidades organizacionais

Suponha que você tenha um servidor LDAP com a seguinte estrutura de diretórios:

dc=my-domain,dc=com

- ou=Grupos
  - cn=Desenvolvimento
  - cn=RH
  - cn=Vendas
- ou=Usuários
  - ou=Desenvolvimento
  - ou=RH
  - ou=Vendas

Suponha ainda que você queira excluir o grupo de RH e os usuários de RH da aplicação. Faça o seguinte:

1. Crie um registro de servidor LDAP com um diretório de pesquisa inicial de dc=my-domain,dc=com.
2. Crie um registro de definição de OU para ou=Grupos com um filtro para excluir cn=RH.
3. Crie um registro de definição de OU para ou=Usuários com um filtro para excluir ou=RH.

Se atributos ou filtros adicionais com uma definição de OU não forem especificados, a consulta LDAP retornará a subárvore completa do diretório inicial e do RDN.

Nesses exemplos, uma definição de OU com o valor de RDN de ou=Grupos e nenhum filtro retornaria todos os grupos. Da mesma forma, uma definição de OU com o valor de RDN de ou=Usuários e nenhum filtro retornaria todos os usuários e unidades organizacionais secundárias.

Criação de uma origem de dados para o LDAP

Cada definição de unidade organizacional (OU) LDAP tem sua própria lista relacionada de fontes de dados.

Antes de Iniciar

Função necessária: administrador

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

Nota: O **Servidor LDAP** e a **Definição de OU LDAP** devem estar ativos para que a ação de carregamento do teste funcione corretamente. Quando a carga de teste é ativada pela primeira vez, o sistema obtém amostras de até 20 registros para determinar o tamanho dos campos do conjunto para importação. Se os registros de amostra não contiverem valores para o campo **ID do usuário**, o sistema definirá o tamanho do campo para todas as importações subsequentes com o tamanho-padrão de 40. A importação trunca todos os dados importados que excedem o tamanho do campo da tabela de conjunto para importação. Além disso, o campo **ID do usuário** é truncado para um máximo de 40 caracteres. Esteja ciente de que os 20 registros carregados não podem ser transformados e são destinados somente para teste. Se os registros de teste contiverem valores para o campo **ID do usuário**, o tamanho do campo será definido com base no tamanho do campo da ID de usuário mais longo nos registros de teste.

Para criar uma nova origem de dados:

Procedimento

1. Navegue até **Todos** > **Sistema LDAP** > **Servidores LDAP**.
2. Selecione o servidor LDAP a ser configurado.
3. Na lista relacionada **Definições de OU LDAP**, selecione um item como **Grupos** ou **Usuários**.
4. Na lista relacionada de **Fontes de dados**, clique em **Novo**.
5. Preencha o formulário Fonte de dados (consulte a tabela).
6. Clique em **Enviar**.
7. Em **Links relacionados**, clique em **Testar carregamento de 20 registros** para testar se a origem de dados pode trazer dados LDAP para a tabela de importação.

Formulário de Fontes de dados

Campo	Descrição
Nome	Especifique o nome usado pela integração ao fazer referência a esta origem de dados.
Nome da tabela de conjunto para importação	Insira o nome da tabela de preparação em que o sistema temporariamente aloca os registros e atributos LDAP importados. Revise esta tabela para exibir registros LDAP importados. É possível usar o mesmo nome da tabela de conjunto para importação para todas as fontes de dados LDAP.
Tipo	Selecione **LDAP** para indicar que os dados importados são dados LDAP. Depois de selecionar o tipo **LDAP**, o formulário exibe o campo **Destino LDAP**.
Destino LDAP	Selecione a definição de OU LDAP associada a esta origem de dados.

Provisionamento automático de usuários LDAP

É possível provisionar usuários automaticamente que estão no servidor LDAP, mas ainda não estão em sua instância.

Antes de Iniciar

Função necessária: administrador

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

Crie as seguintes propriedades na tabela Propriedades do sistema [sys_properties]:

Propriedades LDAP

Propriedade LDAP	Descrição
glide.ldap.authentication	Habilita a autenticação LDAP usando o LDAP para autenticar usuários. Defina esta propriedade como **verdadeira** (o valor padrão).
glide.ldap.user.autoprovision	Permite que o sistema LDAP crie usuários na tabela Usuário [sys_user] automaticamente quando o usuário existir LDAP, mas ainda não estiver na instância. Defina esta propriedade como **verdadeira** (o valo-padrão).

Ambas as propriedades devem ser definidas como **verdadeiras** para que o provisionamento automático funcione.

Integração LDAP via MID Server

Os administradores podem fazer integrações usando uma origem de dados LDAP em um servidor de gestão, instrumentação e descoberta (MID).

O MID Server permite a comunicação e a movimentação de dados entre Now Platform e aplicações, fontes de dados e serviços externos. Para obter detalhes sobre como instalar um MID Server, consulte Instalação de MID Server.

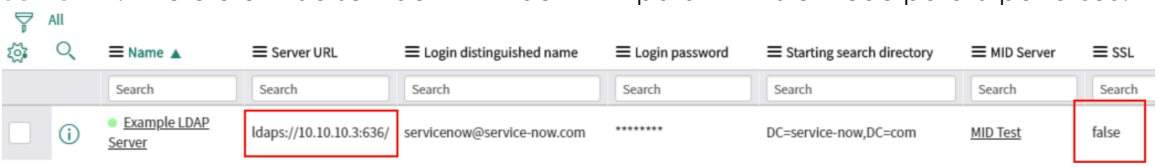
Usar um MID Server para estabelecer uma conexão LDAP evita a necessidade de expor o servidor LDAP ao tráfego de rede externa. Isso elimina a necessidade de estabelecer um túnel VPN entre o servidor LDAP e os datacenters. O usuário do MID Server deve ter a função user_admin para ler registros de configuração do servidor LDAP.

Nota: O MID Server não permite o uso da ação de IU `<instance>/sys_ui_action.do?sys_id=1b4f7ef30a0001060058e223c9a5744c` para atualizar registros de usuários e grupos LDAP.

Por padrão, uma conexão do MID Server se comunica por HTTP na porta 80. Este canal de comunicação não requer um certificado. A conexão entre o MID Server e a instância é feita por HTTPS (porta 443). A instância se conecta ao servidor LDAP diretamente usando LDAP ou LDAPS. Esta conexão pode ser estabelecida pela Internet ou por meio de um túnel VPN.

Nota: O LDAP não pode se comunicar por meio do MID Server com autenticação de senha.

Para uma comunicação segura por SSL, você deve adicionar um certificado SSL para o MID Server. Altere o URL do servidor LDAP de LDAP para LDAPS e mude para a porta 636.



Nota: Se um novo servidor LDAP for criado, o sinalizador SSL do MID Server será definido como falso por padrão. É possível ignorar este comportamento.

Para definir propriedades de conexão para um servidor LDAP específico, consulte Definição de um servidor LDAP.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configuração do monitoramento de conexão LDAP

Altere ou desabilite o monitoramento e as notificações da conexão LDAP.

Antes de Iniciar
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa
A instância envia um e-mail automaticamente para usuários configurados no grupo Administradores LDAP quando uma conexão de servidor LDAP falha. Ela usa a notificação de por e-mail, que é iniciada pelo trabalho agendado **Teste de conexão LDAP**. Esta notificação por e-mail está habilitada por padrão.

Nota: A instância não envia a notificação por e-mail a menos que haja pelo menos um membro no grupo Administradores LDAP. Certifique-se de preencher este grupo com os usuários para os quais deseja que o e-mail seja enviado.

Por padrão, o trabalho agendado testa a conexão a cada 15 minutos. Para mudar esse intervalo ou desabilitar o monitoramento:

Procedimento

1. Navegue até **Todos** > **Definição do sistema** > **Trabalhos agendados**.
2. Abra **o Teste de conexão LDAP**.
3. Faça um dos seguintes:
   - Altere o intervalo no campo **Intervalo de repetição**.
   - Desabilite o monitoramento desmarcando a caixa de seleção **Ativo**.

Importação de dados binários por meio de um MID Server

Como administrador, é possível importar dados de objeto binário grande (BLOB) com uma integração LDAP por meio do MID Server.

Antes de Iniciar
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

Procedimento

1. Adicione o nome da coluna LDAP da qual você deseja importar dados binários para a propriedade do sistema `glide.ldap.binary_attributes`.
2. Adicione uma propriedade de MID Server com o nome `glide.ldap.binary_attributes` e o mesmo valor definido para a propriedade do sistema.

Solução de problemas de integração LDAP via MID Server

É possível encontrar problemas nas áreas a seguir ao integrar o LDAP por meio de MID Server.

É possível solucionar esses problemas exibindo as saídas encontradas na fila do canal de comunicação externa (ECC) (**Saída** > **da Descoberta** > **e Fila do ECC de artefatos**).

Problemas de teste de conexão

Ao definir OUs no servidor, uma lista relacionada de **teste de conexão** é usada para verificar a conexão LDAP. Ao clicar neste link, a fila do ECC deve mostrar uma única mensagem

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

de saída com um nome de tópico de **LDAPConnectionTesterProbe**. Após a conclusão do teste no MID Server, a fila do ECC deve mostrar uma mensagem de entrada com o mesmo nome de tópico. Se a coluna **Nome** da mensagem de entrada for **verdadeira**, o teste terá sido bem-sucedido. Detalhe o registro para exibir a carga e garantir que ele não contenha mensagens de erro.

Testar conexão

Created	Agent	Topic	Name	Source	Queue	State	Processed
2013-07-29 13:24:17	mid.server.local_mid	LDAPConnectionTesterProbe	true	04a952038f21010036bf21ca47e79a30	input	processed	2013-07-29 13:24:19
2013-07-29 13:24:04	mid.server.local_mid	LDAPConnectionTesterProbe		04a952038f21010036bf21ca47e79a30	output	processed	2013-07-29 13:24:17

Procura de problemas

Ao definir OUs no servidor, uma lista relacionada de **Pesquisa** é usada para exibir os registros do diretório LDAP retornados pela definição da OU. Ao clicar neste link, a fila do ECC deve mostrar uma única mensagem de saída com um nome de tópico de **LDAPBrowseProbe**. Depois que os dados forem retornados do MID Server, a fila do ECC deve mostrar uma mensagem de entrada com o mesmo nome de tópico. Se a coluna **Nome** da mensagem de entrada for **verdadeira**, o teste terá sido bem-sucedido. Detalhe o registro para exibir a carga e garantir que ele não contenha mensagens de erro.

Problemas de importação de carga

Ao carregar dados (por exemplo, usando o recurso Testar carregamento de 20 registros), a fila do ECC deve mostrar uma única mensagem de saída com um nome de tópico **LDAPProbe**.

Depois que os dados forem retornados do MID Server, a fila do ECC deve mostrar outra mensagem de entrada chamada **LDAPProbeCompleted**. A coluna **Nome** desta mensagem de entrada mostra o número total de registros retornados.

Uma mensagem de entrada adicional, também chamada **LDAPProbe**, é exibida. A coluna **Nome** desta mensagem de entrada exibe o número de registro mais alto no lote. Se o número total de registros retornados for 258 e o tamanho do lote for 200 (o padrão), duas mensagens de entrada LDAPProbe (200, 258) serão recebidas, e uma mensagem de entrada LDAPProbeCompleted (258) será recebida.

Detalhe o registro para exibir a carga e garantir que ele não contenha mensagens de erro.

Importação de carga

Created	Agent	Topic	Name	Source	Queue	State	Processed
2013-07-29 13:09:48	mid.server.local_mid	LDAPProbeCompleted	11	ed0a0d7a8f32010036bf21ca47e79a56	input	processed	2013-07-29 13:09:51
2013-07-29 13:09:48	LDAPProbeResult	LDAPProbe	11	ed0a0d7a8f32010036bf21ca47e79a56	input	processed	2013-07-29 13:09:51
2013-07-29 13:09:36	mid.server.local_mid	LDAPProbe		ed0a0d7a8f32010036bf21ca47e79a56	output	processed	2013-07-29 13:09:46

Além disso, fique atento a uma mensagem de saída chamada **LDAPProbeError**.

Mensagem de erro

All > Created on Today > Topic = LDAPProbeError

Created	Agent	Topic	Source	Queue	State	Processed	Error string
2014-02-20 14:52:55	mid.server.localdublinmid	LDAPProbeError	MID Server reported error: java.lang.Exc...	output	error	2014-02-20 14:53:02	No message handler for this message.

Clique no link na coluna **Nome** para exibir os detalhes do erro.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Paginação LDAP

A paginação LDAP não funcionará se o tamanho da paginação no servidor LDAP for inferior a 1000. Defina a propriedade do MID Server *glide.ldap.max_results* com um valor menor ou igual ao tamanho da paginação do servidor LDAP.

Falha LDAP ao importar dados binários

Para importar dados binários via LDAP, como uma foto do usuário, é preciso incluir o atributo binário na propriedade do MID Server *glide.ldap.binary_attributes*. No caso do exemplo da foto do usuário, o atributo pode ser `jpegphoto`.

Importação e mapeamento de dados

Os mapas de importação LDAP correspondem aos campos do banco de dados LDAP e aos campos da sua instância.

Nota: O mapeamento LDAP tem efeito sobre o desempenho, portanto a abordagem recomendada é programá-lo fora do horário de pico ou processar apenas alguns registros por vez para manter a disponibilidade do sistema.

Defina um mapa de transformação que importe somente os atributos necessários. Dependendo da versão da instância usada, o método para especificar relacionamentos de mapeamento LDAP pode variar.

A maneira mais fácil de saber se você está executando uma versão que usa a aplicação LDAP do sistema para integração LDAP é localizar a aplicação no navegador de aplicações.

A opção **Executar regras de negócios** é aplicada somente à tabela de destino. Somente mapas de transformação associados à tabela de destino executam as regras de negócios associadas a tabelas diferentes. Se um grupo de usuários contendo regras de negócios em execução em uma tabela de grupo de usuários estiver sendo atualizado, o grupo deverá ter funções definidas.

Opções de mapeamento de importação LDAP

Aplicação LDAP do sistema?	Mapa
Sim	Use um mapa de transformação para especificar seu mapeamento.
Não	Use um mapa de importação legado LDAP para especificar seu mapeamento ou a transformação LDAP padrão inclusa nas instâncias de linha de base. Lembre-se de ajustar o campo **Aglutinar** para corresponder aos campos corretos.

Importações programadas

Uma importação programada permite que os administradores importem dados LDAP em uma programação regular. Por padrão, a integração LDAP inclui duas importações programadas como exemplo:

- Exemplo de importação de usuário LDAP
- Exemplo de importação de grupo LDAP

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nenhum exemplo está ativo por padrão. Altere essas importações programadas para atender às necessidades de negócios da sua empresa.

Mapas de transformação LDAP

O mapa de transformação move dados da tabela de conjunto para importação para a tabela de destino (Usuário ou Grupo).

A integração LDAP usa conjuntos para importação padrão e mapas de transformação. Também é possível criar mapas de transformação LDAP personalizados.

Importante: Ao selecionar ou criar mapas de transformação LDAP personalizados, deve haver um mapa de transformação ativo para um conjunto de tabelas de origem e de destino. Habilitar vários mapas de transformação para as mesmas tabelas de origem e de destino pode produzir entradas duplicadas na tabela de destino, a menos que os campos correspondentes sejam aglutinados.

Mapas de transformação LDAP padrão

Por padrão, o sistema fornece dois mapas de transformação para dados LDAP.

Mapas de transformação LDAP padrão

Mapa de transformações	Tabela de fonte	Tabela de destino	Descrição
Importação de usuário LDAP	[ldap_import]	[sys_user]	Mapa de transformação padrão para criar registros de usuário a partir de credenciais LDAP como parte do login LDAP sob demanda. Contém mapeamentos para um servidor LDAP do Active Directory.
Importação de grupo LDAP	[ldap_group_import]	[sys_user_group]	Mapa de transformação padrão para criar registros de grupo de OUs LDAP. Contém mapeamentos para um servidor LDAP do Active Directory.

Nota: Por padrão, o sistema não tem um mapa de transformação para registros de departamento LDAP.

Requisitos para mapas de transformação LDAP personalizados

Se você optar por criar um mapa de transformação personalizado, ele deverá atender aos seguintes requisitos de mapeamento.

Requisitos para mapas de transformação LDAP personalizados

Tabela de fonte	Campo de fonte	Tabela de destino	Campo de destino	Aglutinar	Descrição
`ldap_import`	`u_source`	`sys_user`	fonte	falso	O campo **u_source** identifica o DN LDAP do usuário ou grupo importado. O sistema usa este campo para

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Requisitos para mapas de transformação LDAP personalizados

Tabela de fonte	Campo de fonte	Tabela de destino	Campo de destino	Aglutinar	Descrição
					determinar que um usuário requer autenticação LDAP para encontrar o gerente de um usuário e alocar usuários em grupos.
`ldap_import`	Selecione um dos seguintes campos: • `u_samaccountname` • `u_dn` • `u_cn`	`sys_user`	`user_name`	verdadeiro	Se o LDAP se integrar ao Active Directory, selecione **u_samaccountname** como o campo de fonte. Se outros diretórios LDAP forem usados, selecione **u_dn** ou **u_cn** como o campo de fonte.

Diferenças entre mapas de transformação LDSP e mapas de importação de legado

Ao especificar relacionamentos de mapeamento LDAP usando mapas de transformação, há uma grande diferença em como os campos de referência são definidos para o gerente e o departamento.

Ao usar um mapa de transformação, é necessário usar um script de transformação para criar referências. Isso ocorre porque o valor associado a um atributo LDAP como "gerente" é o nome diferenciado (DN) do gerente.

Sem alguma lógica adicional em vigor, o resultado é a criação de um registro de usuário com um nome de gerente igual ao nome diferenciado desse usuário LDAP. A integração inclui um script de transformação para facilitar a criação dessas referências. O mapa de transformação padrão "Importação de usuário LDAP" inclui scripts de transformação para essas referências.

Relacionamentos de mapeamento existentes

Ao atualizar mapas de importação legados para mapas de transformação, é possível manter os relacionamentos de mapeamento LDAP existentes antes da adição da aplicação LDAP do sistema. O servidor LDAP tem um campo de **mapa** que é uma referência ao mapa de importação legado.

Nota: Por padrão, este campo está oculto. Portanto, é preciso configurar o formulário para exibi-lo.

Se quiser fazer a transição usando um mapa de transformação, limpe a referência para o mapa de importação legado.

Configurações de mapa de importação LDAP

Verifique e use atributos para limitar os campos que a integração importa da fonte LDAP. Além disso, é importante mapear o campo user_name para o

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

atributo LDAP que contém o ID de login do usuário. No Active Directory, este geralmente é o atributo sAMAccountName. Se quiser importar e aglutinar em um atributo binário (como objectSID ou objectGUID), será necessário criar um script de transformação personalizado.

Nota: Qualquer valor mapeado para o campo user_name deve ser exclusivo.

Se um mapa de transformação (como importação de usuário LDAP) não for especificado, a integração usará os seguintes mapeamentos-padrão:

Mapeamento-padrão de importação LDAP

Campo de usuário ou variável	Atributo LDAP
user_name	sAMAccountName
e-mail	mail
telefone	telephoneNumber
home_phone	homePhone
mobile_phone	para celular
first_name	givenName
last_name	sn
título	título
departamento	departamento
gerente	gerente
middle_name	iniciais
u_memberof	grupos
u_member	membros
u_manager	gerente

Transformação de dados LDAP

Se um atributo LDAP contiver dados simples, o mapa de transformação vinculará um atributo LDAP importado a um campo apropriado na tabela de destino (Usuário ou Grupo). Por exemplo, dados de amostra no atributo sAMAccountName são mapeados para o campo **ID** do usuário na tabela de usuários.

Se os dados LDAP importados forem mapeados para um campo de referência, a instância procurará um registro existente correspondente. Se não houver nenhum registro correspondente, a instância criará um novo registro para o campo de referência, a menos que o mapeamento do campo especifique o contrário.

Por exemplo, suponha que o atributo LDAP seja mapeado para o campo de referência **Local** na tabela de usuários. Sempre que a importação traz um valor de atributo não correspondente a um valor de registro de local existente, o mapa de transformação cria um novo registro de local. O novo registro de local tem o mesmo valor do atributo importado, e o registro do usuário importado agora tem um link para o novo registro de local.

No entanto, há momentos em que o atributo LDAP retorna um nome diferenciado (DN), que é essencialmente uma referência a outro registro no diretório LDAP. Por exemplo, o atributo

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

gerente normalmente contém o nome diferenciado do gerente da entrada do diretório LDAP atual. Em geral, um DN importado usa uma cadeia de caracteres de texto longa, como: cn=Beth Anglin,ou=Users,dc=my-domain,dc=com.

> ⚠ **Aviso:** Certifique-se de que os campos de destino sejam longos o suficiente para conter um DN. Muitos campos de texto usam o tamanho-padrão de 40 caracteres, que pode não ser longo o suficiente para alguns valores de DN. O sistema ServiceNow trunca quaisquer valores que excedam o tamanho do campo.

Os administradores normalmente não desejam que o sistema crie novos usuários a partir do valor DN porque o novo usuário não tem associação com um usuário existente. Em vez disso, os administradores desejam que a importação localize o registro de usuário existente do gerente e o associe ao usuário recém-importado. A inclusão de script `LDAPUtils` contém as funções `setManager` e `processManagers`, que podem analisar um DN e pesquisar um usuário existente. Para obter melhores resultados, use essas funções para criar um mapa de transformação personalizado.

Por exemplo, o script de mapa de transformação `de importação de usuário LDAP` chama a função `setManager` :

```
//
// The manager coming in from LDAP is the DN value for the manager.
// The line of code below will locate the manager that matches the
// DN value and set it into the target record.  If you are not
// interested in getting the manager from LDAP then remove or
// comment out the line below
ldapUtils. setManager (source , target ) ;
```

Em alguns casos, a integração importa o registro de um usuário antes de importar o registro de usuário do gerente associado. Para lidar com esses casos, convém chamar a função `processManagers` após a conclusão da transformação. Por exemplo, o mapa de transformação de **importação de usuário LDAP** usa um script de transformação `onComplete` para chamar a função `processManagers`.

```
// It is possible that the manager for a user did not exist in the
 database when // the user was processed and therefore we could not
 locate and set the manager field. // The processManagers call below will
 find all those records for which a manager could  // not be found and
 attempt to locate the manager again. This happens at the end of the  //
 import and therefore all users should have been created and we should be
 able to  // locate the manager at this point
ldapUtils. processManagers ( ) ;
```

Remova ou comente as chamadas de função `setManager` e `processManagers` se sua integração LDAP não usar o atributo gerente.

Script LDAP

Crie mapas de transformaçãp personalizados, scripts e regras de negócios para especificar requisitos ao importar dados.

Mapas de transformação personalizados devem incluir scripts de transformação `onStart` e `onAfter`.

O script `onStart` deve chamar a inclusão de script `LDAPUtils` e iniciar o registro em log. Por exemplo, o mapa de transformação de **importação de usuário LDAP** tem um script `onStart` que usa este código:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

```
gs.include ( "LDAPUtils" ) ; var ldapUtils  = new LDAPUtils ( ) ;
ldapUtils. setLog (log ) ;
```

O script `onAfter` deve chamar a função `addMembers`. Por exemplo:

```
ldapUtils.addMembers (source , target ) ;
```

Definição de usuários desabilitados do Active Directory como inativos

Use o script a seguir para desativar automaticamente os usuários quando o usuário do AD associado estiver desabilitado.

Antes de Iniciar

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

É possível identificar usuários desabilitados do Active Directory verificando o valor do atributo `userAccountControl`. Essa regra será executada sempre que o valor `userAccountControl` mudar e desativar contas de usuário se o **Controle de contas de usuário** significar uma conta do AD desabilitada.

Use o script a seguir para desativar automaticamente os usuários quando o usuário do AD associado estiver desabilitado.

Procedimento

1. Configure o formulário do usuário e crie um novo campo de número inteiro chamado **Controle de contas de usuário**.
2. Adicione o mapeamento de userAccountControl (externo) ao novo campo.
3. Crie uma nova regra de negócios com as seguintes propriedades:

Desabilitação da regra de negócios de usuários do AD

Campo da regra de negócios	valor
Nome	Desabilitar usuários do AD
Tabela	Usuário [sys_user]
Quando	Antes
Condição	current.u_user_account_control.changes()

O campo Script deve conter o seguinte:

```
var disabledFlag = 2;
//perform a bitwise comparison on userAccountControl to see if the 2
 bit flag is enabled
if (current.u_user_account_control & disabledFlag) {
  gs.log('Disabling user: ' + current.user_name + 'userAccountControl='
 + current.u_user_account_control);
  current.active='false';
  current.locked_out='true';
}
```

Atribuição de valores de campo LDAP

É possível usar um script para atribuir um valor a qualquer campo para o qual exista um mapeamento de campo.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por exemplo, para atribuir um valor ao campo sys_user.company, crie um mapa de campo para o campo da empresa e adicione um script de transformação para:

```
company = "Don's Sporting Goods";
```

Exclusão de usuários LDAP específicos

Se não puder filtrar completamente a lista de usuários LDAP usando as propriedades de filtro LDAP, é possível excluir usuários com um script de mapa.

Depois de executar a lógica para identificar um usuário que não deve ser importado, defina o campo user_name como uma cadeia de caracteres vazia e esse usuário não será importado.

```
user_name='';
```

Uma maneira de identificar usuários para serem filtrados é procurar uma cadeia de caracteres no atributo `distinguishedName`. Por exemplo, este script exclui contas que não estão em uma OU de usuários. Será possível usar este script se houver muitos usuários na OU para incluir na opção LDAP da OU de destino.

```
//vdn is a variable mapped to distinguishedName
gs.include("LDAPUtils");
var vdn = source.getElement(this.distinguishedName);
if (vdn.indexOf('OU=Users')<0) {
  user_name='';
  gs.log('LDAP Import Skipping User: ' + vdn);
}
```

Um método mais complexo de filtragem é usar expressões regulares.

```
//vcn is a variable mapped to cn
//vdn is a variable mapped to distinguishedName
//c is the regular expression string
gs.include("LDAPUtils");
var vdn = source.getElement(this.distinguishedName);
var vcn = source.getElement(this.cn);
var c = /^[a-z][a-z][a-z][0-9][0-9][0-9]$/;
var nvcn = vcn.toLowerCase();
//test to see if the cn is in the form of 3 letters followed by 3
 numbers, only import these
if (c.test(nvcn)) {
 user_name = nvcn;
} else {
 gs.log("LDAP import rejected username: " + vcn + " for DN: " + vdn);
 user_name = "";
}
```

Definição da ação de escolha para importações de campo de referência

O mapa de transformação LDAP determina como os campos na tabela Conjunto para importação são mapeados para os campos em tabelas existentes, como Incidente ou Usuário.

Antes de Iniciar

Função necessária: administrador

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

Se o mapa de transformação LDAP atualizar um campo na tabela Conjunto para importação, a integração criará automaticamente um novo registro sempre que houver um novo registro nos dados LDAP. Se o mapa de transformação LDAP atualizar um campo de referência que armazena dados de outra tabela, o administrador poderá optar por criar, ignorar ou rejeitar novos registros LDAP.
Por exemplo, se a integração receber um novo registro de departamento que não corresponda a nenhum departamento existente, convirá atualizar todos os outros campos de registro LDAP sem criar um novo registro de departamento na instância. O mapa de transformação permite que você defina as opções de criação de registro para cada campo de referência.

Procedimento

1. Navegue até **Todos** > **Sistema LDAP** > **Mapas de transformação**.
2. Na lista relacionada Mapas de campo, selecione uma das seguintes ações no campo **Ação de escolha** :
   - **criar**: cria um novo registro de campo de referência se não existir um registro correspondente.
   - **ignorar**: ignora novos registros no campo de referência e conclui o processamento de todos os outros campos no mapa de transformação.
   - **rejeitar**: interrompe a transformação de todo o registro.

   Nota: O mapa de campo exibe o campo **Ação de escolha** somente para campos de referência.

Verificação de mapeamento LDAP

Depois de criar um mapa de transformação LDAP, atualize os dados LDAP para verificar se ele funciona conforme o esperado.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Navegue até **Todos** > **Sistema LDAP** > **Cargas programadas**.
2. Clique no seu trabalho de importação LDAP.
3. Clique em **Executar agora**.

Solução de problemas de integração LDAP

Se você estiver integrando o servidor LDAP e tiver dúvidas, esses itens poderão ajudá-lo a solucionar o problema.

Verificações preliminares

- Se o LDAP não estiver disponível, os usuários não poderão fazer login na instância. Recomendamos a manutenção de contas locais para administradores para que, se o LDAP estiver inativo, os administradores ainda possam acessar a instância.
- Verifique a conta de serviço para garantir que ela não esteja expirada ou bloqueada.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Verifique o formato do nome de usuário. Em vez de usar apenas o nome de usuário, tente usar o domínio com o nome de usuário ou username@domain.
- Verifique se você alterou a entrada `system_id` no registro `ldap_server_config`. Se o `system_id` for modificado não intencionalmente com um conjunto de atualizações, o `system_id` apontará para o nó incorreto da instância de destino e não funcionará.

Códigos de erro

O arquivo de log LDAP lista os códigos de erro padrão do setor para o LDAP e o Active Directory (AD). O arquivo de log LDAP está contido no arquivo wrapper. Os códigos de erro LDAP são números de dois dígitos, e os códigos de erro do Active Directory são números de três dígitos. Para obter uma lista dos códigos de erro mais comuns, consulte Códigos de erro LDAP.

Integração de vários domínios

É possível integrar vários domínios na mesma floresta ou em domínios totalmente não confiáveis. Recomendamos a criação de um registro de servidor LDAP separado para cada domínio. Cada registro do servidor LDAP deve apontar para um controlador de domínio para esse domínio específico. Com isso, será necessário permitir conexões com cada um dos controladores de domínio. Não há suporte para várias florestas do AD por meio LDAP com uma conta LDAP.

Ao expandir para mais de um domínio, é essencial identificar atributos LDAP exclusivos para os nomes de usuário da aplicação e importar valores de aglutinação. Um atributo de aglutinação exclusivo comum para o Active Directory é `objectSid`. Os nomes de usuário exclusivos variam de acordo com o design de dados LDAP. Atributos exclusivos comuns são `e-mail` ou `userPrincipalName`.

Registros de entrada

Consulte Mapas de transformação LDAP para definir como a integração processa registros LDAP de entrada que não contém valores correspondentes nos campos de referência.

Erros comuns de autenticação

- O usuário não consegue fazer login (DN inválido)
- CN inválido
- Conexões inválidas

Testes automáticos de conexão LDAP

É possível testar as conexões com os servidores LDAP manualmente ou permitir que ServiceNow teste as conexões automaticamente.

O sistema testa a conexão automaticamente:

- Toda vez que um usuário abre o formulário do servidor LDAP.
- Por meio do trabalho agendado do teste de conexão LDAP, que é executado a cada 15 minutos por padrão.

  É possível alterar a frequência com que esse trabalho agendado é executado. Se esse trabalho agendado não puder estabelecer uma conexão, um novo trabalho de programação única repetirá o teste de conexão após cinco minutos ou metade do valor do **intervalo de repetição** no trabalho agendado, o que ocorrer primeiro.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mensagens de erro aparecerão no formulário se houver algum problema de conexão com o servidor LDAP. Também há suporte para conexões de teste para servidores de apoio de um MID Server.

Exibição do monitor LDAP

É possível exibir informações atuais sobre servidores LDAP e ouvintes usando o monitor LDAP.

Antes de Iniciar

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

Os estados disponíveis são:

- Ativo
- Inativo
- Erro
- Ativo (desligando...)
- Erro (desligando...)

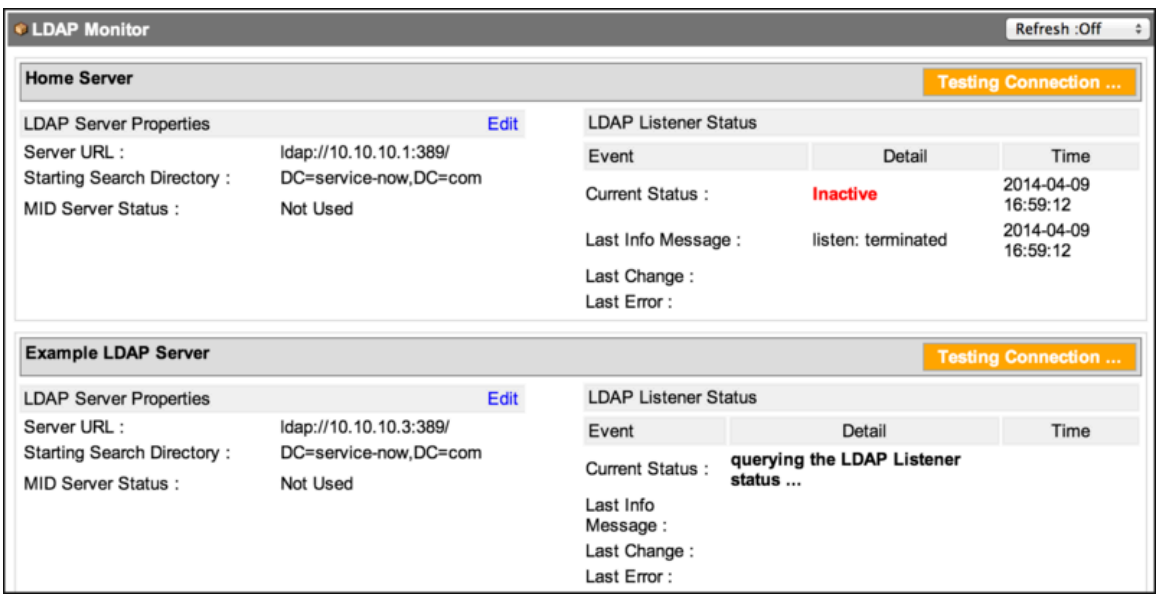
Além do estado atual, o monitor também exibe:

- A última mensagem detectada pelo ouvinte, como aguardar mudanças de LDAP, erro de conexão e assim por diante.
- A última mudança de usuário LDAP, como novo usuário, usuário atualizado e assim por diante.
- O último erro ocorrido.

Para exibir o monitor LDAP:

Procedimento

Navegue até **Todos** > **LDAP** > **Sistema LDAP** > **Monitor LDAP**.



Consulte a tabela para obter descrições das propriedades e dos campos da tela.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Monitor LDAP

Campo	Descrição
Atualizar	É possível configurar a taxa de atualização clicando no campo **Atualizar** na barra de cabeçalho do monitor do servidor LDAP e selecionando o número de segundos entre cada atualização de dados. Também é possível selecionar **Nenhum** para suprimir a atualização.
Status da conexão	O indicador de conexão do servidor está localizado no lado direito, acima dos campos de status do ouvinte LDAP. Quando o servidor está conectado, a caixa fica verde e informa o status *Conectado*. Quando o servidor não está conectado, a caixa fica vermelha e informa o status *Não conectado*. Quando a conexão do servidor está sendo testada, a caixa fica amarela e informa o status *Conexão de teste*.
Propriedades do servidor LDAP	
Editar	Ao monitorar os servidores LDAP, é possível fazer mudanças nas propriedades clicando em **Editar** na tela Monitor do servidor LDAP.
URL do servidor	A combinação do nome do servidor e da porta do servidor em que o servidor LDAP está ouvindo. Frequentemente, a porta é definida como uma das seguintes: • 389: a porta-padrão para conexão LDAP em texto não criptografado • 636: a porta-padrão para conexão LDAP por meio de uma conexão SSL Valor de exemplo: ldap://10.10.10.3:389/ Seu servidor LDAP pode ter mais de um endereço URL. Isso NÃO estabelece várias estruturas de diretório das quais é possível importar dados, o que é feito por meio da criação de outra entrada de servidor LDAP, mas fornece redundância para evitar um ponto único de falha quando há vários servidores LDAP. Os endereços de URL LDAP são separados por um caractere de espaço, e o sistema testa automaticamente cada endereço de servidor até que uma conexão válida possa ser feita.
Diretório de pesquisa inicial	O diretório inicial ou RDN (Nome distinto relativo) onde o sistema começa a pesquisar usuários ou grupos. Valor de exemplo: DC=service-now,DC=com Não há dados ACIMA deste ponto disponíveis para importação. A instância tem visibilidade no diretório especificado e nos diretórios ABAIXO na hierarquia LDAP.
Status do MID Server	O status da conexão atual do MID Server.
Status do ouvinte LDAP	
Status atual	Isso indica se o ouvinte está ativo.
Última mensagem de informação	Exibe a última mensagem recebida pelo servidor LDAP relacionada às mudanças de usuário e grupo e a hora em que a mensagem foi recebida.
Última mudança	Exibe a última mudança feita no servidor LDAP e a hora em que ocorreu.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Último erro	Exibe o último erro ocorrido no servidor LDAP e a hora em que ocorreu.

Códigos de erro LDAP

O arquivo de log LDAP lista os códigos de erro padrão do setor para o LDAP e o Active Directory (AD).

Códigos de erro padrão

Erros LDAP padrão

Erro/ código de dados	Texto	Descrição
0	LDAP_SUCCESS	Indica que a operação do cliente solicitada foi concluída com sucesso.
2	LDAP_PROTOCOL_ERROR	Indica que o servidor recebeu uma solicitação inválida ou malformada do cliente.
3	LDAP_TIMELIMIT_EXCEEDED	Indica que o limite de tempo da operação especificado pelo cliente ou pelo servidor foi excedido. Nas operações de pesquisa, são retornados resultados incompletos.
4	LDAP_SIZELIMIT_EXCEEDED	Indica que o limite de tamanho especificado pelo cliente ou servidor foi excedido em uma operação de pesquisa. Resultados incompletos são retornados.
5	LDAP_COMPARE_FALSE	Não indica uma condição de erro. Indica que os resultados de uma operação de comparação são falsos.
6	LDAP_COMPARE_TRUE	Não indica uma condição de erro. Indica que os resultados de uma operação de comparação são verdadeiros.
7	LDAP_AUTH_METHOD_NOT_SUPPORTED	Indica que, durante uma operação de vinculação, o cliente solicitou um método de autenticação não compatível com o servidor LDAP.
8	LDAP_STRONG_AUTH_REQUIRED	Indica um dos seguintes: em solicitações de vinculação, o servidor LDAP aceita somente autenticação forte. Em uma solicitação do cliente, ele solicitou uma operação como "excluir", que requer autenticação forte. Em um aviso não solicitado de desconexão, o servidor LDAP descobre que a segurança protegendo a

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Erros LDAP padrão

Erro/ código de dados	Texto	Descrição
		comunicação entre o cliente e o servidor falhou inesperadamente ou foi comprometida.
9		Reservado.
10	LDAP_REFERRAL	Não indica uma condição de erro. LDAPv3, indica que o servidor não contém a entrada de destino da solicitação, mas os servidores no campo de referência podem contê-la.
11	LDAP_ADMINLIMIT_EXCEEDED	Indica que um limite do servidor LDAP definido por uma autoridade administrativa foi excedido.
12	LDAP_UNAVAILABLE_CRITICAL_EXTENSION	Indica que o servidor LDAP foi incapaz de satisfazer uma solicitação porque uma ou mais extensões críticas não estavam disponíveis. O servidor não oferece suporte ao controle ou o controle não é apropriado para o tipo de operação.
13	LDAP_CONFIDENTIALITY_REQUIRED	Indica que a sessão não está protegida por um protocolo como o TLS (Transport Layer Security), que fornece confidencialidade à sessão.
14	LDAP_SASL_BIND_IN_PROGRESS	Não indica uma condição de erro, mas indica que o servidor está pronto para a próxima etapa do processo. O cliente deve enviar o mesmo mecanismo SASL ao servidor para continuar o processo.
15		Não usado.
16	LDAP_NO_SUCH_ATTRIBUTE	Indica que o atributo especificado na operação de modificação ou comparação não existe na entrada.
17	LDAP_UNDEFINED_TYPE	Indica que o atributo especificado na operação de modificação ou adição não existe no esquema do servidor LDAP.
18	LDAP_INAPPROPRIATE_MATCHING	Indica que a regra correspondente especificada no filtro de pesquisa não corresponde a uma regra definida para a sintaxe do atributo.
19	LDAP_CONSTRAINT_VIOLATION	Indica que o valor do atributo especificado em uma operação de modificação, adição ou modificação

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Erros LDAP padrão

Erro/ código de dados	Texto	Descrição
		do DN viola as restrições definidas no atributo. A restrição pode ser de tamanho ou conteúdo (somente cadeia de caracteres, não binária).
20	LDAP_TYPE_OR_VALUE_EXISTS	Indica que o valor do atributo especificado em uma operação de modificação ou adição já existe como um valor para esse atributo.
21	LDAP_INVALID_SYNTAX	Indica que o valor do atributo especificado em uma operação de adição, comparação ou modificação é uma sintaxe inválida ou não reconhecida para o atributo.
22-31		Não usado.
32	LDAP_NO_SUCH_OBJECT	Indica que o objeto de destino não foi encontrado. Este código não é retornado nas seguintes operações: operações de pesquisa que localizam a base de pesquisa, mas não encontram entradas correspondentes ao filtro de pesquisa. Operações de vinculação.
33	LDAP_ALIAS_PROBLEM	Indica que ocorreu um erro quando um alias foi cancelado.
34	LDAP_INVALID_DN_SYNTAX	Indica que a sintaxe do DN está incorreta. (Se a sintaxe do DN estiver correta, mas as regras de estrutura do servidor LDAP não permitirem a operação, o servidor retornará o código 53: LDAP_UNWILLING_TO_PERFORM.)
35	LDAP_IS_LEAF	Indica que a operação especificada não pode ser executada em uma entrada leaf. (Este código não está nas especificações LDAP, mas está reservado para esta constante.)
36	LDAP_ALIAS_DEREF_PROBLEM	Indica que, durante uma operação de pesquisa, o cliente não tem direitos de acesso para leitura do nome do objeto com alias ou o cancelamento da referência não é permitido.
37-47		Não usado.
48	LDAP_INAPPROPRIATE_AUTH	Indica que, durante uma operação de vinculação, o cliente está tentando

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Erros LDAP padrão

Erro/ código de dados	Texto	Descrição
		usar um método de autenticação que ele não pode usar corretamente. Por exemplo, qualquer um dos itens a seguir causa esse erro: o cliente retorna credenciais simples quando credenciais fortes são necessárias OU o retorna um DN e uma senha para uma vinculação simples quando a entrada não tem uma senha definida.
49	LDAP_INVALID_CREDENTIALS	Indica que, durante uma operação de vinculação, ocorreu um dos seguintes: o cliente passou um DN ou senha incorretos ou a senha está incorreta porque expirou, a detecção de invasão bloqueou a conta ou outro motivo semelhante. Consulte o código de dados para obter mais informações.
49/52e	CREDENCIAIS AD_INVALID	Indica um erro AcceptSecurityContext do Active Directory (AD), que é retornado quando o nome de usuário é válido, mas a combinação de senha e credencial do usuário é inválida. Este é o AD equivalente ao código de erro 49 LDAP.
49/525	USUÁRIO NÃO ENCONTRADO	Indica um erro de dados AcceptSecurityContext do Active Directory (AD) que é retornado quando o nome de usuário é inválido.
49/530	NOT_PERMITTED_TO_LOGON_AT_THIS_TIME	Indica um erro de dados AcceptSecurityContext do Active Directory (AD), que é uma falha de logon causada porque o usuário atualmente não tem permissão para fazer logon. Retorna somente quando é apresentado um nome de usuário e uma credencial de senha válidos.
49/531	RESTRICTED_TO_SPECIFIC_MACHINES	Indica um erro de dados AcceptSecurityContext do Active Directory (AD) que é uma falha de logon causada porque o usuário não tem permissão para fazer logon neste computador. Retorna somente quando é apresentado um nome de usuário e uma credencial de senha válidos.
49/532	PASSWORD_EXPIRED	Indica um erro de dados AcceptSecurityContext do Active

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Erros LDAP padrão

Erro/ código de dados	Texto	Descrição
		Directory (AD), que é uma falha de logon. A senha da conta especificada expirou. Retorna somente quando apresentado com nome de usuário e credencial de senha válidos.
49/533	ACCOUNT_DISABLED	Indica um erro de dados AcceptSecurityContext do Active Directory (AD), que é uma falha de logon. A conta está desabilitada no momento. Retorna somente quando apresentado com nome de usuário e credencial de senha válidos.
49/568	ERROR_TOO_MANY_CONTEXT_IDS	Indica que, durante uma tentativa de logon, o contexto de segurança do usuário acumulou muitas IDs de segurança. Este é um problema com o objeto/conta do usuário LDAP específico que deve ser investigado pelo administrador LDAP.
49/701	ACCOUNT_EXPIRED	Indica um erro de dados AcceptSecurityContext do Active Directory (AD), que é uma falha de logon. A conta do usuário expirou. Retorna somente quando apresentado com nome de usuário e credencial de senha válidos.
49/773	O USUÁRIO DEVE REDEFINIR A SENHA	Indica um erro de dados AcceptSecurityContext do Active Directory (AD). A senha do usuário deve ser alterada antes que o primeiro login seja realizado. Retorna somente quando apresentado com nome de usuário e credencial de senha válidos.
50	LDAP_INSUFFICIENT_ACCESS	Indica que o chamador não tem direitos suficientes para executar a operação solicitada.
51	LDAP_BUSY	Indica que o servidor LDAP está muito ocupado para processar a solicitação do cliente no momento, mas, se o cliente aguardar e reenviar a solicitação, o servidor poderá processá-la.
52	LDAP_UNAVAILABLE	Indica que o servidor LDAP não pode processar a solicitação de vinculação do cliente geralmente porque está sendo encerrado.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Erros LDAP padrão

Erro/ código de dados	Texto	Descrição
52e	CREDENCIAIS AD_INVALID	Indica um erro AcceptSecurityContext do Active Directory (AD), que é retornado quando o nome de usuário é válido, mas a combinação de senha e credencial do usuário é inválida. Este é o equivalente AD do código de erro 49 LDAP: LDAP_INVALID_CREDENTIALS.
53	LDAP_UNWILLING_TO_PERFORM	Indica que o servidor LDAP não pode processar a solicitação devido a restrições definidas pelo servidor. Este erro é retornado pelos seguintes motivos: a solicitação de adição de entrada viola as regras de estrutura do servidor OU a solicitação de modificação de atributo especifica atributos que os usuários não podem modificar OU restrições de senha impedem a ação OU as restrições de conexão impedem a ação.
54	LDAP_LOOP_DETECT	Indica que o cliente descobriu um alias ou loop de referência e, portanto, não pode concluir esta solicitação.
55-63		Não usado.
64	LDAP_NAMING_VIOLATION	Indica que a operação de adição ou modificação do DN viola as regras de estrutura do esquema. Por exemplo, a solicitação subordina a entrada um alias. A solicitação subordina a entrada a um contêiner proibido pelas regras de contenção. O RDN da entrada usa um tipo de atributo proibido.
65	LDAP_OBJECT_CLASS_VIOLATION	Indica que a operação de adição, modificação ou modificação do DN viola as regras de classe de objeto da entrada. Por exemplo, os seguintes tipos de solicitação retornam este erro: a operação de adição ou modificação tenta adicionar uma entrada sem um valor para um atributo obrigatório. A operação de adição ou modificação tenta adicionar uma entrada com um valor para um atributo não contido pela definição de classe. A operação de modificação tenta remover um atributo obrigatório

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Erros LDAP padrão

Erro/ código de dados	Texto	Descrição
		sem remover a classe auxiliar que define o atributo como necessário.
66	LDAP_NOT_ALLOWED_ON_NONLEAF	Indica que a operação solicitada é permitida somente em entradas leaf. Por exemplo, os seguintes tipos de solicitações retornam este erro: o cliente solicita uma operação de exclusão em uma entrada primária. O cliente solicita uma operação de modificação de DN em uma entrada primária.
67	LDAP_NOT_ALLOWED_ON_RDN	Indica que a operação de modificação tentou remover um valor de atributo que forma o nome distinto relativo da entrada.
68	LDAP_ALREADY_EXISTS	Indica que a operação de adição tentou adicionar uma entrada já existente ou que a operação de modificação tentou renomear uma entrada com o nome de uma entrada já existente.
69	LDAP_NO_OBJECT_CLASS_MODS	Indica que a operação de modificação tentou modificar as regras de estrutura de uma classe de objeto.
70	LDAP_RESULTS_TOO_LARGE	Reservado para o CLDAP.
71	LDAP_AFFECTS_MULTIPLE_DSAS	Indica que a operação de modificação do DN move a entrada de um servidor LDAP para outro e requer mais de um servidor LDAP.
72-79		Não usado.
80	LDAP_OTHER	Indica uma condição de erro desconhecida. Este é o valor-padrão para códigos de erro de NDS que não são mapeados para outros códigos de erro LDAP.
775	USER_ACCOUNT_LOCKED	Indica que os usuários não podem fazer login porque a conta do usuário está bloqueada.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Códigos de erro personalizados

Códigos de erro LDAP personalizados

Erro/código de dados	Texto
10000	LDAP_ERROR_GENEREL
10001	LDAP_ERROR_MAL_FORMED_URL
10002	LDAP_ERROR_UNAUTHENTICATED_BIND
10300	LDAP_ERROR_COMMUNICATION_EXCEPTION
10301	LDAP_ERROR_SOCKET_TIMEOUT
10302	LDAP_ERROR_CONNECTION_REFUSED
10303	LDAP_ERROR_CONNECTION_RESET
10304	LDAP_ERROR_NO_ROUTE
10305	LDAP_ERROR_UNKNOW_HOST
10400	LDAP_ERROR_SSL_EXCEPTION
10401	LDAP_ERROR_SSL_EMPTY_CERT_STORE
10402	LDAP_ERROR_SSL_CERT_NOT_FOUND
10403	LDAP_ERROR_SSL_CERT_EXPIRED
10500	LDAP_ERROR_INVALID_SEARCH_FILTER_EXCEPTION

Envio de uma senha de uso único quando o servidor LDAP estiver inativo

Uma propriedade LDAP está disponível para enviar uma senha de uso único para um usuário se ele não puder fazer login porque o servidor LDAP está inativo. Também é possível configurar outra propriedade para controlar o período em que a senha será válida.

Antes de Iniciar

Função necessária: administrador

Para receber uma senha de uso único, o usuário deve ter notificações habilitadas em seu perfil do usuário. A notificação é apenas uma mensagem de e-mail. Não há suporte para mensagens SMS.

Por Que e Quando Desempenhar Esta Tarefa

Ambas as propriedades estão habilitadas por padrão. O valor-padrão da propriedade que controla a validade da senha é de 10 minutos.

Procedimento

1. Abra a lista de propriedades do sistema inserindo `sys_properties.list` no filtro do navegador de aplicações.
2. Encontre a propriedade *`glide.ldap.onetime.password.enabled`*.
3. Defina a propriedade como `verdadeira`.
4. Para alterar o tempo de validade da senha de um usuário, defina a seguinte propriedade como um número inteiro de minutos: *`glide.authenticate.onetime.password.validity`*.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Sincronização de registro LDAP

Os administradores podem sincronizar registros LDAP inativos, desabilitados ou excluídos com seus registros LDAP.

A sincronização de registro LDAP é o processo que detecta registros inativos no servidor LDAP e atualiza os registros LDAP correspondentes. A detecção de registros LDAP inativos envolve a definição de indicadores de dados consistentes para cada objeto de usuário, a importação de dados LDAP e a avaliação dos indicadores de dados.

Um indicador de dados pode ser:

- Um campo de data
- Associação em uma OU específica (identificada pela análise do atributo *dn*) usando o atributo *useraccountcontrol*
- Uma combinação desses indicadores

Os dados importados chegam à instância por meio de tabelas de conjunto para importação em que os dados podem ser avaliados e processados.

O processo de importação pode usar Filtros de atualização LDAP em vários trabalhos de importação para dividir diferentes tipos de registros de usuário e segregar registros para processamento separado.

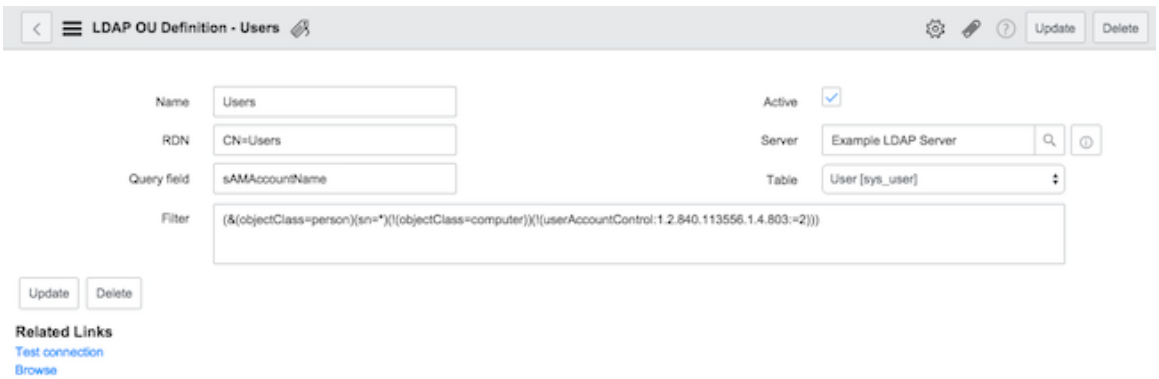
Filtros de atualização LDAP

Filtros no processo de atualização LDAP podem ser usados para especificar o processamento que ignora inserções de usuários desabilitados.

É possível liberar o filtro da OU LDAP para retornar todos os dados para sua tabela de conjunto para importação (incluindo usuários inativos) e, em seguida, especificar o processamento que ignora as inserções de usuários desativados. A amostra de definição de "Usuários" da OU que a instância fornece no exemplo de LDAP pronto para uso contém um filtro.

Esse filtro é importante porque define quais registros de usuário são trazidos para a tabela de conjunto para importação para serem avaliados. Embora obtenha uma carga de dados menor, uma limitação deste filtro é que ele ignora usuários inativos. Consequentemente, os registros de usuários inativos não são importados para as tabelas temporárias do conjunto para importação. Como não há visibilidade dos registros de usuários inativos, não há capacidade de avaliação dos indicadores de registro.

Filtro OU LDAP



Para usar a filtragem no processo de atualização LDAP principal, altere o filtro para trazer todos os registros de usuários. O resultado é que todos os registros serão carregados

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

na tabela temporária de conjunto para importação, onde podem ser avaliados e transformados.

Nota: Atenção: como a filtragem retorna todos os registros, é possível que seja incluída uma grande quantidade de contas LDAP inativas antigas, que não devem ser inseridas na instância. Um registro de usuário nunca deve ser criado para um usuário desabilitado.

Extração LDAP

Um processo de extração LDAP pode ser implementado para a deteção de usuários desabilitados.

Uma extração da origem LDAP pode ser filtrada para usuários desativados usando um sinalizador ativo que pode ser definido como "falso" para cada registro na importação. Especifique ('target.active=false') e copie para o campo **Script** diretamente no registro do mapa de transformação da tabela.

Vantagens

As vantagens deste método incluem:

- Scripts simples
- Os registros de usuário existentes não estão envolvidos no processamento
- Usuários inativos não são carregados em uma tabela de importação temporária
- Sem impacto sobre o desempenho

Desvantagens

As desvantagens deste método incluem:

- Um processo adicional é criado
- O conjunto de extrações deve ser colocado em um local onde sua origem de dados possa acessá-lo

Método alternativo

Filtros de atualização LDAP use vários trabalhos de importação para dividir diferentes tipos de registros de usuários, segregando registros para processamento separado.

Contas de usuário LDAP inativas

Identifique que uma conta de usuário atual está inativa ou foi desabilitada ou excluída de um LDAP do Active Directory (AD).

Um problema comum de integração LDAP é como detectar usuários desabilitados ou excluídos em um Active Directory (AD) e desativá-los na instância. Em um LDAP do Active Directory, um filtro geralmente é definido para excluir usuários inativos na atualização, portanto a instância não reconhece usuários que estão desabilitados ou excluídos no AD. O problema é como detectar se um usuário atual existente está inativo ou foi excluído do AD.

Para mais informações sobre como localizar contas inativas, consulte Encontrar contas LDAP inativas usando o campo userAccountControl.

Nota: A abordagem recomendada é desativar registros de usuários e todos os outros tipos de registros, não os excluir. Cada registro está vinculado a outros registros, e a exclusão de um deles destrói todos os relacionamentos com outros registros. Desativar os registros mantém esses relacionamentos.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Encontrar contas LDAP inativas usando o campo userAccountControl

Identifique quando um usuário do Active Directory (AD) é excluído (ou desativado).

Antes de Iniciar
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa
Um método é rastrear o status ativo dos usuários do AD e criar uma regra de negócios para atualizar as contas correspondentes quando uma conta do AD estiver inativa.

Procedimento

1. Crie um novo campo de cadeia de caracteres na tabela Usuário [sys_user] para rastrear o valor do campo **userAccountControl** do AD.
   Por exemplo: `u_ad_user_account`.
2. Crie um script de transformação LDAP para definir o valor do campo.

   Example

   ```
   target.u_ad_user_account = source.userAccountControl
   ```

3. Atualize o filtro LDAP para exibir contas do AD desabilitadas.

   Example
   Este é um exemplo de um filtro.

   ```
   (&(objectClass=person)(sn=*)(!(objectClass=computer))(!
   (userAccountControl:1.2.840.113556.1.4.803:=2)))
   ```

   Este é um exemplo de um filtro de substituição que pode ser usado.

   ```
   (&(objectClass=person)(sn=*)(!(objectClass=computer)))
   ```

4. Crie uma regra de negócios onChange para definir o campo ativo como falso sempre que o campo u_ad_user_account contiver o valor 514.
   "514" indica uma conta inativa.

Exemplos de script LDAP

Os exemplos de script a seguir presumem que você usa um Active Directory (AD) para o servidor LDAP.

Script de valores do atributo userAccountControl
Este exemplo testa a origem dos valores do atributo userAccountControl associados a um usuário desabilitado (514 ou 546).

```
//Deactivate LDAP-disabled users during transform based on
 'userAccountControl' attribute
if(source.u_useraccountcontrol == '514' || source.u_useraccountcontrol ==
 '546'){
   target.active=false;
   target.locked_out=true;
}
```

Este é um exemplo usando uma verificação de bits:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

```
if(source.u_useraccountcontrol & 2){
   active = false;
}
```

Script do atributo userAccountControl

Este exemplo examina o atributo userAccountControl, mas não testa valores específicos. Ele também contém a opção de reativação de contas de usuário LDAP.

```
/*
* Deactivate LDAP-disabled users during transform based on
 'userAccountControl' attribute
* Convert the userAccountControl attribute back to a hex value
*/
var ctrl = parseInt(source.u_useraccountcontrol, 10);
ctrl = ctrl.toString(16);

/*
* The only digit we care about is the final one
* A final hex digit value of '2' in 'ctrl' means disabled
*/
if(ctrl.substr(-1) == "2"){

   //Deactivate and lock the user account
   target.active = false;
   target.locked_out = true;

   //Ignore any insert of a disabled record
   if(action == 'insert'){
      ignore = true;
   }
}
/* Optional: Uncomment else block to reactivate and unlock the user
 account
else {
   target.active = true;
   target.locked_out = ctrl.substr(-2, 1) == "1";
}
*/
```

Script do mapa de transformação onBefore

Este é um exemplo de um script do mapa de transformação onBefore. O script identifica registros desabilitados e que estão sendo inseridos. Se estiver ocorrendo uma inserção de um usuário desabilitado, a transformação da operação ignorará o registro.

```
//Ignore any insert of a disabled record as defined by the
 'userAccountControl' attribute
var uc = source.u_useraccountcontrol;
if((uc == '514' || uc == '546') && action == 'insert'){
   ignore = true;
}
```

Script de membro DN

Este exemplo de script apresenta flexibilidade ao não contar com os valores de userAccountControl 546 e 514, mas, em vez disso, verifica se o usuário é um membro de um Nome diferenciado (DN) específico. É possível usar este script no campo **Script** do registro "Mapa de transformação da tabela" ou em um script do mapa de transformações onBefore.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

```
//Deactivate LDAP-disabled users during transform based on OU membership
 in 'dn'
if(source.u_dn.indexOf('OU=Disabled Accounts') > -1){
   target.active = false;
   target.locked_out = true;
}
```

Modo de aplicação do Active Directory (ADAM)

O modo de aplicação do Active Directory (ADAM) é um serviço de diretório compatível com LDAP.

Nota: Um nível básico de conhecimento com Microsoft Windows Server e Active Directory é necessário para entender este tópico. Você também deve ter permissões de administrador no servidor configurando para o ADAM.

Estes são procedimentos de amostra. Não é possível fornecer suporte direto devido a variações de instalação e ambiente. Recomendamos o trabalho com um consultor Microsoft.

O ADAM conta com uma instalação simples e é executado como um serviço em sistemas operacionais Windows. Ele pode ser totalmente personalizado e distribuído como um componente de aplicação ou usado como um diretório independente LDAP. O ADAM usa as mesmas tecnologias encontradas nos controladores de domínio do Active Directory (incluindo recursos de replicação e delegação) e tem seus próprios recursos de administração e personalização. Ele pode ser executado como um serviço Windows. O ADAM pode ser instalado nos sistemas operacionais Windows XP, 2000, 2003 e 2008. O ADAM está incluso como parte do Windows Server 2003 R2 e Windows Server 2008. Um download está disponível em http://www.microsoft.com/downloads http://www.microsoft.com/downloads para sistemas operacionais anteriores.

Segurança

Algumas políticas de segurança da empresa proíbem que fornecedores e parceiros externos se conectem diretamente a um controlador de domínio do Active Directory (AD). Se a exposição de determinados objetos ou atributos do AD a um fornecedor ou parceiro externo for proibida, o acesso a objetos e atributos poderá ser bloqueado usando as entradas de controle de acesso de segurança do AD (ACE ou ACL). Dependendo dos requisitos de segurança, esse método pode apresentar complexidade na integração.
É recomendável consolidar vários domínios e florestas. Se todas as importações e autenticações LDAP precisarem ser canalizadas por meio de uma única origem, o ADAM poderá ser usado como uma origem consolidada. Com o lançamento do Windows 2008, esta funcionalidade foi renomeada para Light-Weight-Directory Service, ou LDS. A instalação e a configuração são semelhantes às do Windows Server 2003 R2.

Conhecimento recomendado

Para esta tarefa, é preciso compreender o AD, classes de objeto e atributos. Para obter uma integração bem-sucedida, é preciso conhecimento da estrutura de objetos do AD atual, estar familiarizado com as delegações do Active Directory e ter uma estratégia sobre como usar o ADAM e para quais finalidades. Se você não estiver familiarizado com o AD ou o ADAM, trabalhe com o administrador do AD para configurar um novo ambiente do ADAM.

Trustes

Se objetos `userProxy` forem usados, o computador que hospeda o ADAM deverá ser um membro do domínio contendo as contas do AD ou de um domínio confiável.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Conectividade interna

Se objetos *userProxy* forem usados, o computador do ADAM deverá ter a capacidade de conectividade aos controladores de domínio relacionados para executar a autenticação de proxy.

Informações relacionadas

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

Configure uma instância com o ADAM

A primeira instalação copia os arquivos do ADAM para o seu computador, registra os componentes necessários e cria os atalhos da aplicação.

Antes de Iniciar

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

Por padrão, todos os arquivos de aplicação são instalados em `%systemroot%\ADAM`.

- Windows Server 2003 R2 - ADAM pode ser instalado usando **Painel de controle > Adicionar e remover programas> Gerente de componentes opcionais** .
- Windows Server 2000 e Windows XP - Baixados http://www.microsoft.com/downloads da Microsoft.

Crie o serviço de primeira instância que funciona como o primeiro serviço de diretório hospedado pelo ADAM. Faça um dos seguintes:

Procedimento

- Execute *adaminstall.exe* da pasta do ADAM.
- Use o atalho **Criar uma instância do ADAM** em **Menu iniciar > Programas > Pasta do ADAM** .

1. Selecione a opção **Instalação de uma instância exclusiva**.

   Nota: É possível usar esta opção para instalar uma réplica de instância em um segundo servidor para fornecer um sistema tolerante a falhas.

2. Preencha os campos:

Instância do ADAM

Campo	Descrição
Nome da instância	usado principalmente para identificar o nome do serviço Windows e o nome de exibição
Portas	define os números de porta a serem usados para ouvintes LDAP e LDAPS. A porta-padrão LDAP é 389, e LDAPS é 636. Se essas portas estiverem em uso no servidor, o assistente de configuração selecionará novas portas. Trabalhe com o administrador da rede para determinar as melhores portas a serem usadas
Partição de diretório de aplicações	cria uma partição de diretório de aplicações. Não é necessário nesta etapa. Agora, recomendamos a criação de um nova partição. Uma prática recomendada é usar o mesmo nome

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	diferenciado da floresta ou do domínio, mas substituir o domínio de nível mais alto por "adam" em vez de "com" ou "local". Por exemplo, se a partição de floresta for *dc=myCompany,dc=com*, será possível criar a partição do ADAM como *dc=myCompany,dc=adam*
Locais do arquivo	seleciona o(s) local(is) para os dados da partição do ADAM.
Seleção de conta de serviço	seleciona a conta de serviço sob a qual a instância será executada. Para serviços autônomos, é possível usar a conta de serviço de rede padrão. Se você planeja usar réplicas, será necessário usar uma conta com acesso a todas as instâncias do ADAM.
Administradores do ADAM	a delegação no diretório do ADAM que aproveita a autenticação integrada do Windows. É assim que o acesso inicial é concedido para a administração. Depois que os direitos são concedidos à conta inicial, esse usuário ou grupo delega direitos a outros usuários do Windows ou do ADAM. É possível selecionar o padrão para a concessão de acesso de administrador somente ao usuário atual ou conceder acesso a um usuário ou grupo diferente, com base em suas necessidades.
Importe arquivos LDIF	os arquivos a serem importados. O MS-userProxy é o arquivo mais importante a ser importado, mas vale a pena adicionar todos os arquivos disponíveis, uma vez que há pouca sobrecarga no esquema e você não precisa se preocupar em estendê-lo mais tarde se suas necessidades aumentarem. Confirme os detalhes e o assistente concluirá a configuração.

Informações relacionadas

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

Configurar o console do ADAM

Configure o console do ADAM. Embora haja muitas semelhanças entre o ADAM e o Active Directory, a administração deles pode ser muito diferente, uma vez que não há console de gerenciamento de **Usuários e computadores**.

Antes de Iniciar

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

A maior parte da administração geral é realizada usando o console ADSI do MMC do ADAM, disponível no menu Iniciar do **ADAM**. Na primeira vez que você executar o console ADSI do ADAM, será necessário se conectar à partição criada.

Procedimento

1. Clique com o botão direito do mouse no item **Editar ADSI do ADAM** no quadro esquerdo.
2. Atribua um nome à nova conexão e atualize os campos de nome e porta do servidor com as informações usadas quando você criou a instância.
3. Selecione o **nome diferenciado** ou o **contexto de nomenclatura** e especifique o nome diferenciado da partição da aplicação criada anteriormente.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

É possível se conectar às partições *Configuração e esquema* para obter opções de configuração avançadas.
Agora, deve ser possível ver a partição e os contêineres-padrão para LostAndFound, Cotas de NTDS e Funções. O contêiner Funções ainda não foi configurado.

Informações relacionadas

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

Criação de contêineres e unidades organizacionais para o ADAM

Agrupe logicamente objetos armazenados no ADAM em contêineres e em OUs (organizational units, unidades organizacionais), assim como no Active Directory.

Antes de Iniciar

Função necessária: admin

Procedimento

1. Clique com o botão direito do mouse na partição raiz e navegue até **Novo** > **Objeto** > **Unidade organizacional**.

   Nota: Também é possível exibir a lista de outros objetos disponíveis. Essa lista varia de acordo com as extensões de esquema instaladas quando os arquivos LDF foram importados.

2. Quando um valor for solicitado, insira o nome da OU, por exemplo, `Usuários`.
   A tela exibe um botão **Mais atributos**.
3. Use o botão para atribuir valores a atributos adicionais.
   Nenhum valor adicional é necessário para OUs e contêineres.
   Depois que você criar OUs, as novas OUs serão listadas como secundárias do objeto raiz.

Informações relacionadas

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

Delegação com ADAM

Depois que a estrutura da OU for criada, defina as delegações de permissão para proteger corretamente os objetos para usuários limitados.

Assim como no Active Directory, há duas maneiras gerais de conceder permissões:

- Adicione usuários a um grupo que já tenha as permissões apropriadas atribuídas.
- Defina novas permissões nos objetos do ADAM.

Para essa tarefa, discutiremos as permissões de nível de objeto. Consulte a seção Administração de grupo para obter informações sobre associações de grupo.

Como não temos um console de Usuários e computadores para o ADAM, todas as permissões de nível de objeto são definidas usando o utilitário do Active Directory *DSACLS.exe*. Este arquivo está localizado no diretório do programa do ADAM. Ao executar os utilitários do ADAM, é melhor iniciar o Prompt de comando das ferramentas do ADAM. Isso garante o uso das versões apropriadas das ferramentas. O DSALCS é usado para exibir e definir direitos de acesso a objetos.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exemplo: "`dsacls \\localhost:50010\dc=myCompany,dc=adam`" exibe as permissões atribuídas à raiz da partição *dc=myCompany,dc=adam* em execução no localhost, porta 50010. DSACLS é uma ferramenta complexa usada para criar delegação complexa. Execute *"DSACLS /?"* para observação de uso.

Informações relacionadas

- Criação de contêineres e unidades organizacionais para o ADAM
- Uso do ADAMSync para preencher o ADAM
- http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

Preenchimento de objetos do ADAM

Os objetos do ADAM incluem Objetos do usuário, Objetos userProxy e Objetos de grupo.

Objetos do usuário

Usuários podem ser criados usando o console do ADAM ADSI Edit, assim como fizemos para a criação da OU. Os usuários também podem ser administrados usando ferramentas de linha de comando do AD, que está além do escopo deste documento. O único atributo obrigatório para novos objetos de usuário é o *cn*, que é um nome curto ou o nome completo do usuário. Há também uma ampla variedade de atributos opcionais semelhantes aos atributos do usuário do Active Directory. É possível acessar a lista completa de atributos selecionando propriedades do objeto de usuário.

Objetos userProxy

Para a integração LDAP ServiceNow, recomendamos o uso de objetos *userProxy* no ADAM, o que cria uma conta de proxy vinculada à conta de usuário relacionada do AD. Isso permite que o ADAM autentique as credenciais de logon usando nomes de usuário e senhas do AD do domínio sem que ServiceNow se conecte diretamente ao controlador de domínio. Os objetos *userProxy* são muito semelhantes aos objetos do AD e do usuário do ADAM, exceto por não armazenar senhas e conter um atributo *objectSID* que contém o SID do objeto de usuário do AD vinculado. É assim que o proxy funciona. Os objetos *userProxy* são criados usando o console do *ADSIEdit* ou as ferramentas de linha de comando, mas isso pode ser entediante. Recomendamos que você use um processo automatizado conforme definido abaixo.

Objetos de grupo

Grupos são criados usando o console do ADSIEdit e ferramentas de linha de comando do AD. Os conceitos de grupo são semelhantes ao AD e são usados para integrar grupos e membros para ServiceNow. A maior diferença é que os grupos do ADAM podem conter membros do ADAM ou de domínios confiáveis do AD.

Automatizar a criação de objetos do ADAM

Se você estiver interessado em sincronizar as contas do Active Directory com o ADAM, recomendamos o uso da ferramenta Microsoft *ADAMSync*. Este é o uso mais comum do ADAM para ServiceNow integração LDAP.

Sobre a delegação de permissões

O ADAM contém alguns grupos internos com permissões-padrão. Esses grupos são encontrados no contêiner *cn=roles,dc=myCompany,dc=adam*. Eles são semelhantes aos grupos de nível de domínio e contém direitos para objetos na partição atual. Semelhante

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

ao AD Forests, também é possível definir um nível mais alto de permissões usando os grupos-padrão em *cn=roles,cn=configuration,dc=myCompany,dc=adam*. Você deve se conectar à partição de configuração no *ADSIEdit*. Por padrão, o grupo Administradores inclui a conta especificada durante a configuração. Este membro nem sempre está visível porque é herdado por meio de grupos de configuração. Os administradores têm controle total sobre todos os objetos de partição. O grupo Leitores não contém membros por padrão e tem acesso de leitura a todos os objetos na partição. O grupo Usuários é um grupo dinâmico, assim como no Active Directory. Ele inclui, transitivamente, todos os usuários do ADAM criados na partição.

Informações relacionadas

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

Teste e solução de problemas de configuração do ADAM

A principal ferramenta usada para testes é o LDP. Isso permite que um teste completo da autenticação de usuário seja realizado.

A maior parte do gerenciamento de objetos pode ser concluída usando o console do ADAM ADSI Edit, que fornecerá acesso a toda a coleção de objetos e atributos. O nível mais alto de controle e solução de problemas dos serviços do ADAM é usar o serviço Windows criado durante a configuração da instância. O nome do serviço varia e depende do nome da instância criada. Este serviço deve estar em execução para que o serviço do ADAM seja executado. Se problemas de conexão estiverem ocorrendo, revise as configurações de rede para garantir que você tenha o acesso de rede apropriado para se conectar ao servidor e à porta ADAM. Um log de eventos do Windows é criado para cada instância do ADAM instalada. Essa também é uma ferramenta ideal para solucionar problemas de serviços do ADAM.

O Windows Log de eventos de segurança também é útil na solução de problemas de autenticação de *userProxy*. Todas as tentativas de logon de *userProxy* são registradas no log de segurança e fazem referência ao endereço do dispositivo do cliente remoto, ao nome diferenciado do usuário que está tentando fazer logon e ao código de status ou resultado.

Informações relacionadas

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

Backup e recuperação com o ADAM

É possível fazer backup de todos os dados do ADAM usando métodos de backup do sistema de arquivos padrão.

Redundância

O ADAM tem utilitários de replicação internos com base na mesma tecnologia do AD. Uma réplica de leitura e gravação completa de uma partição do ADAM pode existir no mesmo computador ou em outro. É possível usar esta réplica de várias maneiras para fornecer uma integração LDAP tolerante a falhas com a instância. Uma opção é expor ambas as partições à instância por meio do firewall e definir ambos os servidores no campo de servidor Propriedades LDAP.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Informações relacionadas

Modo de aplicação do Active Directory (ADAM)

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

Uso de LDAPS com ADAM

A configuração-padrão para autenticação de objeto *userProxy* é impor comunicações LDAPS (LDAP seguro). O LDAPS requer certificados SSL para proteger o tráfego da rede.

Para remover este requisito, faça a seguinte mudança usando o console *ADSIEdit* conectado à partição de configuração.

```
Object: CN=Directory Service, CN=Windows NT, CN=Services,
 CN=Configuration
Attribute: msDS-Other-Setings
Value: change RequiresSecureProxyBind from 1 (enforced) to 0 (disabled)
```

Reinicie o serviço do ADAM para usar a nova configuração.

Para oferecer suporte a vinculações seguras e criptografar as informações de usuário e senha que estão sendo transmitidas, um certificado SSL deve ser instalado no servidor e em qualquer cliente LDAP. Como há usos limitados e controlados para o serviço do ADAM, é viável usar um certificado autoassinado que atenderia às necessidades sem incorrer em custos de certificação ou criar uma infraestrutura de autoridade de certificação (CA). Se você já tiver uma CA, poderá emitir um certificado. Caso contrário, crie um certificado autoassinado.

Criação de um certificado autoassinado

Para usar o utilitário *selfssl*, o Serviço de informações da Internet (IIS) deve estar instalado. Este serviço pode ser removido depois que o certificado for gerado. É possível obter o utilitário selfssl.exe no IIS Resource Kit. Se o IIS já estiver instalado, crie um novo site para que os sites atuais não sejam afetados durante a geração do certificado. Selfssl precisa anexar temporariamente o novo certificado emitido por conta própria a um site válido.

Selfssl é uma ferramenta de linha de comando e tem os seguintes parâmetros comuns.

Descrições dos parâmetros selfssl

Parâmetro	Descrição
/T	Adiciona o certificado aos "Certificados confiáveis" na máquina local
/N:cn	Define o nome comum do certificado. Ele deve corresponder ao nome do domínio totalmente qualificado do servidor que executa o serviço Web usando o certificado
/K	Define a força do tamanho da chave em bits
/V	Número de dias pelos quais o certificado é válido
/S	ID do site ao qual o certificado será anexado
/P	Porta IP do serviço Web

O atributo de nome comum deve corresponder ao nome ou endereço externo usado pela instância para se conectar ao computador ADAM. Será necessário obter a ID do site do site do IIS, a menos que o site-padrão, que é 1, esteja em uso e não precise ser definido no

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

comando selfssl. Um exemplo de comando para gerar um certificado para myCompany seria:

```
selfssl /N:CN=myCompany.externaldomain.com /K:1024 /V:3650 /S:12345 /
P:50001 /T
```

Esta declaração cria um certificado válido por 10 anos. Defina o valor com qualquer duração, mas esteja ciente de que o novo certificado deve ser gerado e enviado para a instância antes que o antigo expire. Recomendamos anotar a data de vencimento no certificado.

Depois que o certificado for gerado, será possível removê-lo do site ou excluir o site por completo caso um site temporário tenha sido criado.

Informações relacionadas

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

Atribuir o certificado ao ADAM

Instale um certificado SSL no servidor e em qualquer cliente LDAP para oferecer suporte a vinculações seguras e criptografar as informações de usuário e senha que estão sendo transmitidas.

Antes de Iniciar

Função necessária: admin

Por Que e Quando Desempenhar Esta Tarefa

Como há usos limitados e controlados para o serviço do ADAM, é viável usar um certificado autoassinado para atender às suas necessidades sem incorrer em custos de certificação ou criar uma infraestrutura de CA (Certificate Authority, autoridade de certificação).

Procedimento

1. Abra o console do MMC de certificados e crie duas conexões de console, uma para Certificados de computador local e outra para Certificados de serviços de computador local no novo serviço do ADAM.
   O novo certificado pode ser encontrado em `Certificados (computador local)\Pessoal\Certificados`.
2. Copie o certificado para o contêiner do serviço do ADAM, `Certificados – Serviço (nome do serviço do ADAM)\Nome do serviço ADAM_ADAM\Certificados raiz confiáveis\Certificados` e copie o certificado para `Certificados – Serviço (nome do serviço do ADAM)\Nome do serviço ADAM_ADAM\Pessoal\Certificados`.
3. Abra a guia de detalhes no certificado que você copiou, observe o carimbo de data Válido desde e atribua acesso de leitura ao arquivo de chave do certificado.
   Vá para `C:\Documents and Settings\All Users\Application Data\Microsoft\Crypto\RSA\MachineKeys` e identifique o certificado com o carimbo de data/hora correspondente. Atribua direitos de leitura e execução à conta de serviço que executa o ADAM. Por padrão, este é o **Serviço de rede**.
4. Reinicie o serviço do ADAM para ativar o novo certificado.

Informações relacionadas

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exportar o certificado de chave pública

Os clientes LDAPS, incluindo a instância, precisam do certificado de chave pública para fazer uma conexão segura com o ADAM.

Antes de Iniciar
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa
Nos consoles de certificação do servidor usados acima, exporte uma chave pública para ser usada pelos clientes.

Procedimento
1. Selecione o certificado, clique com o botão direito e selecione **todas as tarefas/exportar**. Não exporte a chave privada. Selecione o formato X.509 binário codificado por DER padrão e especifique o nome do arquivo de exportação.
2. Instale o certificado público nos clientes LDAP que se conectam ao servidor usando LDAPS.
   Quando solicitado, adicione o certificado ao armazenamento de *autoridades de certificação raiz*.

Informações relacionadas

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

Conta de acesso ao modo de aplicação do Active Directory (ADAM)

O sistema requer uma conta de usuário para ler as informações do objeto do modo de aplicação do Active Directory (ADAM) que são importadas para a instância da aplicação.

Crie a conta usando um dos seguintes métodos:

- Crie uma conta de usuário local do ADAM, atribua uma senha e permissões.
- Atribua permissões a uma conta de domínio Windows na partição do ADAM.
- Use uma conta *userProxy*.

Ao usar o ADAM como uma origem LDAP, é preciso especificar o nome diferenciado totalmente qualificado (FQDN) da conta do ADAM no campo **Nome distinto de login** do servidor LDAP.

Informações relacionadas

Modo de aplicação do Active Directory (ADAM)

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

Testar as conexões LDAPS

Teste as conexões LDAPS. Há duas conexões de console, uma para Certificados de computador local e outra para Certificados de serviços de computador local no novo serviço do ADAM.

Antes de Iniciar
Função necessária: administrador

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Execute *LDP.exe* da pasta de instalação do ADAM `c:\windows\adam`.
   Verifique se a versão do ADAM está selecionada, uma vez que este não é o cliente LDP padrão Windows .
2. Abra uma nova conexão usando o menu **Conexão/conectar**.
   O nome do servidor deve corresponder ao CN atribuído ao certificado.
3. Insira a **porta LDAPS** e marque a caixa de seleção **SSL**.
   Os resultados de uma conexão bem-sucedida são algumas informações gerais do servidor e nenhum erro.
4. Vincular (fazer login) ao serviço.
   Para replicar conexões de cliente LDAP típicas, selecione a opção de vinculação Simples.
   Insira um usuário do ADAM ou nome diferenciado do *userProxy* no campo de usuário e senha associada.
   Se você vir uma mensagem de retorno informando "Autenticado como: ..." sua conexão usando o LDAPS terá sido bem-sucedida.

Informações relacionadas

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

Uso do ADAMSync para preencher o ADAM

Os administradores usam o MS ADAMSync para preencher os diretórios LDAP que usam o MS ADAM.

Nota:

Este documento pressupõe que você tenha pelo menos um nível básico de conhecimento com o Microsoft Windows Server, Active Directory e ADAM e que já tenha uma instância funcional Modo de aplicação do Active Directory (ADAM) com uma partição.

Estes são procedimentos de amostra. Devido à complexidade e ao fato de ele estar sendo executado no seu ambiente, não é possível oferecer suporte direto. Recomendamos que, caso tenha problemas, você trabalhe com Microsoft ou um consultor Microsoft.

Depois que o ADAM tiver sido instalado e a primeira partição tiver sido criada, será possível preenchê-lo com objetos.

As seguintes opções estão disponíveis:

- Criação manual de objetos usando GUI ou scripts. Esta opção é ineficiente e lenta.
- Integre com o Active Directory usando o Microsoft Integration Information Server. Esta opção fornece mais flexibilidade e funcionalidade, mas requer algumas configurações avançadas. Uma versão gratuita do MIIS compatível com o Active Directory, ADAM eMicrosoft listas de endereços globais do Exchange está disponível. A menos que você já tenha experiência com MIIS, é aconselhável não tentar implementar um novo ambiente exclusivo para integração LDAP.
- Use o ADAMSync, uma ferramenta de sincronização fornecida por Microsoft com o ADAM. Esta é a opção explicada.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Defina contas de usuário do ADAM

Defina as contas de usuário no ADAM. Uma conta de usuário é usada para a conexão da instância, e a outra conta de usuário é para o ADAMSync.

Antes de Iniciar
Função necessária: admin

Por Que e Quando Desempenhar Esta Tarefa
Essas contas podem ser objetos de usuário do ADAM local, objetos userProxy ou uma conta do Windows de um domínio confiável.

A conta *ADAM User* requer acesso somente leitura à estrutura de diretórios a ser importada para sua instância. A melhor maneira de fazer isso é adicionar a conta ao atributo de membro no grupo Leitores encontrado em cn=roles,dc=myCompany,dc=adam.

As novas contas de usuário do ADAM são desabilitadas por padrão. Será preciso habilitar as novas contas e definir uma senha.

Procedimento

1. Habilite os usuários alterando o atributo msDS-UserAccountDisabled para FALSO.
2. Clique com o botão direito do mouse no objeto do usuário e redefina a senha.
3. Teste as novas contas usando o LDP conforme definido no Modo de aplicação do Active Directory (ADAM) para se certificar de que elas possam se conectar.
   Use a opção **LDAP** > **Exibição/árvore**, deixando o DN de base em branco para garantir que seja possível exibir os objetos no diretório usando as novas contas. A configuração, o esquema e a partição do domínio devem estar visíveis no painel esquerdo. Percorra a partição de domínio. Se uma nova conta do ADAM local estiver em uso, a informação "Nenhum secundário" será exibida, indicando que você não tem acesso de leitura aos objetos. Verifique as associações do grupo de configuração e teste novamente.

   O ADAMSync usa a conta *ADAMSync User* para gerenciar objetos na partição do ADAM. Esta conta requer direitos de nível de administrador, uma vez que criará, atualizará e excluirá objetos do ADAM.

   O ADAMSync usa a conta *ADAMSync AD* para ler os objetos do AD que serão sincronizados com o ADAM.

Configure o ADAMSync

O ADAMSync está incluso no Windows Server 2003 R2. Baixe e instale o ADAMSync se estiver usando um sistema operacional diferente.

Como estender o esquema

O esquema do ADAM precisa ser estendido para oferecer suporte ao ADAMSync.

1. Execute o seguinte comando em c:\windows\adam para importar as extensões do esquema do ADAMSync. Se o usuário atual não tiver acesso, poderá ser necessário mudar o server:port e adicionar credenciais. Consulte o arquivo AdamSyncMetadata.ldf para obter detalhes.

```
ldifde -i -f MS-AdamSyncMetadata.LDF -s localhost:50000 -j . -c
 "cn=Configuration,dc=X" #configurationNamingContext
```

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

2. Faça o mesmo com MS-AdamSchemaW2k3.ldf para oferecer suporte a atributos do Windows 2003.

```
ldifde -i -u -f MS-AdamSchemaW2K3.LDF -s localhost:50000 -j . -c
 "cn=Configuration,dc=X" #configurationNamingContext
```

Mudanças de esquema recomendadas

Estas são algumas mudanças de esquema adicionais recomendáveis.

1. Abra um novo console do MMC e adicione o Snap-in de esquema do ADAM.
2. Conecte-se à instância do ADAM.
3. Expanda a pasta Classes, localize a classe userProxy e abra **Propriedades**.
4. Verifique os seguintes atributos opcionais na guia Atributos, adicione qualquer um que ainda não exista.
   - empresa
   - departamento
   - givenNane
   - mail
   - physicalDeliveryOfficeName
   - sAMAccountName
   - sn
   - telephoneNumber
   - título
   - userAccountControl
   - userPrincipalName
5. Reinicie o serviço ADAM para habilitar as novas configurações.

Instalação do arquivo de configuração do ADAM

Instale o arquivo de configuração do ADAM por meio da linha de comando do Windows.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Instale o arquivo de configuração.

```
C:\WINDOWS\adam>adamsync /install localhost:50000
MS-AdamSyncConf-SNC.XML
```

2. Execute o arquivo de sincronização a ser registrado no console.

```
C:\WINDOWS\adam>adamsync /sync localhost:50000
"ou=users,dc=service-now,dc=adam" /log -
```

3. Revise os resultados usando o console do ADSIEdit.
   Verifique os novos objetos e atributos que foram criados pelo ADAMSync.
4. Execute o ldap para testar a autenticação userProxy.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Automatização do processo de sincronização

Configure o processo de sincronização como uma Tarefa programada Windows. É preciso fornecer as credenciais no arquivo de configuração, na linha de comando, ou executar a tarefa programada com uma conta que tenha acesso.

Observações especiais

- É possível criar vários arquivos de configuração e trabalhos agendados para sincronizar o ADAM a partir de várias fontes.

  Este exemplo importa o atributo sAMAccountName, que pode ser usado como logon da aplicação. Para sincronizar a origem, será preciso ter certeza de que tem um valor de atributo exclusivo que pode ser usado para as credenciais de logon. sAMAccountName certamente será exclusivo em um domínio, mas não em vários domínios.

- Se o Microsoft Exchange estiver em uso, recomendamos a exclusão dos objetos cn=SystemMailbox* como parte da configuração de filtro de objeto.

Exemplo de arquivos de configuração do ADAM

Todas as configurações do ADAMSync são armazenadas em arquivos xml.

Arquivo de configuração padrão com comentários

Há um arquivo de configuração padrão chamado MS-AdamSyncConf.xml incluso na instalação do ADAMSync. Faça uma cópia desse arquivo para ter um exemplo base para consultar no futuro. Este exemplo é o arquivo de configuração padrão com comentários adicionados.

```
<?xml version="1.0"?>
<doc>
 <configuration>
<!-- Sync File Description -->
<description>MyCompany ADAMSync Configuration</description>
  <security-mode>object</security-mode>;
<!-- source-ad-name = fqdn of the domain controller -->;

 <source-ad-
name>;fully.qualified.domain.name.of.domain.controller</source-ad-name>;
<!-- source-ad-partition = root AD domain partition -->;
  <source-ad-partition>;dc=myCompany,dc=com</source-ad-partition>;
<!-- source-ad-account = use this to specify an account to connect to AD
 -->;
<!-- if not used, the current user will be used  -->;
  <source-ad-account>;</source-ad-account>;
  <account-domain>;</account-domain>;
<!-- target-dn = target ADAM OU -->;
  <target-dn>;ou=servicenow users,dc=myCompany,dc=adam</target-dn>;
  <query>;
<!-- base-dn = should be the root AD partition if you want all users -->;
   <base-dn>;dc=myCompany,dc=com</base-dn>;
<!-- object-filter = standard ldap query format, this will grab all users
 -->;
<!-- need to review results to see if you should modify this filter -->;
   <object-filter>;(objectCategory=person)</object-filter>;
   <attributes>;
```

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

```
<!-- include=userproxy requires objectSID to link back to the AD account
 -->;
    <include>;objectSID</include>;
    <include>;givenName</include>;
    <include>;sn</include>;
    <include>;description</include>;
    <include>;title</include>;
    <include>;company</include>;
    <include>;department</include>;
    <include>;mail</include>;
    <include>;physicalDeliveryOfficeName</include>;
    <include>;telephoneNumber</include>;
    <include>;sAMAccountName</include>;
   </attributes>;
  </query>;
<!-- map for user-to-userproxy object types -->;
  <user-proxy>;
    <source-object-class>;user</source-object-class>;
    <target-object-class>;userProxy</target-object-class>;
  </user-proxy>;
  <schedule>;
   <aging>;
    <frequency>;0</frequency>;
    <num-objects>;0</num-objects>;
   </aging>;
   <schtasks-cmd>;</schtasks-cmd>;
  </schedule>;
 </configuration>;
 <synchronizer-state>;
  <dirsync-cookie>;</dirsync-cookie>;
  <status>;</status>;
  <authoritative-adam-instance>;</authoritative-adam-instance>;
  <configuration-file-guid>;</configuration-file-guid>;
  <last-sync-attempt-time>;</last-sync-attempt-time>;
  <last-sync-success-time>;</last-sync-success-time>;
  <last-sync-error-time>;</last-sync-error-time>;
  <last-sync-error-string>;</last-sync-error-string>;
  <consecutive-sync-failures>;</consecutive-sync-failures>;
  <user-credentials>;</user-credentials>;
  <runs-since-last-object-update>;</runs-since-last-object-update>;
  <runs-since-last-full-sync>;</runs-since-last-full-sync>;
 </synchronizer-state>;
</doc>;
```

Arquivo de configuração de filtros LDAP

É possível fornecer qualquer nível de filtragem no valor do filtro de objeto no arquivo de configuração. Use a sintaxe de consulta LDAP padrão com os seguintes caracteres de escape xml em vez dos operadores padrão.

- E = "&" substituir por &
- OU = "|" (linha vertical) substituir por |
- NÃO = "!" substituir por !

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Arquivo de configuração de referência

Este é um arquivo de configuração real que pode ser consultado como uma amostra.

```
<?xml version="1.0"?>;
<doc>;
 <configuration>;
<description>;SNCTest ADAMSync Configuration</description>;
  <security-mode>;object</security-mode>;
  <source-ad-name>;domaincontroller.service-now.com</source-ad-name>;
  <source-ad-partition>;dc=service-now,dc=com</source-ad-partition>;
  <source-ad-account>;</source-ad-account>;
  <account-domain>;</account-domain>;
  <target-dn>;ou=servicenow users,dc=service-now,dc=adam</target-dn>;
  <query>;
   <base-dn>;dc=service-now,dc=com</base-dn>;
   <object-filter>;(objectCategory=person)</object-filter>;
   <attributes>;
    <include>;objectSID</include>;
    <include>;givenName</include>;
    <include>;sn</include>;
    <include>;description</include>;
    <include>;title</include>;
    <include>;company</include>;
    <include>;department</include>;
    <include>;mail</include>;
    <include>;physicalDeliveryOfficeName</include>;
    <include>;telephoneNumber</include>;
    <include>;userAccountControl</include>;
   </attributes>;
  </query>;
  <user-proxy>;
    <source-object-class>;user</source-object-class>;
    <target-object-class>;userProxy</target-object-class>;
  </user-proxy>;
  <schedule>;
   <aging>;
    <frequency>;0</frequency>;
    <num-objects>;0</num-objects>;
   </aging>;
   <schtasks-cmd>;</schtasks-cmd>;
  </schedule>;
 </configuration>;
 <synchronizer-state>;
  <dirsync-cookie>;</dirsync-cookie>;
  <status>;</status>;
  <authoritative-adam-instance>;</authoritative-adam-instance>;
  <configuration-file-guid>;</configuration-file-guid>;
  <last-sync-attempt-time>;</last-sync-attempt-time>;
  <last-sync-success-time>;</last-sync-success-time>;
  <last-sync-error-time>;</last-sync-error-time>;
  <last-sync-error-string>;</last-sync-error-string>;
  <consecutive-sync-failures>;</consecutive-sync-failures>;
  <user-credentials>;</user-credentials>;
  <runs-since-last-object-update>;</runs-since-last-object-update>;
  <runs-since-last-full-sync>;</runs-since-last-full-sync>;
 </synchronizer-state>;
```

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

```
</doc>;
```

Configuração do Microsoft Active Directory para comunicação segura de LDAPS

Use pares de certificados para habilitar as comunicações de LDAPS do Microsoft Active Directory (AD).

Nota: Esses procedimentos foram projetados e testados usando o Windows 2003 R2 Standard Edition e funcionam com todas as versões do Windows 2003.

A comunicação de LDAP segura (LDAPS) é semelhante à comunicação SSL (HTTPS), em que ambos criptografam os dados entre servidores e clientes. Para fazer isso, servidor e clientes compartilham informações comuns usando pares de certificados. O servidor contém o certificado de chave privada, e os clientes têm o certificado de chave pública. Esses certificados são necessários para habilitar as comunicações LDAPS do Microsoft Active Directory (AD).

Para configurar o LDAPS para o Active Directory:

- Certifique-se de que o domínio do Active Directory esteja configurado e que a instância seja capaz de se conectar ao servidor do Active Directory por meio do firewall.
- Verifique se há uma autoridade de certificação (CA) que possa emitir um certificado para o controlador de domínio (DC). Duas opções estão disponíveis caso você ainda não tenha uma infraestrutura de CA.
  - Configure uma CA autônoma para emitir o certificado
  - Solicite um certificado de terceiros
- Se você já tiver uma CA, poderá gerar um certificado a partir de uma CA interna.

Todos os certificados têm uma data de expiração definida, que pode ser exibida nas propriedades do certificado. Se o certificado expirar, todo o tráfego de LDAPS falhará, e os usuários não poderão mais fazer login na instância. Para resolver isso, um novo certificado deve ser emitido e instalado em sua instância.

Por padrão, os certificados de CA da Microsoft expiram em um ano. Certificados de CA externa geralmente são adquiridos em incrementos de um ano. Marque a data de expiração do seu certificado ou use a função de notificação de expiração da aplicação (localizada em **Certificados** > **LDAP do sistema**). Certifique-se de providenciar um novo certificado antes que o antigo expire. Isso fornecerá tempo para que o novo certificado seja instalado e testado antes que o antigo expire.

Configuração de uma autoridade de certificação independente para o Active Directory

A primeira etapa para configurar o Microsoft Active Directory para acesso SSL é configurar uma autoridade de certificação (CA) autônoma.

Antes de Iniciar
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa
Não se preocupe com a adição da utilização de recursos porque ambos os serviços necessários (IIS e CA) podem ser desabilitados após a emissão do(s) certificado(s).

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Instale o Servidor de informações da Internet (IIS).
2. Instale os serviços de autoridade de certificação no modo autônomo.
3. Verifique se a aplicação da Web de serviços de certificação está instalada e ativa.

O que Fazer Depois

Usando o console do gerente do IIS, expanda o computador local e selecione *Sites*. O estado do **Site-padrão** deve ser *Executando*. Uma aplicação *CertSrv* também deve estar listada na opção **Site-padrão**. Se o site não estiver em execução ou a aplicação estiver ausente, será necessário resolver o problema antes de prosseguir.

Como gerar um certificado de uma autoridade de certificação interna

Ao configurar o Microsoft Active Directory para acesso SSL, é preciso gerar um certificado interno e solicitar o certificado externo.

Antes de Iniciar

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

Essas etapas se aplicam aos serviços de CA da Microsoft. Se estiver usando uma plataforma interna de CA diferente, consulte o administrador de CA local para obter assistência.

Procedimento

1. No controlador de domínio (DC) para o qual você deseja criar um certificado, navegue até `http://localhost/certsrv` ou especifique o nome do servidor CA se estiver em um servidor remoto.
2. Na página de boas-vindas, clique em **Solicitar um certificado** e selecione *Solicitação de certificado avançado*.
3. Na página Solicitação de certificado avançado, selecione **Criar** e envie uma solicitação para esta CA.
4. Conclua a solicitação de certificado avançado da seguinte forma:

Campos de solicitação de certificado avançado

Campo	Entrada
Nome	O nome do domínio totalmente qualificado (FQDN) do DC que está solicitando o certificado.
E-mail	O endereço de e-mail da pessoa responsável pela certificação.
Empresa	Nome de sua empresa.
Configurações de opções de chave	
Criar novo conjunto de chaves	Selecione.
CSR	Provedor de criptografia do Microsoft RSA SChannel.
Uso de chave	Exchange.
Tamanho da chave	Recomendamos 1024. A instância oferece suporte a até 2048.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Entrada
Nome do recipiente de chave automático	Selecione.
Armazene certificados no armazenamento de certificados do computador local	Selecione.

5. Clique em **Enviar**.
   Você será direcionado para uma página que fornece sua **ID de solicitação**. Anote essa ID.
6. Para processar a solicitação pendente, conclua as seguintes etapas:
   a. Abra o console de gerenciamento da autoridade de certificação.
   b. Expanda o nó do servidor e selecione **Solicitações pendentes**.
   c. Localize a ID da solicitação que acabou de enviar, clique com o botão direito e selecione *Todas as tarefas/problemas na aprovação da solicitação e emissão do certificado*.
7. Para recuperar o certificado emitido:
   a. No DC para o qual você fez a solicitação, navegue até `http://localhost/certsrv`ou especifique o nome do servidor CA se estiver em um servidor remoto.
   b. Selecione `Exibir o status de uma solicitação de certificação pendente`.
   c. Selecione o link para o novo certificado.
   d. Selecione o link para **Instalar este certificado**.

O que Fazer Depois

É necessário solicitar um certificado de terceiros. Certificados de CAs externas podem ser adquiridos por apenas $ 30 ao ano. Para obter informações de procedimentos detalhados sobre como solicitar um certificado de uma CA externa, consulte o artigo 321051 da Microsoft. Depois que o certificado for recebido, instalado e testado, siga o procedimento de exportação.

Testar a conectividade de LDAPS localmente

Teste a conectividade de LDAPS depois de instalar os certificados internos e de terceiros ao configurar o Microsoft Active Directory para acesso SSL.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Certifique-se de que as ferramentas de suporte do Windows estejam instaladas no controlador de domínio (DC).
   A configuração das ferramentas de suporte (suptools.msi) pode ser encontrada no diretório `\Suporte\Ferramentas` no CD do Windows Server.
2. Navegue até **Iniciar** > **Todos os programas** > **Ferramentas de suporte do Windows** > **Prompt de comando**.
   Na linha de comando, digite `ldp` para iniciar a ferramenta.
3. Na janela do *ldp*, selecione **Conexão** > **Conectar** e forneça o FQDN local e o número da porta (636).

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Selecione também o *SSL*.
Se tudo correr como esperado, uma janela exibirá e listará as informações relacionadas à conexão SSL do Active Directory. Se a conexão for malsucedida, tente reiniciar o sistema e repetir este procedimento.

Exportação do certificado de chave pública para confiar no certificado LDAP

Exporte o certificado de chave pública e importe-o para a aplicação ao configurar o Microsoft Active Directory para acesso SSL.

Antes de Iniciar
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa
Se sua autoridade de certificação não for um fornecedor de terceiros confiável, será necessário exportar o certificado da CA de emissão para que seja possível confiar nela e, por associação, confiar no certificado do servidor LDAP. Para usuários dos serviços de certificação MS, é possível exibir o caminho do certificado no console usado para a exportação. Selecione a guia **Caminho do certificado**. É necessário exportar todos os certificados na cadeia. O certificado da CA pode ser encontrado na mesma pasta do certificado LDAP ao pesquisar pelo nome no Caminho do certificado. Envie todos os certificados a serem importados para sua instância.

Procedimento

1. Em um console do MMC atual ou novo, adicione o snap-in Certificado (computador local).
2. Abra a pasta `Pessoal/certificados`.
3. Localize o novo certificado.
   A coluna "Emitido para" mostra o FQDN do controlador de domínio.
4. Clique com o botão direito do mouse no certificado e selecione *Todas as tarefas/ exportar*.
5. Exporte para o formato DER ou Base-64.
   Nomeie o arquivo usando o formato `MyCompany.cer`. Este é o certificado de chave pública a ser usado na instância para a comunicação segura com o controlador de domínio.
6. Teste o LDAPS localmente antes de enviar o certificado para a instância.

O que Fazer Depois
Depois de concluir este procedimento, importe o certificado de chave pública para a aplicação.
Consulte Instalação do certificado SSL LDAP X.509 para carregar o certificado na aplicação.

Uso do catálogo global de LDAP

Um DC pode receber a função de Catálogo global (GC). A função de Catálogo global (GC) é um diretório compatível com LDAP que consiste em uma representação parcial de cada objeto de cada domínio em uma floresta.

Os administradores configuram o Active Directory para hospedar informações de diretório do protocolo LDAP usando um dos seguintes métodos de hospedagem.

- O método comum de hospedagem de informações do diretório LDAP é usar o LDAP padrão ou LDAPS (LDAP seguro) nas portas 389 ou 636. Essas portas de LDAP padrão sempre existem em um controlador de domínio (DC) e raramente são alteradas. Acessar esta partição de diretório fornece acesso a todos os objetos no domínio que está

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

hospedado no DC. Não há como acessar objetos de outros domínios usando este método.

- Um DC também pode receber a função de Catálogo global (GC). A função de Catálogo global (GC) é um diretório compatível com LDAP que consiste em uma representação parcial de cada objeto de cada domínio na floresta. Este diretório LDAP pode ser acessado na porta 3268, com o LDAPS na porta 3269. Os requisitos de certificação das portas LDAPS e LDAP padrão são os mesmos.

Dependências de LDAP do Catálogo global

- O controlador de domínio ao qual sua instância se conecta deve ter a função de Catálogo global habilitada.
- As regras de firewall devem permitir o tráfego de entrada para o controlador de domínio na porta 3268 (LDAP) ou 3269 (LDAPS).

Observações especiais

- Nem todos os atributos são replicados para a partição do GC. Atributos comuns, como nome, sobrenome, e-mail, número de telefone, descrição e endereço, estão incluídos. Atributos adicionais podem ser adicionados ao GC, mas devem ser limitados para minimizar o impacto sobre o tráfego de replicação da floresta.
- As integrações de LDAP padrão geralmente usam sAMAccountName como o UserID da instância e a chave de aglutinação no mapa de importação LDAP, já que é garantido que isso seja exclusivo em um domínio. Este atributo não é mais exclusivo ao exibir uma floresta inteira de domínios. Um novo atributo exclusivo deve ser identificado como o UserID e a chave de aglutinação. Não é necessário que seja o mesmo atributo e pode variar de acordo com o design da floresta. Consulte o administrador do Active Directory. Normalmente, o userPrinicpalName é um atributo exclusivo entre domínios, podendo não ser um nome amigável para login, mas que pode ser usado para o identificador exclusivo nas importações. Um atributo comum usado para o UserID é o endereço de e-mail. Essas decisões afetam as propriedades e o mapeamento de LDAP.
- O valor usado para a chave de aglutinação no mapa de importação LDAP deve ser exclusivo e existir em todos os objetos que estão sendo importados. Se o valor não for exclusivo ou não existir, os registros incorretos serão atualizados com as mudanças.
- Se você tiver uma integração LDAP e deseja alterá-la para um GC, mude a chave de aglutinação de importação. Os novos valores de chave devem ser importados antes que seja possível alterar a chave de aglutinação.
- Se mudanças que interrompam a integração forem feitas na integração LDAP, a primeira etapa será reverter essas mudanças. Em seguida, entre em contato com Suporte e atendimento ao cliente com informações detalhadas sobre o que está tentando realizar.

Modificação secundária do esquema do OpenLDAP

Em sistemas OpenLDAP 2.3 que usam o back-bdb (back-end Berkley), os administradores fazem uma pequena modificação em seu esquema para facilitar a integração.

> ⚠ **Aviso:** A personalização descrita aqui foi desenvolvida para uso em instâncias específicas e não é compatível com Now Support. Este método é fornecido no estado em que se encontra e deve ser testado cuidadosamente antes da implementação. Publique todas as perguntas e comentários sobre esta personalização no fórum da nossa comunidade.

No OpenLDAP 2.3, o back-bdb tem suporte limitado para indexação de inequação (ordenação). Ele é implementado somente para as sintaxes generalizedTime e

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

ChangeSequenceNumber. Não há suporte para sintaxes compatíveis com substrings. Os filtros de pesquisa que contêm inequações são processados usando o índice de presença.

Recomendamos criar um atributo personalizado para essa finalidade em vez de alterar o que já está indexado ou presente no esquema (por exemplo, *servnowid*).

Modificação do esquema OpenLDAP

Modifique o esquema OpenLDAP. Essas etapas detalham uma modificação de esquema no OpenLDAP 2.3 fornecida por um de nossos clientes que os ajudou a integrá-lo à sua instância.

Antes de Iniciar

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

Aviso: A personalização descrita aqui foi desenvolvida para uso em instâncias específicas e não é compatível com Now Support. Este método é fornecido no estado em que se encontra e deve ser testado cuidadosamente antes da implementação. Publique todas as perguntas e comentários sobre esta personalização no fórum da nossa comunidade.

Para modificar o esquema do OpenLDAP para integração com a instância:

Procedimento

1. Crie um atributo personalizado

   Example

   ```
   attribute ( 1.3.6.1.4.1.3403000.2.1.8

       NAME 'servnowid'
     ORDERING caseIgnoreOrderingMatch
     EQUALITY caseIgnoreMatch
     SYNTAX '1.3.6.1.4.1.1466.115.121.1.15' )
   ```

2. Inclua o atributo no OID objectclass selecionado.

   Example

   ```
   objectclass ( 1.3.6.1.4.1.3403000.2.2.1
       NAME 'BcfUserIdentifiers' SUP top AUXILIARY
     MAY ( uniqid $ unixid $ servnowid ) )
   ```

   No OpenLDAP 2.3, é possível mudar as configurações do servidor dinamicamente, mas você pode apenas estender o esquema. Não é possível modificar ou excluir o esquema existente. Em vez de criar outra classe de objeto para este atributo na configuração dinâmica, use o arquivo de configuração estática slapd.conf.

3. Em slapd.conf, inclua a indexação para o novo atributo na seção bdb do back-end do banco de dados principal.

   Example

   ```
   database bdb (configs here) ....

   index servnowid pres
   ```

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

```
(other indexes here) .....
```

4. Como raiz, execute slapindex para indexar este atributo e torná-lo disponível nos filtros de pesquisa.
   Certifique-se de que o daemon OpenLDAP não esteja em execução ou no modo somente leitura antes de iniciar o slapindex.

Exclusões de registro do LDAP

Por padrão, a instância não exclui entradas depois que elas desaparecem do LDAP.

A exclusão de uma entrada, também conhecida como registro, também exclui todo o histórico e referências à entrada excluída.

Por exemplo, itens de configuração (ICs), acordos de ANS, licenças de software, ordens de compra e entradas do catálogo de serviços têm uma referência ao departamento e, se um departamento for excluído, a integração limpará todas as referências ao departamento. Além disso, a exclusão de um usuário resulta na perda de todo o histórico de ações do usuário.

Decida se deseja reter ou Excluir todos os registros de uma tabela de acordo com as necessidades da sua organização.

Limitar sessões simultâneas

É possível limitar o número de sessões interativas simultâneas para um usuário ou função em uma instância em todos os nós.

Explorar

Conheça os recursos e o valor comercial da limitação de sessões simultâneas.

Ativar

Entenda como ativar a limitação de sessões simultâneas.

Definir

Desabilitar

Saiba como desabilitar a limitação de sessões simultâneas.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configure a limitação de sessões simultâneas por usuário ou função.

Explorar limitação de sessões simultâneas

É possível limitar o número de sessões interativas simultâneas para um usuário ou função em uma instância em todos os nós.

As sessões interativas simultâneas se referem ao número de sessões que um usuário pode ter ativas por instância ServiceNow. Uma sessão de instância ativa ocorre com cada novo login em uma instância ServiceNow específica. Por padrão, não há limitações ao número de sessões de instância ativas que um usuário pode ter.

Na versão Jakarta, é possível limitar o número de sessões simultâneas ativas por usuário. Quando o usuário faz login após atingir o número máximo de sessões ativas, a sessão ativa mais antiga é encerrada, e uma nova sessão interativa se torna ativa. Se um usuário tentar acessar uma sessão encerrada por meio de um navegador, ele será redirecionado para a página de login.

Nota: O plug-in **Limitar sessões simultâneas** deve estar ativo para habilitar um limite máximo de sessões. Os limites são definidos por meio da propriedade glide.authenticate.max.concurrent.interactive.sessions. Um valor de limite máximo se aplica a qualquer usuário ou função que tenha a propriedade de limite ativa. Um usuário ou uma função conectada ao usuário deve ter o valor de limit_concurrent_sessions definido como verdadeiro para que o limite de sessões seja iniciado. Na versão Jakarta, esse recurso não oferece suporte a sessões criadas por meio do aplicativo para celular nativo ou de mecanismos não interativos.

Este é um caso de uso típico se o máximo de 1 sessão simultânea for definido:

1. O usuário acessa a instância inicial ServiceNow por meio do Chrome.
2. Depois que o usuário faz login com sucesso, ServiceNow cria a sessão 1 (S1) para o usuário.
3. O usuário decide iniciar outro acesso à instância ServiceNow pelo Firefox.
4. Depois que o usuário faz login com sucesso, ServiceNow cria a sessão 2 (S2) para o usuário.
5. Uma vez que o usuário tem um limite máximo de 1 sessão simultânea, a sessão S1 é invalidada quando a S2 é criada.
6. Quando retorna ao Chrome para acessar a instância S1 ServiceNow, o usuário redirecionado para a página de login, uma vez que S1 é inválido.

Os limites de sessão simultânea funcionam com todos os mecanismos de autenticação ServiceNow: SAML, LDAP e autenticação de banco de dados local. Isso também funciona com autenticação multifator e todos os mecanismos de autenticação interativos ServiceNow. A origem da sessão pode ser visualizada por meio da tabela **sys_user_session**, na coluna **Tipo**. Os valores podem ser:

- Navegador da Web
- Navegador de dispositivo móvel
- ServiceNow Aplicativo para celular
- Não interativo (SOAP, WSDL, OAuth)

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países. Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Ativação e configuração do plug-in Limitar sessões simultâneas

Você poderá ativar o plug-in Limitar sessões simultâneas (com.glide.limit.concurrent.sessions) se tiver a função de administrador.

Antes de Iniciar

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

Procedimento

1. Navegue até **Todos** > **Definição do sistema** > **Plug-ins**.
2. Encontre e clique no plug-in Limitar sessões simultâneas.
3. No formulário Plug-in do sistema, revise os detalhes do plug-in e, em seguida, clique no link relacionado **Ativar/Fazer upgrade**.
4. Clique em **Ativar**.
5. Para habilitar este recurso e definir um limite máximo de sessões simultâneas, acesse a guia **Arquivos de plug-in**, localize as seguintes propriedades e altere os valores de configuração.

Opção	Descrição
glide.authenticate.limit.concurrent.interactive.sessions	É possível habilitar a capacidade de limitar sessões simultâneas definindo o valor como **Verdadeiro**. Por padrão, esta propriedade é definida como **Falso**, o que significa que não há limite para o número de sessões interativas que um usuário pode ter ativas. **Nota:** Para desabilitar esse recurso, defina essa propriedade novamente como **Falso**.
glide.authenticate.max.concurrent.interactive.sessions	É possível definir o número máximo de sessões interativas ativas simultâneas que um usuário pode ter na instância em todos os nós.

6. Opcional: Também será possível corrigir as propriedades a seguir, se necessário.

Opção	Descrição
glide.authenticate.types.to.limit.concurrency	Esta propriedade limita os tipos de sessão. Por padrão, somente as sessões do navegador da Web têm um limite. Os tipos de sessão incluem: ◦ Navegador da Web (1) ◦ Navegador de dispositivo móvel (2) ◦ ServiceNow Aplicativo para celular (3) ◦ Não interativo (10) É possível configurar e definir o valor como "1" para navegador da Web, "2" para na-

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	vegador de dispositivo móvel ou "1,2" para ambos. **Nota:** Somente sessões do navegador de dispositivo móvel e da Web podem ter um limite. Não há limites para sessões que se originam do aplicativo para celular ServiceNow ou sessões não interativas.
glide.authenticate.limit.concurrent.sessions-.across.all.nodes	Esta propriedade restringe o limite de sessões simultâneas por nó em vez de restringi-las em todos os nós de uma instância ServiceNow. Por padrão, o valor é definido como verdadeiro, o que limita as sessões do usuário em todos os nós. Se a propriedade for definida como falsa, somente as sessões nesse nó, não as dos outros nós, estarão sujeitas à limitação.

7. Clique em **Atualizar** para que as configurações tenham efeito.

O que Fazer Depois

Definir um limite de sessão simultânea por usuário ou função.

Informações relacionadas

Lista de plug-ins (Xanadu)

Definir um limite de sessão simultânea por usuário ou função

É possível definir um limite de sessão simultânea em um usuário específico ou função específica.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Navegue até **Todos** > **Administração de usuários** > **Usuários** ou **Administração de usuários** > **Funções**.
2. Selecione um usuário ou função para o qual você deseja definir um limite de sessão simultânea, marque a caixa de seleção **Limitar sessões simultâneas** e clique em **Atualizar**. O usuário ou função tem um limite de quantas sessões simultâneas podem ser abertas de uma vez.

Desabilitar um limite de sessão simultânea por usuário ou função

É possível desabilitar um limite de sessão simultânea em um usuário específico ou função específica.

Antes de Iniciar

Função necessária: administrador

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegue até **Todos** > **Administração de usuários** > **Usuários** ou **Administração de usuários** > **Funções**.
2. Selecione um usuário ou função que deseja desabilitar um limite de sessão simultânea, desmarque a caixa de seleção **Limitar sessões simultâneas** e clique em **Atualizar**.
   O usuário ou função não está sujeito a um limite de quantas sessões simultâneas podem ser abertas ao mesmo tempo.

Autenticação local

Use a autenticação local da ServiceNow® para proteger o login dos usuários em um dispositivo local.

A autenticação local é um método de verificação da identidade de um usuário em um dispositivo local. Ela usa características ou credenciais exclusivas em posse do usuário para validar o login dele.

Use os recursos de autenticação local da ServiceNow® para acessar com segurança a instância da ServiceNow® em seus dispositivos locais.

Segurança de login e autenticação

Configure as opções de segurança de login para controlar o acesso à sua instância.

Configure sua segurança de login

Entenda como configurar a segurança de login.

Defina cenários de login

Defina cenários de login.

Redefinição de senha

Saiba mais sobre redefinições de senha de login.

Explorar segurança de login e autenticação

Configure as opções de segurança de login para controlar o acesso à sua instância.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opções de segurança

Você pode controlar vários aspectos do login do usuário e da segurança da autenticação:

Recurso	Descrição	Tópicos relacionados
Controles de login e logout	Controlar várias dimensões do processo de login e logout dos usuários, como especificar uma página principal que o usuário vê ao fazer login e controlar como os usuários fazem logout.	• Definir cenários de login • Configurar o prompt de confirmação de logout • Saídas de instalação • Especificar bloqueio para tentativas de login com falha
Segurança de autenticação	Controlar o Processo de Redefinição de senha e recursos como a opção Lembrar-me. Você também pode usar controles baseados em endereço IP para acessar a instância e implementar um nonce a ser usado com autenticação Digest de login único.	• Configurar política de senha • Redefinição de senha • Lembrar minhas informações • Autenticação baseada no intervalo de IP • Implementar um nonce

Definir cenários de login

Você pode direcionar todos os usuários para a mesma página após o login.

Antes de Iniciar

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

Quando os usuários se conectam a uma instância diretamente, por exemplo, acessando http://{instance_name}.service-now.com/, o sistema faz o seguinte:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

1. Acessa o valor na propriedade *glide.entry.page.script*. O valor padrão da propriedade é derivado de uma inclusão de script chamada *CMSEntryPage*.
2. Direciona o usuário para a página de login da instância se a página de entrada exigir um login.
3. Aplica regras de login ao usuário, se houver.

Para forçar o sistema a direcionar todos os usuários para a mesma página após o login:

Procedimento

1. Navegue até **Todos** > **Gestão de conteúdo** > **Configuração** > **Página de configuração**.
2. Selecione um valor para o campo *Página de login* ou crie uma nova página conforme desejado.

   Se esta página não for a página padrão do site, ela sempre será redirecionada para cá. Se for uma página padrão do site, ele aplicará regras de login. Se este valor for nulo, o sistema usará navpage.do como a página de entrada. Não insira uma página de login aqui; caso contrário, os usuários precisarão fazer login duas vezes.

   Fazer login em uma instância para acessar um registro:

   Quando os usuários fazem login em uma instância para acessar um registro por seu identificador exclusivo global (sys_id), como http://{instance}.service-now.com/incident.do? Sys_id = {sys_id}, o sistema faz o seguinte:

   a. Direciona o usuário para uma página de login se ainda não estiver conectado.
   b. Direciona o usuário para o registro apropriado se ele tiver permissão para acessá-lo. Se o usuário não tiver direitos de acesso ao registro, será exibida uma mensagem de negação de acesso.

   Fazer login no Portal de serviços ou em um site do CMS:

   Quando os usuários fazem login no Portal de serviços ou em um site do CMS, como http://<instance>.service-now.com/site-name/page.do, o sistema faz o seguinte:

   - Se houver um valor no campo *Página de login* no Portal de serviços ou no formulário do site do CMS, ele direcionará o usuário para essa página de login e aplicará as regras de login, se houver, ao usuário.
   - Se não houver página de login especificada, ele direcionará o usuário para o valor no campo *Página inicial* no Portal de serviços ou no formulário do site do CMS.

   Fazer login no Portal de serviços ou em um site do CMS para acessar um registro:

   Quando os usuários fazem login no Portal de serviços ou em um site do CMS para acessar um registro, como http://{instance}.service-now.com/ess/incident_detail.do?sysparm_document_key=incident, {sys_id}, o sistema segue o mesmo procedimento e, por fim, leva o usuário ao registro. Se o usuário não tiver direitos de acesso ao registro, será exibida uma mensagem de negação de acesso.

Logins e o portal de autoatendimento para funcionários

O sistema rastreia a primeira página inicial que um usuário está tentando acessar, mesmo se o usuário quiser fazer login no Portal de autoatendimento para funcionários.

Considere os seguintes cenários:

Exemplo 1:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países. Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

1. Um usuário não está conectado e tenta acessar um registro usando um ID SYS específico no URL.
2. O sistema redireciona o usuário para a página de login.
3. Em vez de fazer login, o usuário tenta acessar outro site, como o Portal de autoatendimento para funcionários (/ess).
4. O sistema redireciona o usuário para a página de login novamente.
5. O usuário faz login e é redirecionado para o registro que o usuário tentou acessar pela primeira vez, em vez do Portal de autoatendimento para funcionários.

Exemplo 2:

1. Um usuário não está conectado e tenta acessar um registro usando um ID SYS específico no URL por meio do Portal de autoatendimento para funcionários (/ess)
2. O sistema redireciona o usuário para a página de login.
3. Em vez de fazer o login, o usuário tenta acessar outro registro por meio do Portal de autoatendimento para funcionários (/ess).
4. O sistema redireciona o usuário para a página de login novamente.
5. O usuário faz login e é redirecionado para o primeiro registro em vez do segundo.

Especifique uma página principal de login

Por padrão, os usuários veem sua página inicial ao fazer login. Você pode especificar uma página principal de login diferente usando uma propriedade do sistema ou o sistema de gestão de conteúdo.

Antes de Iniciar
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa
Para especificar uma página principal de login para todos os usuários, altere o valor da propriedade na tabela sys_properties.

Procedimento

1. Digite `sys_properties.list` no filtro de navegação.
2. Localize a propriedade de sistema **glide.login.home**.
3. No campo **Valor**, insira o nome da página que todos os usuários veem no login.

   Use `<page name>.do`; você pode omitir a parte `http://''instance''.service-now.com/` do URL. Para determinar o nome da página ou o URL de uma página no sistema, você pode apontar para um link. Algumas páginas possíveis são `welcome.do` e `incident.do`.

   Para especificar uma página principal do painel, defina a propriedade como `$dashboards.do?Dashboard=<SYS_ID>`. Substituir <SYS_ID> com o sys_id do painel.

   Para direcionar os usuários ao portal de serviço, defina a propriedade como `/sp`

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Esta propriedade aplica-se a todo o sistema, portanto, sua configuração afeta todos os usuários. Para definir um login especificamente para usuários sem funções, você pode aplicar essas mesmas etapas e usar a propriedade **glide.entry.loggedin.page_ess**.

Você também pode especificar uma página principal de login com o sistema de gestão de conteúdo.

Especificar bloqueio para tentativas de login com falha

O sistema fornece ações de script inativas que permitem especificar o número de tentativas de login com falha antes que uma conta de usuário seja bloqueada e redefinir a contagem após um login bem-sucedido.

Antes de Iniciar

Função necessária: administrador

Procedimento

Navegue até **Todos** > **Política do Sistema** > **Ações de Script** para exibir ou ativar os scripts.

Nota: Começando com a versão Kingston, após um zBoot, as ações de script **Verificação de bloqueio do usuário SNC com desbloqueio automático** e **Limpeza do usuário SNC** são ativadas.

Para saber mais sobre as propriedades que afetam as tentativas de login com falha, consulte Gestão das tentativas de login sem êxito (reforço de segurança da instância) em Configurações de proteção de segurança da instância.

Ação de script	Descrição
Verificação de bloqueio do usuário SNC com desbloqueio automático	• Usa o valor da propriedade *glide.user.max_unlock_attempts* para definir o limite de tentativas de login com falha. • Desbloqueia a conta do usuário após o período de tempo especificado para a propriedade *glide.user.unlock_timeout_in_mins*. Se nenhum valor for especificado, o sistema desbloqueará a conta do usuário após o período padrão de 15 minutos.
Verificação de bloqueio do usuário SNC	Rastreia o número de tentativas de login com falha e bloqueia a conta do usuário após um número especificado de tentativas de login com falha (padrão: 5).
Limpeza do Usuário SNC	Atualiza o registro do usuário após um login bem-sucedido: redefine o número de tentativas de login com falha e atualiza a data do último login.

O que Fazer Depois

Cada vez que um usuário tenta fazer login, a ação é registrada em um log de eventos. Você pode exibir um log de tentativas de login com falha.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

1. Navegue até **Política do Sistema** > **Logs de eventos**.
2. Filtre por **login.failed** no campo **Nome**. Você pode visualizar o nome, a data e o endereço IP da tentativa de login.

Tornar as páginas de IU públicas ou privadas

Você pode tornar as páginas públicas se quiser que seus usuários vejam as páginas sem fazer login.

Antes de Iniciar
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa
A maioria das páginas só pode ser visualizada por usuários conectados. Um número limitado de páginas é público para que os usuários não precisem fazer login para exibi-las, como a página de boas-vindas, a página inicial e as páginas de login e logout.

> ⚠ **Aviso:** Várias páginas públicas do sistema básico são necessárias para a funcionalidade de muitos recursos. Não desabilite as páginas públicas do sistema básico.

Procedimento
1. No filtro do navegador de aplicações, digite `sys_public.list`.
2. Clique em **Novo**.
3. Na tabela sys_public, crie um registro com os seguintes valores.

Campo	Descrição
Página	O nome da página. Por exemplo: $sp
Ativo	Quando selecionada, a página é acessível publicamente. Desmarque a opção Ativo quando quiser que a página seja privada.

4. Clique em **Salvar**.
   Ao definir ativo como verdadeiro, a página se torna pública, portanto, todos os visitantes de `<instance_name>/sp` ou `<instance_name>/$sp.do` podem acessar a página.

Requisitos de complexidade de senha

As senhas em sua instância da ServiceNow® devem atender aos requisitos de complexidade.

Explorar

Habilitar

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Conheça os recursos e o valor comercial dos Requisitos de complexidade de senha.

Entenda como habilitar os Requisitos de complexidade de senha.

Configurar

Configure os Requisitos de complexidade de senha.

Referência - Caracteres de senha não compatíveis

Conheça os caracteres de senha não compatíveis.

Explorar requisitos de complexidade de senha

As senhas em sua instância da ServiceNow® devem atender aos requisitos de complexidade.

A configuração de política de requisitos de complexidade de senhas determina se as senhas devem atender a uma série de diretrizes de senha forte.

Os requisitos de complexidade de senha são impostos quando uma senha é alterada ou criada.

Os requisitos de complexidade de senha aderem e funcionam com base no seguinte:

- Se a propriedade *glide.apply.password_policy.on_login* estiver habilitada, a verificação da política de senha será aplicada ao usuário durante o login. Durante o login, o usuário deve aderir à política de senha e mudar a senha da instância.
- Os requisitos da política de senha são baseados no BMP (Basic Multilingual Plane, plano multilíngue básico) que contém caracteres para todos os idiomas modernos. As instâncias da ServiceNow são enviadas com BMPs de cerca de 10.000 caracteres.
- As senhas dentro dos BMPs permitidas podem ser definidas para sua instância. Senhas que não estejam em conformidade com esses BMPs não são permitidas.

Se necessário, você pode exigir que as senhas sejam alteradas regularmente, pelo menos a cada 90 dias.

Requisitos e caracteres proibidos

Para habilitar um ambiente de rede seguro, é necessário que os usuários usem senhas fortes que incluam uma combinação de letras, números e símbolos. Essas combinações ajudam a evitar que usuários não autorizados que geralmente usam métodos manuais ou automatizados adivinhem senhas fracas.

A senha da sua instância deve atender aos seguintes requisitos:

- Mínimo de 8 caracteres.
- Máximo de 100 caracteres.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Contém minúsculas e maiúsculas
- Contém caracteres especiais.
- Conter dígitos.

Você pode proibir uma lista de senhas ruins comuns, como a seguinte:

- Sequências previsíveis e repetidas, como "123456", "qwerty", "!@#$%^", "aaaaa" e assim por diante.
- Nome do funcionário ou nomes de usuário.
- Nomes de marcas ou produtos relevantes.
- Locais, como sede, cidade, país da empresa e assim por diante.
- Abreviações ou termos internos específicos da empresa.
- Emojis.

Nota: Caracteres específicos do usuário, da marca ou da empresa que não podem ser usados na senha podem ser configurados na página Política de senha ou Excluir senha.

Habilitação das políticas de senha na sua instância

Implemente controles de política de senha no login. Force os usuários a mudar a senha se a senha não atender aos critérios da política de senha.

Antes de Iniciar

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

O plug-in Password Policy (com.glide.password_policy) está habilitado por padrão. A política entra em vigor quando um usuário muda ou redefine a senha.
O campo **Predefinição de força da senha** é definido automaticamente como **Padrão forte**.
Se você quiser adicionar novos critérios, poderá executar o procedimento a seguir.

Se você personalizou sua instância por meio da *ValidatePasswordStronger*saída de instalação ou do armazenamento de credenciais da Redefinição de senha*pwd_cred_store*, consulte Propriedades da política de senha para saber como implementar uma política de senha para sua instância.

Nota: A política de senha ativa é realçada para a instância, conforme mostrado.

Para mudar a política de senha, navegue até **Todos** > **Redefinição de senha** > **Armazenamentos de credenciais**, selecione as credenciais e altere o campo **Política de senha** para a entrada de política necessária.

Procedimento

1. Navegue até **Todos** > **Política de senha** > **Políticas de senha**.
2. Clique em **Nova**.
   O formulário Política de senha é exibido.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Especifique o **Nome** da sua política de senha.
4. Na seção Critérios da política de senha, selecione uma das predefinições a seguir no campo **Predefinição de força da senha**.

Predefinição de força da senha	Descrição
Padrão	Preenche automaticamente os campos para caracteres de senha obrigatórios da seguinte forma: ◦ Define o **mínimo de caractere(s) maiúsculo(s)** como 1. ◦ Define o **mínimo de caractere(s) minúsculo(s)** como 1. ◦ Define o **mínimo de caractere(s) numérico(s)** como 1. ◦ Define o **mínimo de caractere(s) especial(is)** como 0. O comprimento mínimo da senha é de 8 caracteres e o máximo é 100.
Médio	Preenche automaticamente os campos para caracteres de senha obrigatórios da seguinte forma: ◦ Define o **mínimo de caractere(s) maiúsculo(s)** como 1. ◦ Define o **mínimo de caractere(s) minúsculo(s)** como 1. ◦ Define o **mínimo de caractere(s) numérico(s)** como 1. ◦ Define o **mínimo de caractere(s) especial(is)** como 1. O comprimento mínimo da senha é de 12 caracteres e o máximo é de 40.
Alto	Preenche automaticamente os campos para caracteres de senha obrigatórios da seguinte forma: ◦ Define o **mínimo de caractere(s) maiúsculo(s)** como 1. ◦ Define o **mínimo de caractere(s) minúsculo(s)** como 2. ◦ Define o **mínimo de caractere(s) numérico(s)** como 1. ◦ Define o **mínimo de caractere(s) especial(is)** como 3. O comprimento mínimo da senha é de 8 caracteres e o máximo é 100.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Predefinição de força da senha	Descrição
Padrão forte	Preenche automaticamente os campos para caracteres de senha obrigatórios da seguinte forma: ◦ Define o **mínimo de caractere(s) maiúsculo(s)** como 1. ◦ Define o **mínimo de caractere(s) minúsculo(s)** como 1. ◦ Define o **mínimo de caractere(s) numérico(s)** como 1. ◦ Define o **mínimo de caractere(s) especial(is)** como 1. O comprimento mínimo da senha é de 8 caracteres e o máximo é 100.
Personalizado	Preenche automaticamente os campos para caracteres de senha obrigatórios da seguinte forma: ◦ Define o **mínimo de caractere(s) maiúsculo(s)** como 1. ◦ Define o **mínimo de caractere(s) minúsculo(s)** como 1. ◦ Define o **mínimo de caractere(s) numérico(s)** como 1. ◦ Define o **mínimo de caractere(s) especial(is)** como 1. O comprimento mínimo da senha é de 8 caracteres e o máximo é 100. Você também pode personalizar o **Script da política de senha** exibido.
Avançado	Selecionar **Avançado** exibe o **Script de regra de senha** e o **Script de força da senha**. Com base em seus requisitos, você pode personalizar esses scripts.

Nota: A política de senha é aplicada com base na predefinição selecionada.

5. No formulário, preencha os campos remanescentes.

Formulário Política de senha

Campo	Descrição
Comprimento mínimo da senha	Comprimento mínimo da senha. Esta opção é exibida para todas as predefinições, exceto **Avançado**. Defina este campo com um mínimo de 8 a 10 caracteres.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Comprimento máximo da senha	Comprimento máximo da senha. Esta opção é exibida para todas as predefinições, exceto **Avançado**. Defina este campo para um máximo de 100 caracteres.
Mínimo de caracteres em maiúsculas	Número mínimo de caracteres maiúsculos na senha, de 0 a 10.
Mínimo de caracteres em minúsculas	Mínimo de caracteres minúsculos na senha, de 0 a 10.
Mínimo de caracteres numéricos	Mínimo de caracteres numéricos na senha, de 0 a 10.
Mínimo de caracteres especiais	Número mínimo de caracteres especiais na senha, de 0 a 10.
Caracteres especiais incluídos	Permita um conjunto restrito de caracteres especiais sem qualquer delimitador. Por exemplo, se você inserir `$,!`, os usuários só poderão usar "$" e "!" como caracteres especiais na senha. Nenhum outro caractere especial pode ser usado. Uma senha com outros caracteres especiais não é permitida.
Caracteres especiais excluídos	Permita um conjunto restrito de caracteres especiais sem qualquer delimitador. Por exemplo, se você inserir `@$!`, os usuários não poderão usar '@', '$' e '!' como caracteres especiais em suas senhas. **Nota:** Esta opção estará disponível se a propriedade *glide.password_policy.use_excluded_special_ch* estiver habilitada.
Proibir dados do usuário	Opção para proibir os dados do usuário relacionados à autenticação.
Limite de comprimento de sequência	O comprimento da sequência da sua senha.
Limite de comprimento de repetição	O comprimento de repetição da sua senha.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: ◦ O limite de comprimento de sequência e o limite de comprimento de repetição podem ter no máximo oito caracteres. Esses campos permitem que você restrinja combinações fracas de senhas que tenham sequências previsíveis e repetidas, como "123456", "qwerty", "!@#$%^", "aaaaa" e assim por diante. ◦ Se a **Predefinição de força da senha** estiver definida como **Padrão forte**, o comprimento do limite de comprimento de sequência e do limite de comprimento de repetição será definido como quatro caracteres.
Testar a sua senha	Especifique sua senha efetiva neste campo.

6. Clique em **Testar a sua senha**
7. Depois que a senha for testada como válida, clique em **Enviar** para enviar a senha.

Nota: Sempre teste sua senha antes de enviar.

Propriedades da política de senha

As propriedades da política de senha permitem que você administre políticas de senha, exclua senhas de lista e aplique uma política de senha durante o login.

Navegue até **Política de senha** > **Propriedades** para exibir e editar as propriedades da política de senha.

Propriedade	Descrição
glide.enable.password_policy	Habilita uma política de senha para sua instância. A política entra em vigor quando um usuário altera ou redefine uma senha. Esta propriedade é definida automaticamente como **verdadeira**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Propriedade	Descrição
	Nota: • Se sua instância for personalizada, por meio da saída de instalação *ValidatePasswordStronger* ou do armazenamento de credenciais da Redefinição de senha [pwd_cred_store], você deverá criar esta propriedade e adicioná-la às propriedades do sistema. • Antes da versão Orlando, se sua instância fosse personalizada com a saída de instalação *ValidatePasswordStronger*, você tinha que criar a propriedade Política de senha para fazer a Política de senha funcionar. • Começando com a versão Orlando, não há personalização de saída de instalação. As propriedades da Política de senha funcionam por padrão. Essas propriedades podem ser desativadas manualmente.
glide.enable.blacklist_password	Proíbe o uso de senhas específicas. O administrador pode inserir senhas na tabela Senha excluída. Esta propriedade é definida automaticamente como **verdadeira**.
glide.apply.password_policy.on_login	Força os usuários a mudar as senhas durante o próximo login se as senhas existentes não estiverem em conformidade com a política de senha atual. Essa propriedade é definida automaticamente como **falsa**. Definir o valor como **verdadeiro** impõe uma política de senha durante o login. **Nota:** Habilitar esta propriedade pode forçar um número significativo de usuários que não estão em conformidade com a nova política de senha a mudar suas senhas.
glide.password_policy.user_excluded_special_char	Permite que os usuários usem a opção de caractere especial excluído no formulário Política de senha.
glide.validate.sys_user.password.field	Habilita a validação da senha do usuário em relação à política de senha quando um administrador está editando o formulário sys_user ou a exibição de lista.
glide.password.policy.generate.password.field.disabled	Desativado o campo **Senha** no pop-up de definição de senha no formulário sys_user.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Propriedade	Descrição
glide.user.show.password.field	Ativa o campo **Senha** no formulário sys_user.
glide.password_policy.debug	Habilita o registro em log de depuração para a política de senha

Configurar política de senha

Os critérios da política de senha permitem que você proteja sua senha e cumpra os requisitos mínimos de complexidade de senha.

Antes de Iniciar

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

O plug-in Password Policy [com.glide.password_policy] é habilitado por padrão. Ele entra em vigor quando um usuário altera ou redefine a senha. Se você personalizou sua instância, por meio da saída de instalação ValidatePasswordStronger ou de seu armazenamento de credenciais do Redefinição de senha [pwd_cred_store], consulte as Propriedades da política de senha.

Procedimento

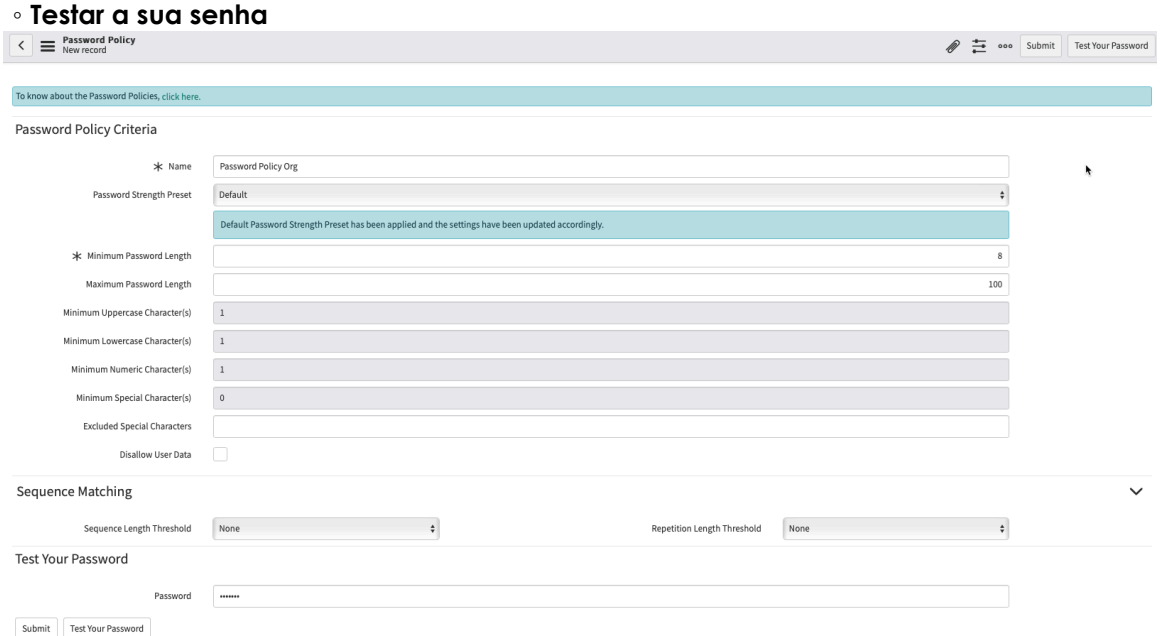
1. Navegue até **Todos** > **Política de senha** > **Políticas de senha**.

   Nota: Predefinição **Padrão forte** habilitada como um critério de aceitação de senha padrão. No caso, se quiser adicionar um novo critério, você pode executar as seguintes etapas.

2. Clique em **Novo**.

   A página de registro da Nova política de senha tem as seguintes seções que você deve especificar para definir sua senha:

   - **Critérios da política de senha**
   - **Correspondência de sequência**
   - **Testar a sua senha**



© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Especifique o **Nome** da sua política de senha.
4. Na seção **Critérios de política de senha**, selecione a predefinição em **Predefinição de força de senha**. As predefinições disponíveis são as seguintes:

Predefinição de força da senha e sua descrição

Predefinição de força da senha	Descrição
Padrão	Selecionar **Padrão** preenche automaticamente os caracteres de senha necessários da seguinte forma: ◦ Um caractere maiúsculo mínimo ◦ No mínimo um caractere em minúsculas ◦ Um caractere numérico mínimo
Médio	Selecionar **Médio** preenche automaticamente os caracteres de senha necessários com base nos caracteres a seguir: ◦ Um caractere maiúsculo mínimo ◦ No mínimo um caractere em minúsculas ◦ No mínimo um caractere numérico ◦ No mínimo um caractere especial
Alto	Selecionar **Alto** preenche automaticamente os caracteres de senha da seguinte forma: ◦ Um caractere maiúsculo mínimo ◦ No mínimo dois caracteres em minúsculas ◦ No mínimo um caractere numérico ◦ No mínimo três caracteres especiais
Padrão forte	Selecionar **Padrão forte** preenche automaticamente os caracteres de senha necessários com base nos caracteres a seguir: ◦ Um caractere maiúsculo mínimo ◦ No mínimo um caractere em minúsculas ◦ No mínimo um caractere numérico ◦ Um caractere especial mínimo
Personalizado	Selecionar **Personalizado** preenche automaticamente os caracteres de senha necessários com base nos caracteres a seguir: ◦ Um caractere maiúsculo mínimo ◦ No mínimo um caractere em minúsculas

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Predefinição de força da senha	Descrição
	◦ No mínimo um caractere numérico ◦ Um caractere especial mínimo Você também pode personalizar o **Script da política de senha** exibido.
Avançado	Selecionar **Avançado** exibe o **Script de regra de senha** e o **Script de força da senha**. Com base em seus requisitos, você pode personalizar esses scripts.

Nota: A política de senha é aplicada com base na predefinição selecionada.

5. Especifique os campos descritos na tabela:

Formulário Política de senha

Campo	Descrição
Comprimento mínimo da senha	O comprimento mínimo da senha. Esta opção é exibida para todas as predefinições, exceto **Avançado**. **Nota:** **Comprimento mínimo da senha** é um campo obrigatório e é recomendável defini-lo para um mínimo de 8 a 10 caracteres.
Comprimento máximo da senha	Comprimento máximo da senha. Esta opção é exibida para todas as predefinições, exceto **Avançado**. **Nota:** **Comprimento máximo da senha** é um campo opcional e é recomendável defini-lo para um máximo de 100 caracteres.
Mínimo de caracteres maiúsculos	Número mínimo de caracteres maiúsculos na senha, de 0 a 10.
Mínimo de caracteres em minúsculas	Mínimo de caracteres minúsculos na senha, de 0 a 10.
Mínimo de caracteres numéricos	Mínimo de caracteres numéricos na senha, de 0 a 10.
Mínimo de caracteres especiais	Número mínimo de caracteres especiais na senha, de 0 a 10.
Caracteres especiais incluídos	Permita um conjunto restrito de caracteres especiais sem qualquer delimitador. Por exemplo, se você inserir "$,!" os usuários só poderão usar "$" e "!" como caracteres especiais na senha. Nenhum outro caractere especial pode ser usado e uma

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	senha com outros caracteres especiais não é permitida.
Caracteres especiais excluídos	Permita um conjunto restrito de caracteres especiais sem qualquer delimitador. Por exemplo, quando '@$!' for inserido, os usuários não poderão usar '@', '$' e '!' como caracteres especiais em suas senhas. **Nota:** Esta opção estará disponível se a propriedade glide.password_policy.use_excluded_special_char estiver habilitada.
Proibir dados do usuário	Está habilitado para proibir os dados do usuário.

6. Na seção Correspondência de sequência, especifique o **Limite de comprimento de sequência** e o **Limite de comprimento de repetição**.

   Nota:
   - O limite de comprimento de sequência e o limite de comprimento de repetição podem ter no máximo oito caracteres. Esses campos permitem que você restrinja combinações fracas de senhas que tenham sequências previsíveis e repetidas, como "123456", "qwerty", "!@#$%^", "aaaaa" e assim por diante.
   - Para **Padrão forte**, o comprimento tanto para o limite de comprimento de sequência e o limite de comprimento de repetição é selecionado como quatro caracteres.

7. Na seção **Testar a sua senha**, especifique sua senha.
8. Clique em **Testar a sua senha**
9. Depois que a senha for válida, clique em **Enviar** para enviar a senha.

   Nota: Sempre teste sua senha antes de enviar.

Configurar senha para um usuário

Defina a senha dos usuários para a instância com base na política de senha que está configurada.

Antes de Iniciar

Usuários criados para definir a senha do primeiro login. Para obter mais informações, consulte Criar um usuário.

Para preencher o campo **Senha** diretamente no formulário do usuário, ative o campo **Habilitar para mostrar o campo de senha no formulário sys_user** (glide.user.show.password.field). Para saber mais sobre as propriedades, consulte Propriedades da política de senha.

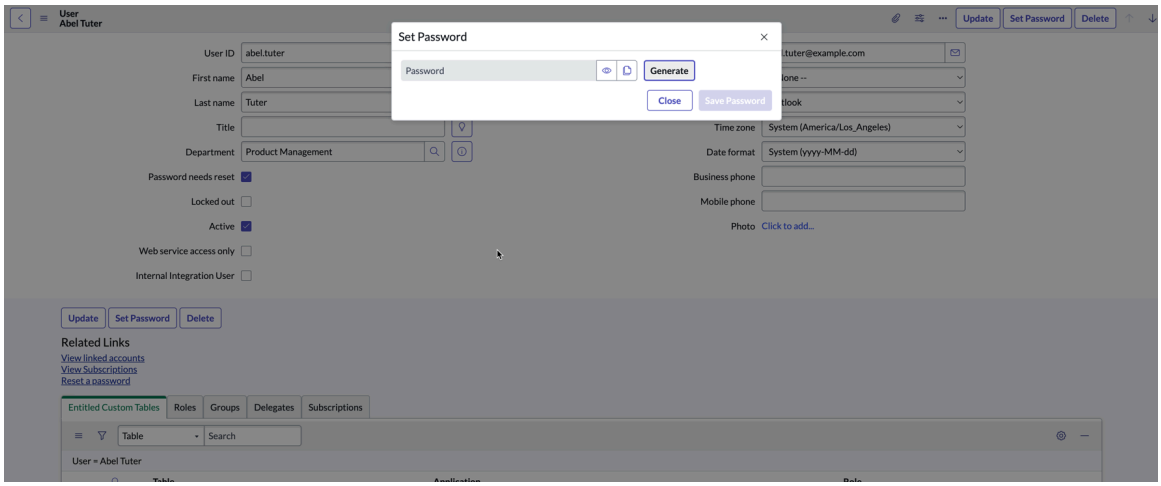
Função necessária: administrador

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

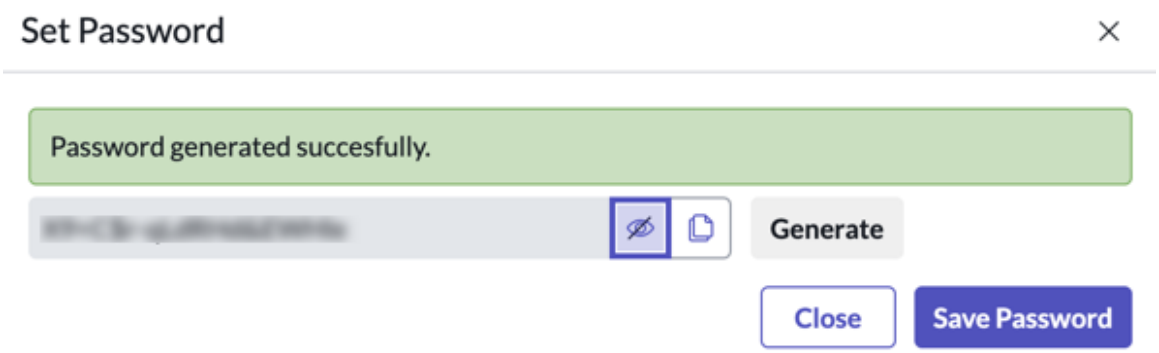
1. Navegue até **Todos** > **Administração de usuários** > **Usuários**.
2. Selecione o usuário na lista na página Usuários.
3. Para definir a senha com base na política de senha, clique em **Definir senha**.

   O pop-up Definir senha é exibido.



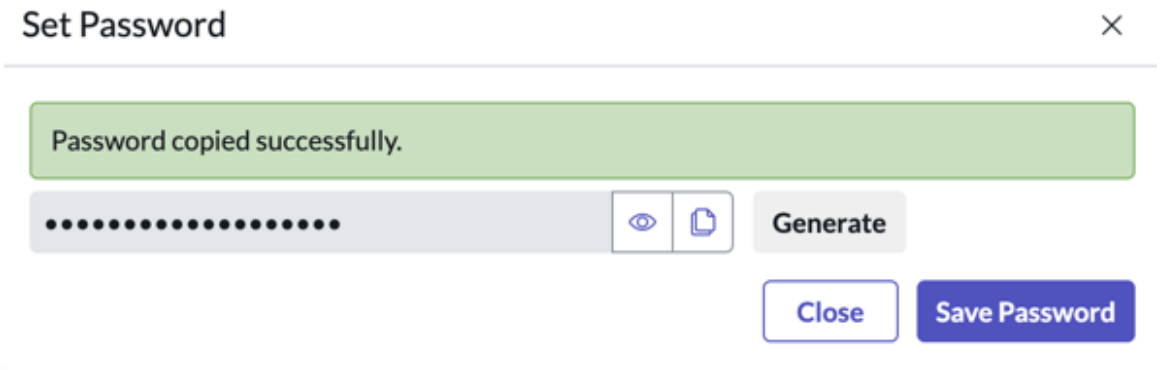
4. Em Definir senha, execute o seguinte.
   a. Clique em **Gerar** para gerar a senha.

   b. Clique no ícone **Exibir** para exibir a senha.



© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

c. Clique no ícone **Copiar** para copiar a senha e compartilhar com o usuário.



5. Clique em **Salvar senha**.

   A senha é definida para o usuário. Além disso, a caixa de seleção A senha precisa ser redefinida é habilitada automaticamente.

   O usuário durante o primeiro login deve usar a mesma senha para login e mudar a senha no momento do login aderindo à política de senhas configurada pelos administradores.

Exclusão de senhas por meio de políticas de senha em sua instância

Adicione senhas à tabela Senha excluída para proibir que senhas específicas sejam usadas por usuários em sua instância.

Antes de Iniciar
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa
Você pode proibir quantas senhas forem necessárias. Alguns dos exemplos são os seguintes:

- Sequências previsíveis e repetidas, como "123456", "qwerty", "!@#$%^", "aaaaa" e assim por diante.
- Nome do funcionário ou nomes de usuário.
- Nomes de marcas ou produtos relevantes.
- Locais, como sede, cidade, país da empresa e assim por diante.
- Abreviações ou termos internos específicos da empresa.
- Emojis.

Procedimento

1. Navegue até **Todos** > **Política de senha** > **Senhas excluídas**.
2. Para adicionar uma senha à sua lista de exclusões, clique em **Nova** e insira a senha.
3. Navegue até **Política de senha** > **Gerenciamento da lista de exclusões** para controlar a senha dos usuários e impedir que usuários usem senhas ruins para a instância.

   O **Gerenciamento da lista de exclusões** tem cerca de 5.000 senhas usadas com frequência.

Caracteres de senha não compatíveis

Há caracteres de senha que não são compatíveis. Os usuários não podem usar esses caracteres, com base em requisitos de complexidade de senha da ServiceNow.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para habilitar um ambiente de rede seguro, é necessário que os usuários usem senhas fortes que incluam uma combinação de letras, números e símbolos. Essas combinações ajudam a evitar que usuários não autorizados que geralmente usam métodos manuais ou automatizados adivinhem senhas fracas.

- Os requisitos da política de senha são baseados no BMP (Basic Multilingual Plane, plano multilíngue básico) que contém caracteres para todos os idiomas modernos. A instância da ServiceNow é enviada com BMPs de cerca de 10.000 caracteres.
- Os caracteres de senha neste BMPs permitidos podem ser definidos para sua instância, os caracteres de senha que não estão em conformidade com este BMPs não são permitidos.

Nota: Os caracteres específicos do usuário ou da empresa que não podem ser usados na senha podem ser configurados na lista de exclusão de senhas.

Para obter mais informações sobre as propriedades da política de senha, consulte Propriedades da política de senha.

Redefinição de senha

O processo padrão de autoatendimento de Redefinição de senha permite que um usuário redefina a senha sem a assistência de agentes da central de serviços.

Example: O fluxo de autoatendimento padrão da Redefinição de senha

1. Se um usuário não se lembrar da senha, ele poderá clicar no link **Esqueceu a senha?** na tela de login.
2. A aplicação Redefinição de senha iniciará. Na página **Identidade**, o usuário se identifica inserindo um **Nome de usuário**.
3. Na página **Verificar**, o usuário prova que é a pessoa associada ao nome de usuário. Neste exemplo, o usuário insere o endereço de e-mail que está associado ao perfil de usuário. O administrador pode configurar um método de verificação diferente ou exigir verificações adicionais, por exemplo, uma pergunta pessoal que somente o usuário pode responder.
4. A página **Redefinir** informa ao usuário para verificar o e-mail para obter instruções.
5. O usuário abre o e-mail e clica no link **aqui** para redefinir a senha. O link é válido por um período que você especificar (use a propriedade **password_reset.request.expiry**).
6. A página **Redefinir senha** orienta o usuário na redefinição da senha.

O processo de autoatendimento padrão do Redefinição de senha (`com.glideapp.password_reset`) define:

- O URI que especifica para onde os usuários são redirecionados quando clicam em **Esqueceu a senha?**. Por padrão, este valor é **/$pwd_reset.do?sysparm_url=ss_default**, que é o mesmo valor usado na propriedade *`glide.security.password_reset.uri`*. Em versões anteriores, este valor era definido como **/reset_password.do**.
- A opção **Habilitar URL da Redefinição de senha** especifica que o usuário deve receber um e-mail com um link para redefinir a senha depois de clicar em **Esqueceu a senha?**.
- O fluxo de verificação Dados pessoais - Inserir endereço de e-mail especifica o fluxo em três etapas da Redefinição de senha.

Consulte Configurar o Processo de redefinição de senha para obter instruções sobre como acessar esse formulário e configurar os campos.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

- Este recurso funciona para usuários autenticados localmente que inserem o nome de usuário e a senha especificados no registro do usuário. Os usuários que fazem login na instância por meio de uma solução SSO ou de uma integração LDAP não podem redefinir senhas usando o processo de autoatendimento do Redefinição de senha de exemplo.
- O usuário final deve habilitar e configurar preferências de notificação. Consulte Notificações baseadas em assinatura. Os administradores podem modificar o e-mail enviado ao usuário final.

Modificar o texto do e-mail de notificação do Redefinição de senha

Os usuários do processo de autoatendimento do Redefinição de senha recebem uma notificação por e-mail quando solicitam a redefinição de senha. Você pode modificar o texto do e-mail e outros aspectos da notificação.

Antes de Iniciar
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa
Este processo é relevante somente se os usuários têm Notificações baseadas em assinatura.

Procedimento
1. Navegue até **Todos** > **Notificação do sistema** > **Notificações**.
2. Selecione a notificação **URL do Redefinição de senha**.
3. Modifique o texto do e-mail na seção **O que ele conterá**.
   Para obter mais informações sobre a configuração de outros aspectos da notificação, consulte Criar uma notificação de e-mail.

Configurar propriedades do Redefinição de senha

Você pode especificar propriedades que configuram a experiência do Redefinição de senha para usuários finais.

Antes de Iniciar
Função necessária: password_reset_admin

Por Que e Quando Desempenhar Esta Tarefa
Embora não haja limites de intervalo para os valores que você pode inserir nas propriedades, considere usar somente valores inteiros positivos começando em 1. Ao determinar o limite do intervalo superior de uma propriedade, considere a tarefa que o usuário está executando.

Por exemplo, você não deseja permitir 100 tentativas de verificação de identidade pelos usuários. Um valor mais comum é 3 tentativas. Da mesma forma, você pode não querer forçar os usuários que estão preenchendo o processo de inscrição a gastar tempo selecionando e respondendo a 30 perguntas de segurança. O número de perguntas de segurança usadas com mais frequência é entre 5 e 7.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegue até **Todos** > **Redefinição de senha** > **Propriedades**.
   Para obter informações sobre as propriedades de Redefinição de senha, consulte Redefinição de senha propriedades globais.
2. Atualize as configurações conforme necessário e clique em **Salvar**.

Lembrar minhas informações

Quando a caixa de seleção **Lembrar-me** é selecionada no login, um cookie é armazenado no computador do usuário. Este cookie autentica automaticamente o usuário nas visitas subsequentes.

Se o usuário fizer logout, o cookie será destruído. O valor padrão da caixa de seleção **Lembrar-me** é controlado por uma propriedade e uma propriedade diferente controla se a caixa de seleção aparecerá ou não na página de login.

Duas propriedades *glide.ui.user_cookie.life_span_in_days* e *glide.ui.user_cookie.max_life_span_in_days* controlam o valor de expiração do cookie gerado pelo sistema glide_user. Quando um usuário acessa uma instância com "lembrar-me" habilitado, o acesso redefine o período de expiração do cookie até que o limite de vida útil máximo (glide.ui.user_cookie.max_life_span_in_days) seja atingido.

Nota: Para saber mais sobre estas propriedades, consulte os seguintes tópicos nas Configurações de proteção de segurança da instância:

- Tempo limite absoluto da sessão
- Tempo limite da sessão

Alterar o valor padrão da caixa de seleção Lembrar-me

Você pode alterar o valor padrão da caixa de seleção **Lembrar-me**.

Antes de Iniciar
Função necessária: administrador

Procedimento

1. Navegue até **Todos** > **Propriedades do sistema** > **Propriedades de IU**.
2. Localize a propriedade *Default value of "Remember me" checkbox on login page* (*glide.ui.remember.me.default*).
3. Para definir o valor padrão da caixa de seleção **Lembrar -me** como **Não**, desmarque a caixa de seleção da propriedade.
4. Para restaurar o valor padrão da caixa de seleção **Lembrar-me** como **Sim**, selecione a caixa de seleção da propriedade.

Remover a caixa de seleção Lembrar-me

Você pode remover a caixa de seleção **Lembrar-me** para que os usuários não tenham acesso a este recurso.

Antes de Iniciar
Função necessária: security_admin

Nota: Para aprender mais sobre essa propriedade, consulte Remover Lembrar-me nas Configurações de proteção de segurança de instância.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Eleve sua função para security_admin.
2. Navegue até **Propriedades do sistema** > **Propriedades de IU**.
3. Localize a propriedade *Remove "Remember me" checkbox from login page* (*glide.ui.forgetme*).
4. Marque caixa de seleção da propriedade.
   Esta configuração remove a caixa de seleção **Lembrar-me**, invalida os cookies existentes e desabilita totalmente a funcionalidade Lembrar-me.
5. Para restaurar a caixa de seleção **Lembrar-me** na página de login, desmarque a caixa de seleção da propriedade.

Configurar o prompt de confirmação de logout

Você pode habilitar um prompt de confirmação de logout para impedir que os usuários façam logout acidentalmente.

Antes de Iniciar

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

Nota: O procedimento a seguir funciona somente em versões de IU anteriores a IU principal, que é a mais recente e a mais usada.

Procedimento

1. Navegue até **Todos** > **Propriedades do sistema** > **Sistema**.
2. Localize a propriedade **Avisar usuário para confirmar uma solicitação de logout** e marque a caixa de seleção.
3. Quando o usuário clica no botão **Logout**, uma caixa de diálogo de confirmação é exibida.

Implementar um nonce

Você pode implementar um nonce a ser usado com autenticação Digest de login único.

Para usar um nonce com o token não criptografado ou métodos de token criptografado de Single Sign-on, essas etapas se aplicam com apenas algumas pequenas mudanças.

Nota: O nonce é usado somente para solicitações de login, não para qualquer outro tipo de solicitação. Se o sistema receber um valor de nonce após o login, o nonce não será consumido.

Benefícios

O uso de um nonce proíbe um usuário mal-intencionado de executar um ataque de repetição para fazer login no seu sistema.

Fluxo do processo do nonce

Quando um cliente implementa o Single Sign-on do token resumido e deseja adicionar a segurança de um nonce, ele segue um determinado fluxo do processo.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

1. Um usuário faz login no portal do cliente.
2. O cliente gera os parâmetros de SSO necessários e anexa um nonce aleatório ao final. Por exemplo, se o cliente estiver encaminhando a resposta de autenticação por meio da cadeia de caracteres de consulta, ela poderá ficar desta forma:

```
SM_USER=itil&DE_USER=V1QuWMmxSfBgfRS099X0cAjKo5Q=&NONCE=1407743018
```

A instância recebe esta solicitação e recupera as variáveis de autenticação. Antes de tentar verificar a integridade da resposta da autenticação, a instância verifica o nonce em relação a uma tabela interna (u_authentication_nonce) para verificar se ele ainda não existe. Se o nonce não existir nessa tabela, ele será adicionado à tabela e o processo de autenticação terá permissão para continuar. No entanto, se esse valor de nonce já existir na tabela, a tentativa de autenticação será cancelada e um código de erro de `failed_missing_requirement` será retornado, o que normalmente leva o usuário de volta para a página de login.

Implementar um nonce

Adicione um nonce criptográfico ao cabeçalho de autenticação para garantir que ele só possa ser usado uma vez.

- Crie uma propriedade do sistema chamada *`glide.authenticate.header.nonce_key`* e defina seu valor com qualquer nome de variável que você esteja usando para o nonce, como NONCE ou NCE.
- Crie uma nova tabela chamada `u_authentication_nonce`. Adicione um campo à tabela chamada `u_nonce`.
- Acesse as **Propriedades do sistema** > **Saídas de instalação** e crie um item chamado `DigestSingleSignOnNonce` que substitui ExternalAuthentication (*`glide.authenticate.external_property`*).
- Adicione o código a seguir à parte do script do DigestSingleSignOnNonce recém-criado.

```
gs.include("PrototypeServer");

var DigestSingleSignOnNonce = Class.create();
DigestSingleSignOnNonce.prototype = {

 process : function() {

  var headerKey = GlideProperties.get("glide.authenticate.header.key",
 "SM_USER");
  var headerDigestKey =
 GlideProperties.get("glide.authenticate.header.encrypted_key",
 "DIGEST");
  var headerNonceKey =
 GlideProperties.get("glide.authenticate.header.nonce_key", "NCE");
  var fieldName =
 GlideProperties.get("glide.authenticate.header.value", "user_name");
  var fkey = GlideProperties.get("glide.authenticate.secret_key");

  // Look in the Headers
  var data = request.getHeader(headerKey);
  var encdata = request.getHeader(headerDigestKey);
  var nonce = request.getHeader(headerNonceKey);
```

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

```
 // If not, then check the URL Parameters
 if (data == null || encdata == null || nonce == null) {
  data = request.getParameter(headerKey);
  encdata = request.getParameter(headerDigestKey);
  nonce = request.getParameter(headerNonceKey);
 }

 // then maybe its a cookie
 if (data == null || encdata == null || nonce == null) {
  var cookies = request.getCookies();
  data = GlideCookieMan.getCookieValue(cookies, headerKey);
  encdata = GlideCookieMan.getCookieValue(cookies, headerDigestKey);
  nonce = GlideCookieMan.getCookieValue(cookies, headerNonceKey);
 }

 // if found run encryption
 if (data != null && encdata != null && nonce != null) {
  try {

   // Replace all spaces with plus(+)'s, converted in url
   encdata = encdata.replaceAll(' ', '+');

   // ----- Encrypt the username|nonce
   var key = this.getDigest( data + "|" + nonce, fkey);

   // Check for match of received encoded data
   // and your encoding of user name
   if (encdata == key) {
    var ugr = new GlideRecord("sys_user");
    ugr.initialize();
    if (!ugr.isValidField(fieldName)) {
     GlideLog.warn("External authorization is set to use field: '"+
fieldName + "' which doesn't exist");
     return "failed_missing_requirement";
    }
    ugr.addQuery(fieldName, data);
    ugr.query();
    if (!ugr.next()) {
     var userLoad = GlideUser.getUser(data);
     if (userLoad == null)
      return "failed_authentication";

     ugr.initialize();
     ugr.addQuery(fieldName, data);
     ugr.query();
     if (!ugr.next())
      return "failed_authentication";

    }

    if (this.processNonce(nonce)){
     var userName = ugr.getValue("user_name");
     return userName;
    }
    else return "failed_missing_requirement";
    }
   else {
```

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

```
    return "failed_authentication";
   }
  } catch(e) {
   gs.log(e);
   return "failed_authentication";
  }
  // Encoded data didn't match recieved Encoded data
 } else {

  return "failed_missing_requirement";
 }
},

getDigest : function( data, fkey ) {
 try {
  // default to something JDK 1.4 has
  var MAC_ALG = "HmacSHA1";
  return SncAuthentication.encode(data, fkey, MAC_ALG);

 } catch (e) {
  gs.log(e.toString());
  throw 'failed_missing_requirement';
 }
} ,

processNonce : function( sentNonce ) {
 var ngr = new GlideRecord("u_authentication_nonce");

 ngr.addQuery("u_nonce", sentNonce);
 ngr.query();
 if (ngr.next()) {
  gs.log("This SSO entry has already been processed! (Nonce: " +
sentNonce + ")");
  return false;
 }
 var ngrNew = new GlideRecord("u_authentication_nonce");
 ngrNew.initialize();
 ngrNew.u_nonce = sentNonce;
 ngrNew.insert();
 gs.log("Inserted new nonce: " + sentNonce);
 return true;
}
};
```

- Depois de salvar sua nova saída de instalação, vá até a saída de instalação DigestSingleSignOn e verifique se ela está definida como Ativa=falsa.

Sua instância agora deve ser configurada para implementar um nonce.

Autenticação multifator (MFA)

Saiba como ativar e configurar a autenticação multifator.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

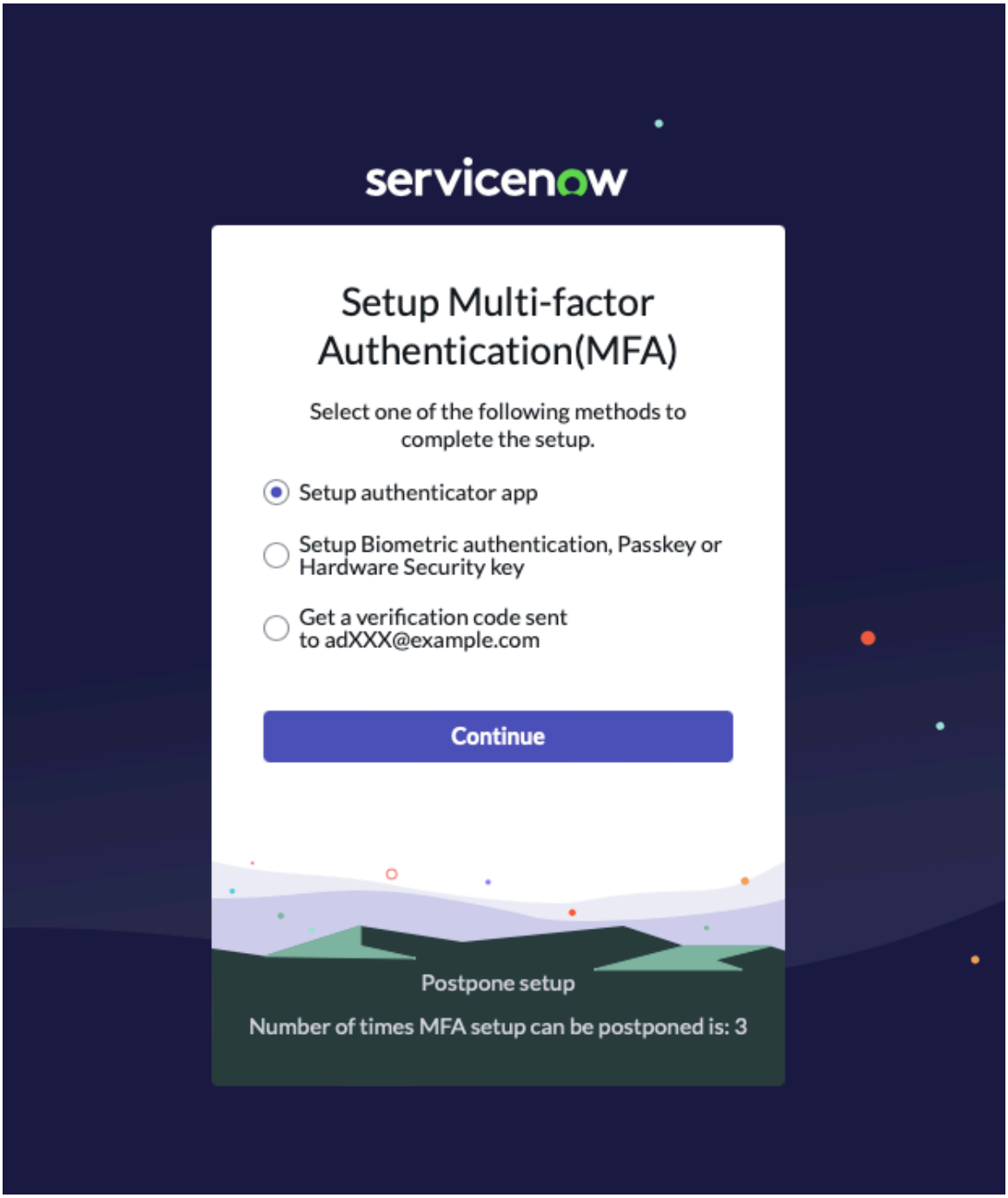
Explorar Conheça os recursos e o valor comercial da MFA.	Ativar Entenda como ativar a MFA.
Usar Configure e use a MFA.	MFA com Single Sign-on (SSO) Saiba como configurar a MFA com Single Sign-on (SSO).

Como explorar a autenticação multifator

A MFA (autenticação multifator) é um método de autenticação que requer que os usuários apresentem outras informações além de suas credenciais básicas.

Para a autenticação, a ServiceNow oferece opções de MFA, como a configuração de um app autenticador, biometria, senha ou chave de segurança de hardware, SMS e e-mail. É possível usar o autenticador FIDO2, senhas, autenticadores biométricos e chaves de segurança de hardware como fatores de MFA sem precisar configurar um app autenticador.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Se o usuário tiver concluído a configuração usando qualquer fator, ele ainda poderá acessar a página de perfil e concluir a configuração dos fatores restantes.

Ativar MFA

Ative o plug-in **Integração - Autenticação multifator** (com.snc.integration.multifactor.authentication) para começar a usar a MFA em uma instância. A MFA é ativada por padrão em ServiceNow.

Critérios multifatores

Use critérios multifatores para determinar quais usuários e funções devem usar a verificação multifator em duas etapas. É possível usar um desses critérios ou a combinação deles para atender às suas necessidades de negócios.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Critérios multifatores baseados no usuário

Use critérios multifatores com base no usuário para selecionar usuários individuais que precisam fazer login usando a MFA. Os administradores atualizam o campo **Habilitar autenticação multifator** em um registro de usuário para habilitar ou desabilitar os requisitos de MFA para um usuário. Para obter detalhes sobre este processo, consulte Configuração dos critérios multifatores baseados no usuário.

Critérios multifatores baseados em função

Use critérios multifatores baseados em função para exigir login por MFA para todos os usuários atribuídos a uma função específica. O registro de **Autenticação multifator baseada em função** na tabela **Critérios multifatores** [multi_factor_criteria] contém a lista de funções que exigem login por MFA. Para obter detalhes sobre como manter esta lista, consulte Configuração dos critérios multifatores baseados em função.

Critérios multifatores baseados em política de autenticação adaptável

Use a autenticação adaptável para determinar quando sua instância requer MFA. A autenticação adaptável usa políticas de autenticação para avaliar critérios como o endereço IP de um usuário ou grupos de usuários. Para obter detalhes sobre o recurso de autenticação adaptável, consulte Autenticação adaptável.

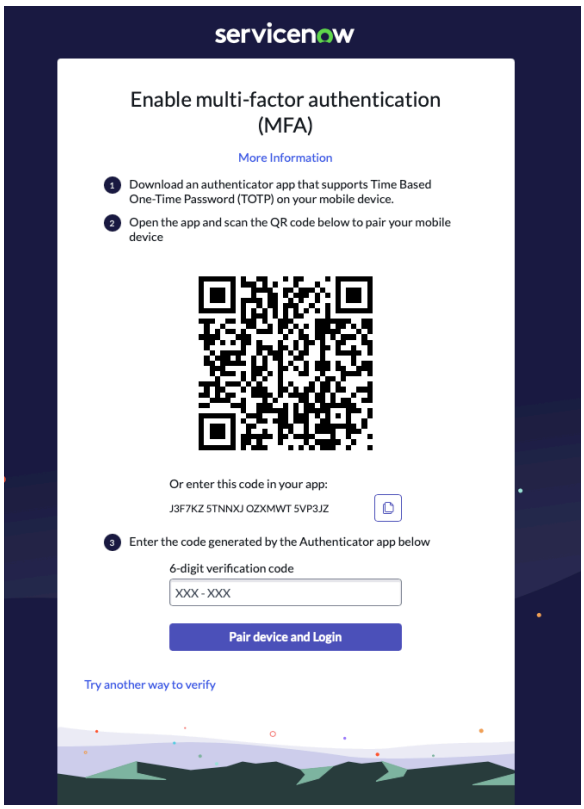
Métodos de autenticação multifator

Os usuários podem utilizar as opções abaixo, além do nome de usuário e da senha, para atender aos requisitos de autenticação multifator. Os usuários podem configurar fatores de MFA, como aplicações autenticadoras, scanners biométricos, chaves de hardware e SMS de forma independente.

Aplicações autenticadoras

Uma aplicação autenticadora é um software de terceiros que gera senhas temporárias. Os usuários podem usar essas senhas junto com sua senha para fazer login em uma instância que requer autenticação multifator (MFA). Para obter mais detalhes sobre essas aplicações, consulte Aplicações autenticadoras.

Siga as instruções na tela para configurar a aplicação autenticadora.

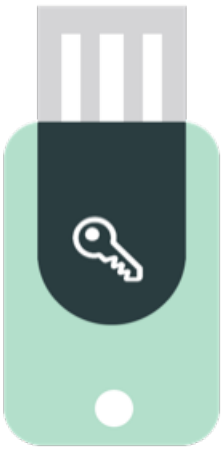


© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Scanners biométricos

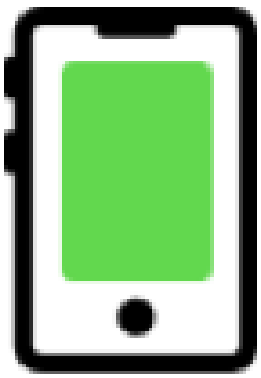
Autenticadores biométricos usam impressão digital ou reconhecimento facial para identificar usuários. Seus usuários podem usar esses autenticadores em seus dispositivos como parte do processo de login multifator. Para obter detalhes sobre como registrar autenticadores biométricos, consulte Registro de um autenticador biométrico.

Chaves de hardware



As chaves de hardware são hardware físico que pode ser usado para a autenticação. As chaves de hardware são inseridas em uma porta no seu dispositivo para fornecer autenticação. Para obter detalhes sobre como registrar chaves de hardware, consulte Registro da chave de segurança de hardware.

SMS



O administrador pode configurar a instância ServiceNow para exigir que os usuários tentem fazer login na instância usando OTP baseada em SMS.

Quando os usuários tentam fazer login em ServiceNow, a OTP do SMS é enviada para o número do celular associado ao registro sys_user. Os usuários podem inserir o código de verificação de seis dígitos enviado para o dispositivo móvel para verificar sua identidade.

Para obter mais informações, consulte Autenticação multifator com SMS.

E-mail

O administrador pode configurar a instância ServiceNow para exigir que os usuários tentem fazer login na instância usando OTP baseada em e-mail.

Quando os usuários tentam fazer login em ServiceNow, a OTP do e-mail é enviada para o endereço de e-mail do usuário. Os usuários

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

podem inserir o código de verificação de seis dígitos enviado para o endereço de e-mail para verificar sua identidade.

Para obter mais informações, consulte Autenticação multifator com e-mail.

Propriedades de autenticação multifator

Use as propriedades de autenticação multifator para habilitar, desabilitar e configurar a MFA em sua instância. Para obter detalhes sobre estas propriedades, consulte Propriedades do sistema de autenticação multifator.

Configuração de MFA, métodos compatíveis e fluxo de trabalho

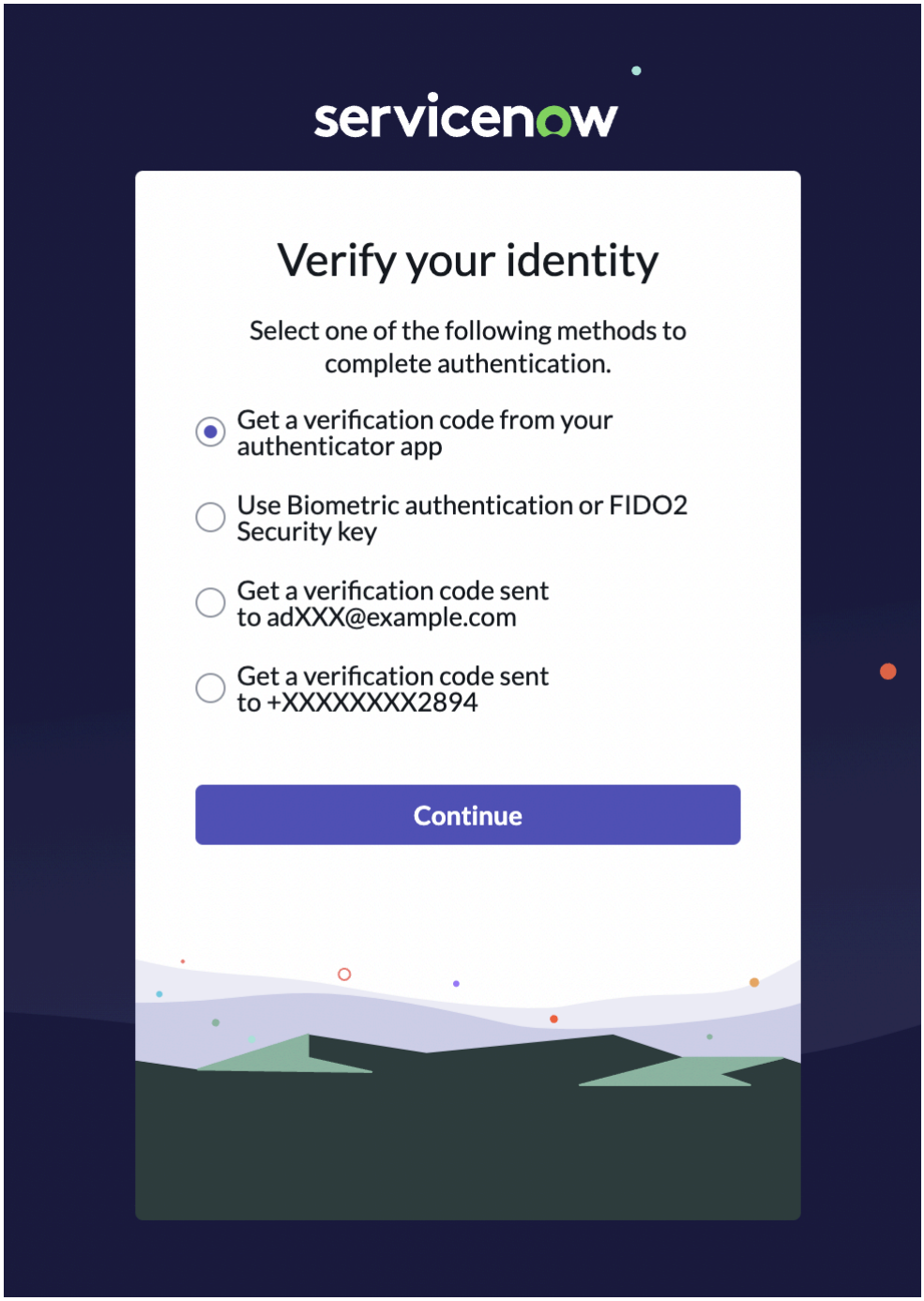
A MFA, também conhecida como verificação em duas etapas, é um requisito de segurança para que os usuários insiram mais de um conjunto de credenciais para acessar uma instância.

O nível básico de autenticação em uma instância é a autenticação de banco de dados local, em que um usuário insere uma combinação de nome de usuário e senha. A MFA oferece aos administradores e usuários a capacidade de exigir um segundo nível de autenticação.

O segundo nível de autenticação pode se basear nos seguintes elementos:

- Uma senha de um app de autenticação
- Uma chave de hardware
- Um autenticador biométrico, como um leitor de impressão digital ou reconhecimento facial.
- Um SMS ou e-mail

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Como administrador, é possível configurar a MFA para usuários individuais ou para todos os usuários de uma função específica. Também é possível permitir que os usuários aceitem a MFA e a utilizem.

Ativação

O plug-in *Integration - Multifactor Authentication* (com.snc.integration.multifactor.authentication) é instalado por padrão em sua instância, mas deve ser habilitado por um administrador usando uma propriedade do sistema. Para obter detalhes, consulte Propriedades do sistema de autenticação multifator.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Depois de clonar uma instância, você deve habilitar novamente a MFA na instância clonada. Para mais informações, consulte os seguintes artigos da base de conhecimento: KB0657100, KB0860689, KB0825390, KB0779908, KB0717367 e KB0727991.

Métodos de autenticação compatíveis

É possível usar a MFA com os seguintes métodos de autenticação:

- Autenticação de banco de dados local (autenticação nativa ServiceNow)
- Integração LDAP
- SSO SAML
- SSO OIDC

Fluxo de trabalho da configuração de autenticação multifator

O administrador ativa a autenticação multifator

O plug-in **Integration - Autenticação multifator** (com.snc.integration.multifactor.authentication) é ativado na sua instância por padrão. Para começar a usar a MFA, os administradores devem habilitar a MFA usando uma propriedade do sistema. Depois de habilitado, os administradores selecionam usuários ou funções que exigem logins MFA.

Para obter mais detalhes sobre a configuração do administrador para MFA, consulte Autenticação multifator (MFA).

Os usuários fazem login usando um aplicativo de autenticação

Os usuários devem usar as opções de MFA para o login. Os usuários podem escolher qualquer uma das opções para concluir a MFA e, se algum usuário tiver concluído a configuração usando qualquer fator, ele ainda poderá acessar a página de perfil e concluir a configuração dos fatores restantes, se quiser.

Autenticação da Web

Ative *Integration - Web Authentication* (com.snc.integration.webauthn) para permitir a autenticação da chave de hardware ou do leitor biométrico em sua instância.

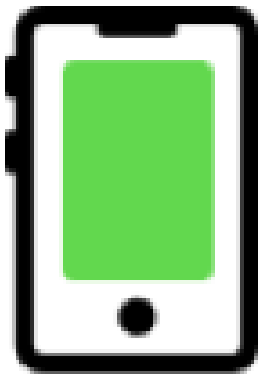
As chaves de hardware são hardware físico que pode ser usado para a autenticação. As chaves de hardware são inseridas em uma porta no seu dispositivo para fornecer autenticação. Para obter detalhes sobre como registrar chaves de hardware, consulte Registro da chave de segurança de hardware.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Autenticadores biométricos usam impressão digital ou reconhecimento facial para identificar usuários. Seus usuários podem usar esses autenticadores em seus dispositivos como parte do processo de login multifator. Para obter detalhes sobre como registrar autenticadores biométricos, consulte Registro de um autenticador biométrico.

SMS ou e-mail (senha de uso único)

Para permitir que os usuários façam login em uma instância ServiceNow e tenham uma experiência mais tranquila em dispositivos móveis, a MFA é compatível com SMS e e-mail.



O administrador pode configurar a instância ServiceNow para exigir que os usuários tentem o login na instância usando OTP baseada em SMS.

Quando os usuários tentam fazer login em ServiceNow, a OTP do SMS é enviada para o número do celular associado ao registro sys_user. Os usuários podem inserir o código de verificação de seis dígitos enviado para o dispositivo móvel para verificar sua identidade.

Para obter mais informações, consulte Autenticação multifator com SMS.

O administrador pode configurar a instância ServiceNow para exigir que os usuários tentem o login na instância usando OTP baseada em e-mail.

Quando os usuários tentam fazer login em ServiceNow, a OTP do e-mail é enviada para o endereço de e-mail associado ao usuário. Os usuários podem inserir o código de verificação de seis dígitos enviado para o endereço de e-mail para verificar sua identidade.

Para obter mais informações, consulte Autenticação multifator com e-mail.

Propriedades do sistema de autenticação multifator

Use as propriedades do sistema para habilitar e personalizar a MFA para atender aos seus requisitos de segurança.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Propriedades de autenticação multifator

Propriedade	Descrição
Ativar autenticação multifator (*glide.authenticate.multifactor*)	Opção que permite que usuários e administradores usem este recurso. O padrão está habilitado. Para aprender mais sobre essa propriedade, consulte Habilitar autenticação multifator (MFA) nas Configurações de proteção de segurança de instância.
Número de vezes que um usuário pode ignorar a autenticação multifator (*glide.authenticate.multifactor.setup.bypass.count*)	Número de vezes que um usuário pode optar por ignorar a configuração de MFA. Seus usuários ainda podem fazer login na instância mesmo se não tiverem um dispositivo móvel em mãos. O contador será reiniciado se este recurso for desativado e, depois, reativado. O padrão é 3.
O tempo em minutos que o código único enviado para o endereço de e-mail do usuário é válido (*glide.multifactor.onetime.code.validity*)	Número de minutos em que o código de redefinição é válido. Consulte Login com autenticação multifator. O padrão é 5. **Nota:** Essa propriedade se refere ao tempo de validação da OTP de e-mail.
Tempo adicional, em segundos, em que o código será válido para acomodar distorções do relógio. O valor máximo é de 60 segundos. (*glide.authenticate.multifactor.clock_skew*)	Número de segundos adicionais em que o código de redefinição é válido. O máximo é `60`. O padrão é `10`. A instância valida o código inserido pelo usuário em relação ao único código gerado pelo app, que é gerado no `horário atual`. É possível distorcer a janela de tempo com essa propriedade e permitir que um ou mais códigos sejam gerados durante uma janela de tempo para serem considerados válidos. O valor da propriedade é usado no seguinte cálculo: `hora atual - X/2` e `hora atual + X/2`, em que `X` é o valor desta propriedade. Por exemplo, se o valor de `10` for usado, a instância considerará válidos todos os códigos gerados pelo app dentro do intervalo de tempo `[a hora atual - 5 segundos]` e `[a hora atual + 5 segundos]`. Use essa propriedade para evitar problemas de login em que o usuário não consiga inserir o código correto no tempo-padrão alocado.
Habilitar opção para lembrar o recurso do navegador na autenticação multifator. (*glide.authenticate.multifactor.remember.browser.enable*)	Defina sua instância para solicitar a MFA de um usuário quando ele fizer login em um novo dispositivo ou navegador. O padrão é sim.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Propriedades de autenticação multifator

Propriedade	Descrição
Validade da impressão digital do navegador em horas. (*glide.authenticate.multifactor.browser.fingerprint.validity*)	Quando a MFA memoriza o navegador, o usuário não é solicitado a fazer um novo procedimento de MFA no mesmo navegador durante esse período. O padrão é 8 horas.
Número máximo de navegadores que um usuário pode memorizar. (*glide.authenticate.multifactor.remembered.browser.max.count*)	O número de navegadores que a MFA memorizou para este usuário.
Valor-padrão da caixa de seleção para memorizar o navegador na página de validação multifator. (*glide.authenticate.multifactor.remember.browser.default*)	Valor-padrão da caixa de seleção para memorizar o navegador na página de validação multifator.
Habilitar autenticação da Web (FIDO2) com base na MFA (*glide.webauthn.enabled*)	Opção para habilitar métodos de autenticação sem senha, como chave de hardware e autenticação biométrica.
Habilitar envio de OTP por e-mail para a autenticação multifator (*glide.authenticate.multifactor.email.otp.enable*)	Opção para ativar a OTP baseada em e-mail como um fator da MFA.
Habilitar a IU aprimorada de configuração da MFA para permitir que os usuários configurem o fator independentemente. *glide.auth.mfa.ui.v2.enabled*	Opção para ativar o fator de MFA de forma independente para os usuários sem configurar um app autenticador.

Critérios da autenticação multifato

Use critérios multifatores para determinar quais usuários e funções devem usar a verificação multifator em duas etapas.

É possível usar um desses critérios ou a combinação deles para atender às suas necessidades de negócios.

Nota: É recomendável usar a MFA baseada na política de Autenticação adaptável.

Critérios da autenticação multifato

Critérios	Descrição
Critérios multifatores baseados no usuário	Use critérios multifatores com base no usuário para selecionar usuários individuais que precisam fazer login usando a MFA. Os administradores atualizam o campo **Habilitar autenticação multifator** em um registro de usuário para habilitar ou desabilitar os requisitos de MFA para um usuário. Para obter detalhes sobre este processo, consulte Configuração dos critérios multifatores baseados no usuário.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Critérios da autenticação multifato

Critérios	Descrição
Critérios multifatores baseados em função	Use critérios multifatores baseados em função para exigir login por MFA para todos os usuários atribuídos a uma função específica. O registro de **Autenticação multifator baseada em função** na tabela **Critérios multifatores** [multi_factor_criteria] contém a lista de funções que exigem login por MFA. Para obter detalhes sobre como manter esta lista, consulte Configuração dos critérios multifatores baseados em função.
Critérios multifatores baseados em política de autenticação adaptável	Use a autenticação adaptável para determinar quando sua instância requer MFA. A autenticação adaptável usa políticas de autenticação para avaliar critérios como o endereço IP de um usuário ou grupos de usuários. Para obter detalhes sobre o recurso de autenticação adaptável, consulte Autenticação adaptável.

Configuração dos critérios multifatores baseados no usuário

Use critérios multifatores baseados no usuário para habilitar a MFA para um usuário.

Antes de Iniciar
Função necessária: administrador

Procedimento

1. Navegue até **Todos** > **Administração de usuários** > **Usuários**.
2. Configure a lista para exibir a coluna **Habilitar autenticação multifator**.
3. Altere os valores da coluna **Habilitar autenticação multifator** dos usuários selecionados para **verdadeiro**.

   Quando o usuário faz login com seu nome de usuário e senha, ele é solicitado a configurar a autenticação multifator.

Configuração dos critérios multifatores baseados em função

Use critérios multifatores baseados em função para impor a autenticação multifator para todos os usuários atribuídos a funções específicas.

Antes de Iniciar
Função necessária: administrador

Procedimento

1. Navegue até **Todos** > **Autenticação multifator** > **Critérios multifatores**.
2. Na lista **Critérios multifatores**, abra o registro de **Autenticação multifator baseada em função**.
3. Use a lista **Funções multifatores** para adicionar ou remover funções.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
Adicionar uma função	Clique duas vezes em **Inserir uma nova linha...** e insira ou selecione um nome de função. Clique no **ícone Salvar** ( ) para salvar a entrada.
Remover uma função	Clique no ícone de exclusão ( ) para remover uma função da lista.

4. Clique em **Atualizar**.

Resultados
Sua instância impõe autenticação multifator para todos os usuários membros das funções listadas na lista **Funções multifatores**.

Importante: O registro deve estar ativo para impor a autenticação multifator baseada em função.

Configuração de critérios multifatores baseados em política de autenticação adaptável

Use políticas adaptáveis para determinar quais usuários devem usar a verificação multifator (MFA) em duas etapas.

Antes de Iniciar
Função necessária: administrador

Nota:

- Se a política padrão for a **Política de MFA em etapa crescente**, a autenticação multifator será mostrada aos usuários caso a política configurada na **Política de MFA em etapa crescente** seja avaliada como verdadeira. A política tem precedência sobre a configuração baseada em função ou em usuário.
- A MFA com login SSO estará disponível apenas se a propriedade `glide.authenticate.mfa.with.multisso.enabled` estiver definida como verdadeira.
- É possível navegar até o registro da Política de autenticação para adicionar ou editar as "Entradas de política" nos campos de política referenciados (**Política de MFA em etapa crescente** ou **Política de MFA em etapa decrescente**).

Procedimento

1. Navegue até **Todos** > **Autenticação adaptável** > **Contextos da política de autenticação** > **Contexto de MFA**.
   O registro de contexto da política de **contexto de MFA** é aberto.
2. Selecione a política-padrão no campo **Política-padrão**.
   Esta seleção determina como sua instância usa as condições de política para determinar se a MFA deve ser solicitada.

Políticas-padrão

Política-padrão	Definição
Política de MFA em etapa crescente	Selecione para impor a MFA quando as condições de política definidas na

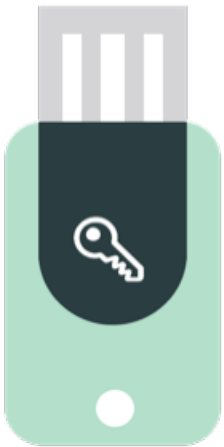
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Política-padrão	Definição
	Política de MFA em etapa crescente forem avaliadas como verdadeiras.
Política de MFA em etapa decrescente	Selecione para ignorar a MFA quando as condições de política definidas na **Política de MFA em etapa decrescente** forem avaliadas como verdadeiras.

3. No campo **Política de MFA em etapa crescente**, selecione uma política para uso com este contexto.
4. Clique em **Atualizar**.
   Depois de salvar o registro, as listas **Entrada de política** e **Condições de política** são atualizadas para exibir as entradas e condições de política associadas à política selecionada no campo **Política de MFA em etapa crescente**.

Autenticação da web — MFA

Use **Integração — Autenticação da web (com.snc.integration.webauthn)** para permitir a autenticação com chave de hardware ou leitor biométrico na sua instância.



As chaves de hardware são hardware físico que pode ser usado para a autenticação. As chaves de hardware são inseridas em uma porta no seu dispositivo para fornecer autenticação. Para obter detalhes sobre como registrar chaves de hardware, consulte Registro da chave de segurança de hardware.

Autenticadores biométricos usam impressão digital ou reconhecimento facial para identificar usuários. Seus usuários podem usar esses autenticadores em seus dispositivos como parte do processo de login multifator. Para obter detalhes sobre como registrar autenticadores biométricos, consulte Registro de um autenticador biométrico.

Configurar MFA com biometria

Os administradores podem usar a lista Credenciais públicas do usuário para exibir e gerenciar as credenciais criadas pelo usuário.

Quando um usuário registra uma aplicação autenticadora, autenticação biométrica ou chave de hardware, sua instância cria um registro na tabela **Credenciais públicas do**

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

usuário[sys_user_public_credential]. Use a tabela para verificar quais usuários registraram um autenticador, bem como quais tipos e quando eles foram registrados e usados. Também é possível marcar esses registros como inativos para evitar que as credenciais sejam usadas pelos usuários.

Formulário Credencial pública do usuário

Campo	Descrição
Apelido da credencial	Apelido para a credencial. Este apelido é escolhido pelo usuário ao registrar um autenticador.
Usuário	Usuário associado à credencial
Ativo	Especifique se esta credencial está ativa. Os administradores podem definir um registro como inativo para impedir que um usuário seja autenticado com essa credencial.
Autenticador	O tipo de autenticador registrado pelo usuário.
Hora de registro	A data e a hora em que a credencial foi criada pelo usuário
Hora do último uso	A última data e hora em que o usuário fez login com a credencial.

Tipos de autenticador restritos

Se você restringiu um método de autenticação, como autenticadores biométricos, os usuários não poderão criar novas credenciais desse tipo. No entanto, todas as credenciais criadas antes da criação da restrição continuarão funcionando. É possível desabilitar registros na tabela **Credenciais públicas do usuário** para impedir que essas credenciais sejam usadas após terem sido criadas.

Opções de configuração do autenticador

Use a página Configuração do autenticador para gerenciar as opções do autenticador em sua instância.

Navegue até **Autenticação multifator** > **Autenticador da Web** > **Configuração do autenticador** para ver e editar as opções de configuração padrão.

Formulário Configuração do autenticador

Campo	Descrição
Tipo de autenticador permitido	Tipo de autenticadores que podem ser registrados. Selecione entre: • Os autenticadores de **plataforma** são anexados ou integrados a um dispositivo. Leitores de impressão digital ou reconhecimento facial disponíveis em dispositivos móveis (como Apple FaceID ou TouchID) se enquadram nesta categoria.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formulário Configuração do autenticador

Campo	Descrição
	• Autenticadores de **roaming** podem ser removidos de um computador ou outro dispositivo do cliente e usados em outro lugar. As chaves de hardware se enquadram nesta categoria.
Tipo de certificação	Definir o valor como direto ou indireto exigirá a importação de metadados do autenticador para atestar a origem de um autenticador durante o registro. • Nenhum • Direto • Indireto
Autocertificação de plataforma	Determina se a auto-certificação está habilitada para autenticadores de plataforma.
Autocertificação de plataforma	Determina se a auto-certificação está habilitada para autenticadores de roaming.
Verificação de usuário	Selecione entre **Preferencial** ou **Obrigatório**. Se necessário, o fluxo de autenticação da Web solicitará aos usuários a verificação usando PIN ou biometria.
Verificar presença do usuário	Determina se o fluxo de autenticação da Web requer a verificação de presença do usuário.
Chave residente	Selecione entre **Preferencial** ou **Obrigatório**. Se necessário, o autenticador mantém as credenciais de chave pública no armazenamento do autenticador.
Tempos limites (ms)	Limite de tempo máximo para concluir o registro e a autenticação da autenticação da Web. O tempo é mostrado em milissegundos.

Autenticação multifator com SMS

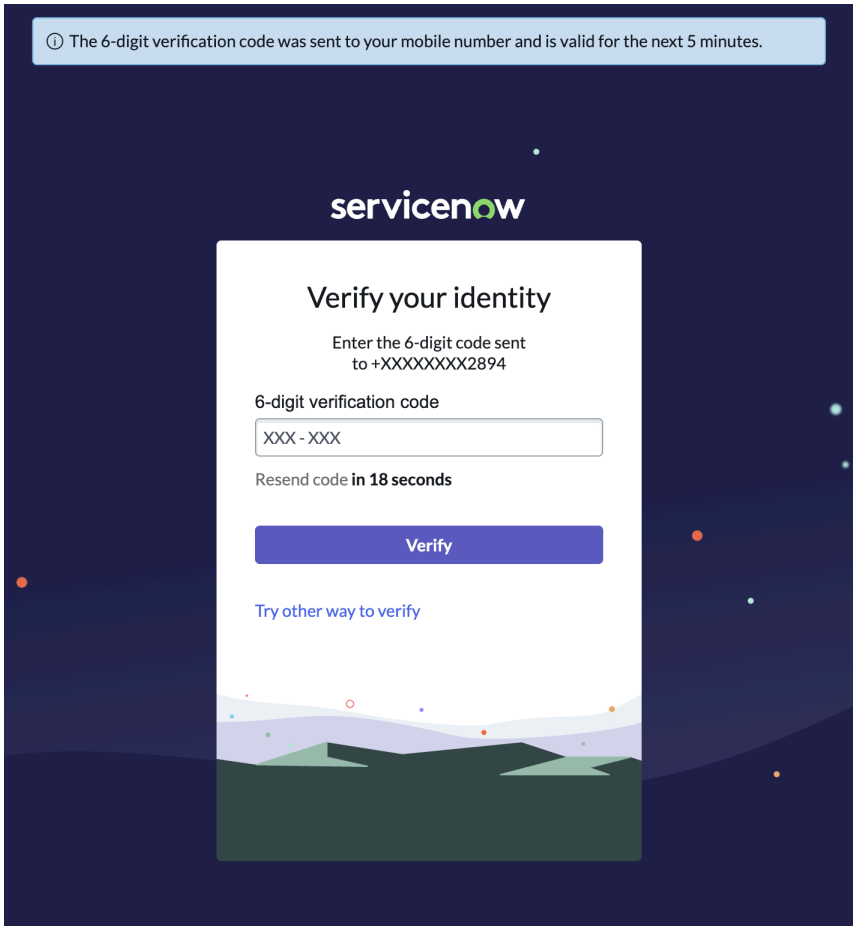
Autenticação multifator (MFA) com SMS como um fator para a sua autenticação.

O administrador pode configurar a instância ServiceNow para exigir que os usuários tentem o login na instância usando OTP baseada em SMS.

Quando os usuários tentam fazer login em ServiceNow, a OTP do SMS é enviada para o número do celular associado ao registro sys_user. Os usuários podem inserir o código de verificação de seis dígitos enviado para o dispositivo móvel para verificar sua identidade.

Também é possível configurar o MFA com SMS usando o Twilio pronto para uso. Para obter mais informações, consulte Provedores de autenticação multifator.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Além disso, a MFA com SMS pode ser controlada com base na entrada da política e nas condições usando critérios de filtro. Estes são os tipos de critérios de filtro:

- Critérios de filtro por IP
- Critérios de filtro por função
- Critérios de filtro por grupo

Ativação da MFA com o plug-in SMS

Para MFA com SMS, instale o plug-in Autenticação multifator com SMS (`com.snc.authentication.sms_mfa`).

Antes de Iniciar

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

Os itens a seguir são instalados com a autenticação multifator com SMS:

- Autenticação adaptável (`com.snc.adaptive_authentication`
- Notify - Twilio Direct Driver (`com.snc.notify.twilio_direct`)

Plug-in dependente: Integration - Autenticação multifator (`com.snc.integration.multifactor.authentication`)

Nota: É possível carregar os dados de demonstração ao instalar o plug-in se provedor personalizado estiver sendo configurado para gerar o SMS.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegue até **Todos** > **Aplicações do sistema** > **Todas as aplicações disponíveis** > **Todas**.
2. Encontre o plug-in Autenticação multifator with SMS (`com.snc.authentication.sms_mfa`) usando os critérios de filtro e a barra de pesquisa.

   Pesquise o plug-in pelo nome ou ID. Se não conseguir encontrar um plug-in, talvez seja necessário solicitá-lo ao pessoal ServiceNow.

3. Selecione **Instalar** para iniciar o processo de instalação.

   Nota: Quando a separação de domínio e o administrador delegado estão habilitados em uma instância, o usuário administrativo deve estar no domínio **global**. Caso contrário, será exibido o seguinte erro: `A instalação da aplicação não está disponível porque há outra operação em execução: ativação de plug-in para <plugin name>.`

   Você verá uma mensagem após a conclusão da instalação.

Configuração de SMS como fator de MFA

Configure a entrada de política e a condição para exibir OTP de SMS como uma política de fator de MFA para autenticação.

Antes de Iniciar

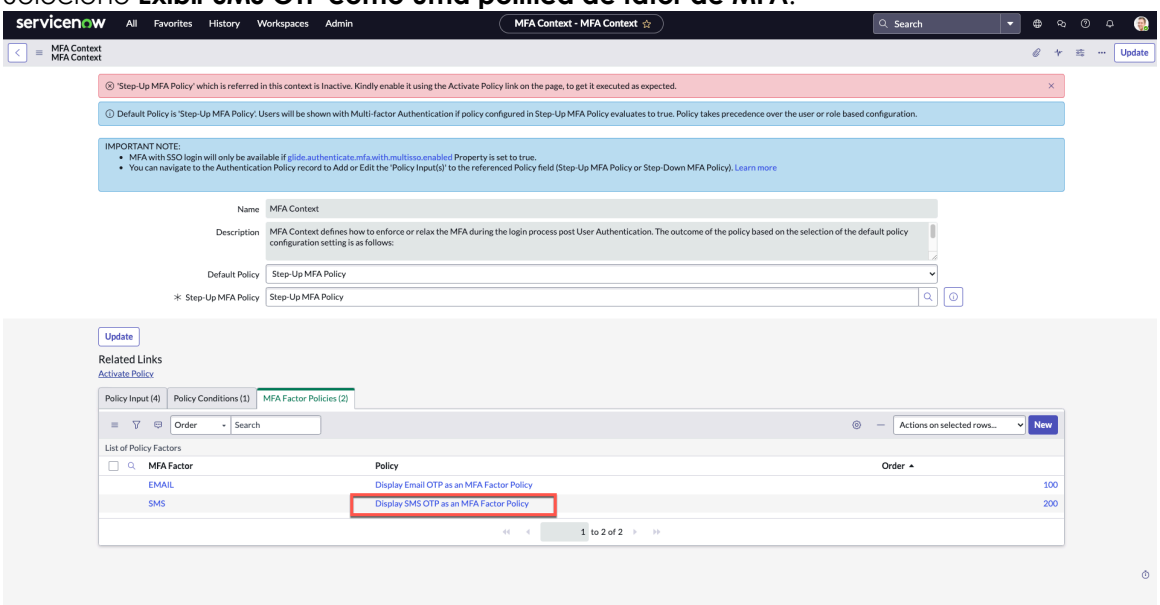
Plug-in necessário: Autenticação multifator com SMS (`com.snc.authentication.sms_mfa`).

Função necessária: administrador

Nota: A política de contexto da MFA deve ser avaliada como `verdadeira` para aplicar a política de fator de SMS.

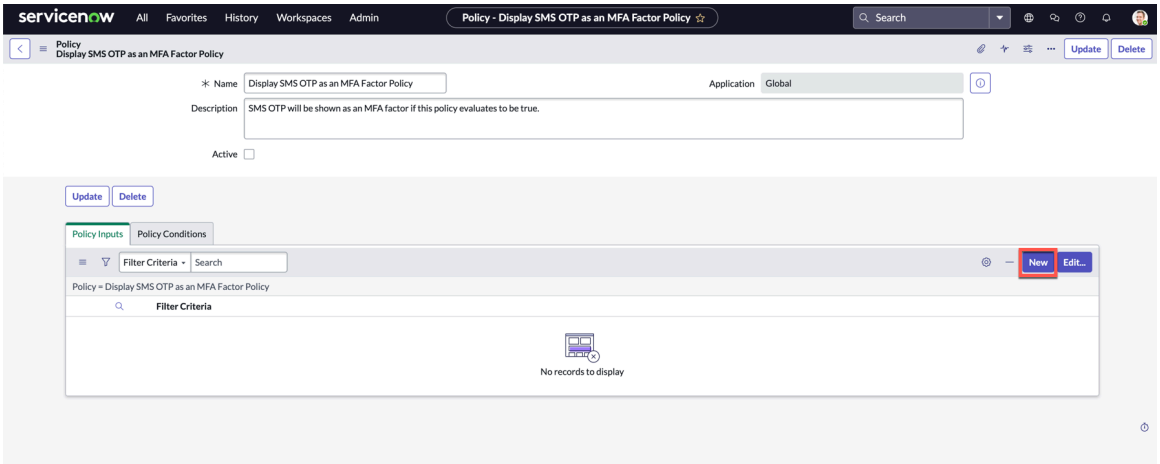
Procedimento

1. Navegue até **Todos** > **Autenticação multifator** > **Contexto de MFA**.
2. Clique na guia **Políticas do fator de MFA**.
3. Selecione **Exibir SMS OTP como uma política de fator de MFA**.



4. Clique em **Novo** para adicionar **Entradas de política**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

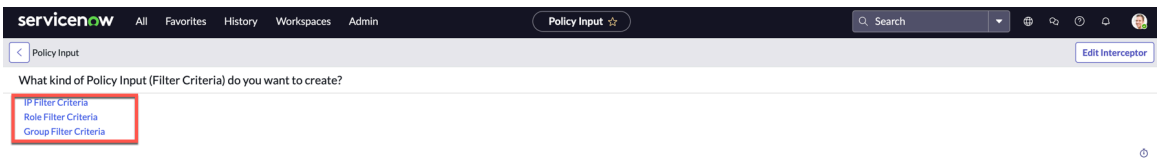


5. Selecione os critérios de filtro que deseja criar.

   Estes são os tipos de critérios de filtro:

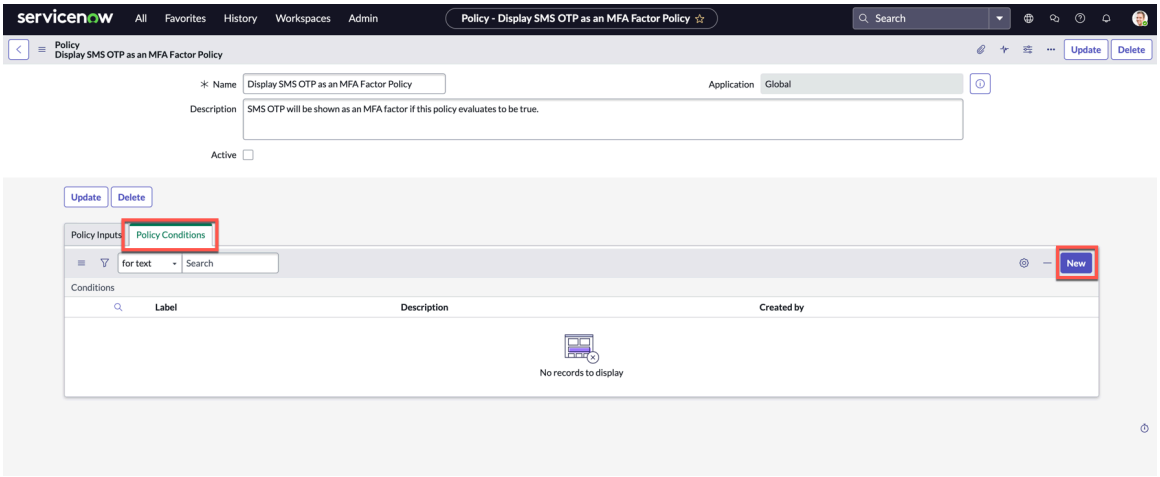
   - Critérios de filtro por IP
   - Critérios de filtro por função
   - Critérios de filtro por grupo

   Por exemplo, Critérios de filtro por função.



6. Clique em **Critérios de filtro por função**, preencha os campos dos critérios de filtro por função e envie o registro.
   A nova política é criada. Para obter mais informações, consulte Critérios de filtro por função.
7. Na página Política - Exibir OTP de SMS como um fator de MFA, clique em Condições da política.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



8. Clique em **Novo** para adicionar **Condições da política**.
9. No formulário, preencha os campos.

Formulário Condição

Campo	Descrição
Rótulo	Nome para identificar a condição.
Descrição	Descrição da condição.
Condição	Combinação lógica de várias entradas de política (critérios de filtro) para avaliar solicitações de autenticação. Selecione a política de critérios de filtro baseada em função que foi criada para a condição.

10. Clique em **Enviar**.
11. Opcional: Repita a etapa 8 para criar condições de política adicionais.

> **Nota:** Se várias condições de política forem criadas, a saída final da política de acesso dependerá da lógica OU da saída de todas as condições de política. Isso significa que a política é avaliada como verdadeira se qualquer uma das condições de política for atendida.

Com base na política de filtro de função (usuários) e nas condições especificadas para a função, o fator de SMS como MFA é mostrado como uma opção de autenticação para os usuários.

Provedores de autenticação multifator

Use provedores de MFA para configurar a autenticação baseada em SMS e e-mail, garantindo que todos os usuários possam fazer login com segurança.

Em Now Platform, é possível configurar provedores de MFA com o mecanismo de autenticação multifator, como e-mail e SMS.

É possível usar a seguinte configuração de provedor disponível para MFA em Now Platform:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Configuração do provedor de e-mail
- Configuração do provedor Twilio
- Configuração do provedor Infobip.

Nota: A configuração dos provedores Twilio e Infobip é preenchida automaticamente ao habilitar o carregamento de dados de demonstração na instalação da autenticação multifator com plug-ins SMS (`com.snc.authentication.sms_mfa`) e Notify — Twilio Direct Driver (`com.snc.notify.twilio_direct`).

Também é possível criar sua própria configuração de provedor para habilitar a autenticação multifator com SMS e e-mail.

Nota: A configuração do provedor Infobip é fornecida como parte dos dados de demonstração. É possível editar os campos com base em seus requisitos para configurar seu próprio provedor.

Configuração de provedor MFA

Configure SMS e e-mail com o provedor para garantir que todos os usuários possam fazer login com segurança.

Antes de Iniciar

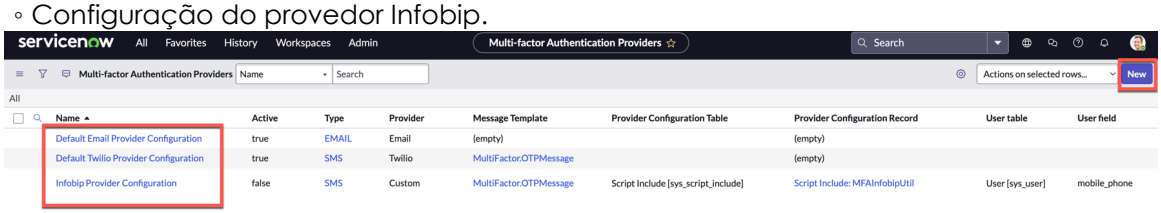
Função necessária: administrador

Procedimento

1. Navegue até **Todos** > **Autenticação multifator** > **Provedores**.

   A configuração do provedor a seguir está disponível para MFA em Now Platform:

   - Configuração do provedor de e-mail
   - Configuração do provedor Twilio
   - Configuração do provedor Infobip.



2. Para criar um novo provedor, clique em **Novo**.
3. No formulário, preencha os campos.

Formulário Condição

Campo	Descrição
Nome	Nome do registro.
Tipo	Descrição do registro.
Provedor	Escolha **Twilio** ou **Personalizado**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: Para configurar o Twilio, consulte Configurar o Notify com o Twilio. Ao escolher **Personalizado**, é preciso especificar os seguintes campos: ◦ Tabela Configuração do provedor ◦ Registro Configuração do provedor ◦ Script ◦ Tabela Usuário ◦ Campo de usuário
Modelo da mensagem	O modelo da mensagem do registro.
Ativo	Opção para ativar a configuração do provedor.

4. Clique em **Enviar**.

   Com base no modelo da mensagem e nas configurações do provedor, o SMS ou e-mail é enviado aos usuários como um fator de autenticação durante o processo de login.

Configuração personalizada do provedor Vonage (tutorial)

Configure um SMS com o provedor Vonage para garantir que todos os usuários possam fazer login com segurança.

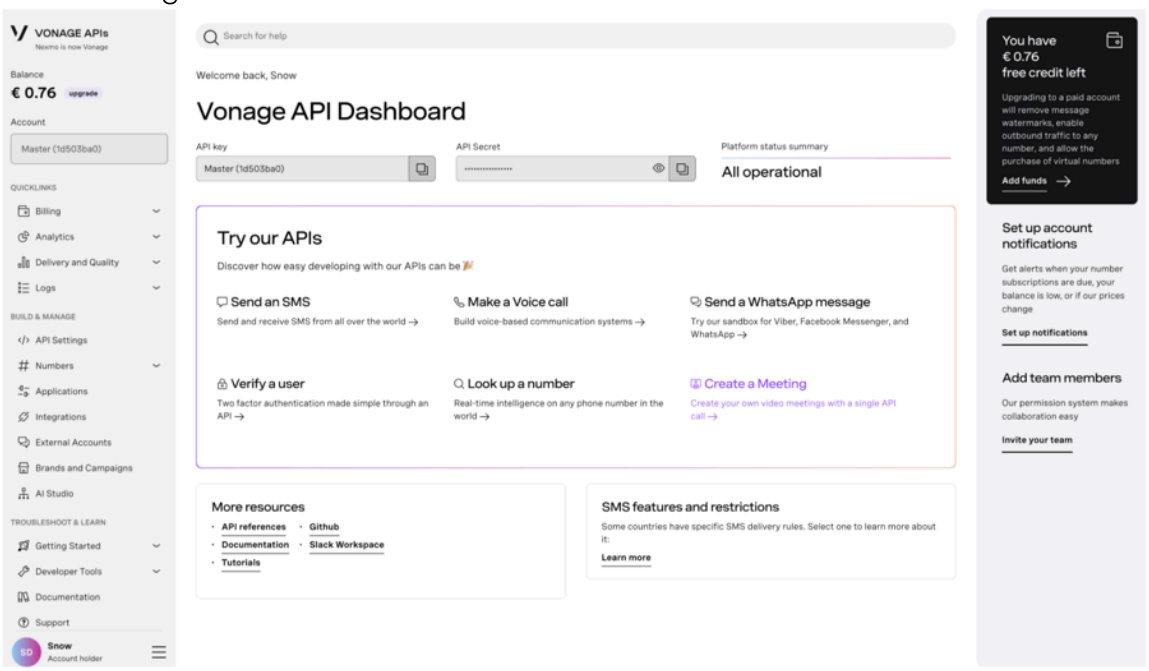
Antes de Iniciar

Função necessária: administrador

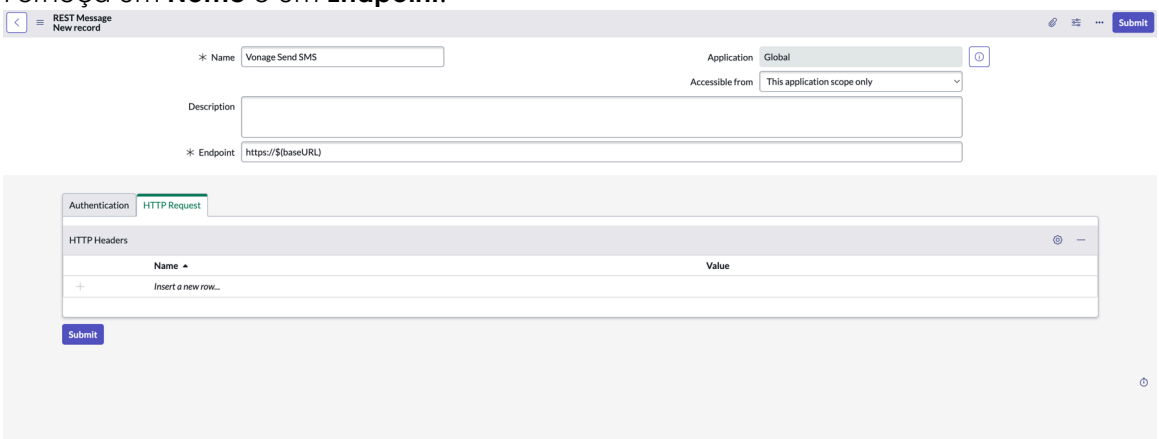
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegue até **Todos** > **Serviços Web do sistema** > **Saída** > **Mensagem REST** e execute a configuração da mensagem REST com base nas informações do painel de controle de API do Vonage.

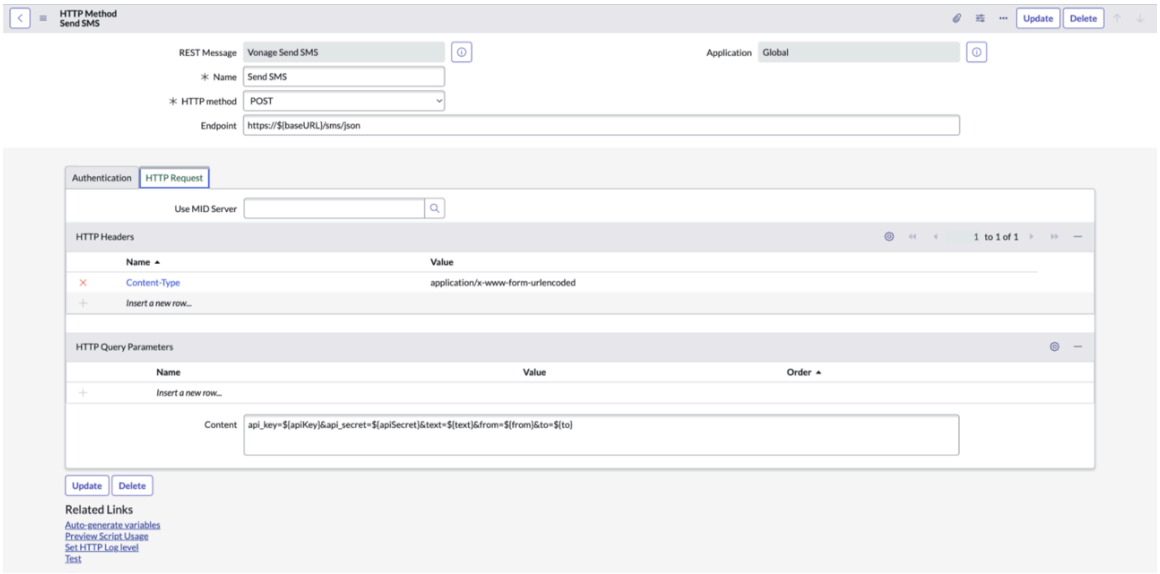


2. Clique em **Novo** para criar uma nova **Mensagem REST**.
3. Forneça um **Nome** e um **Endpoint**.



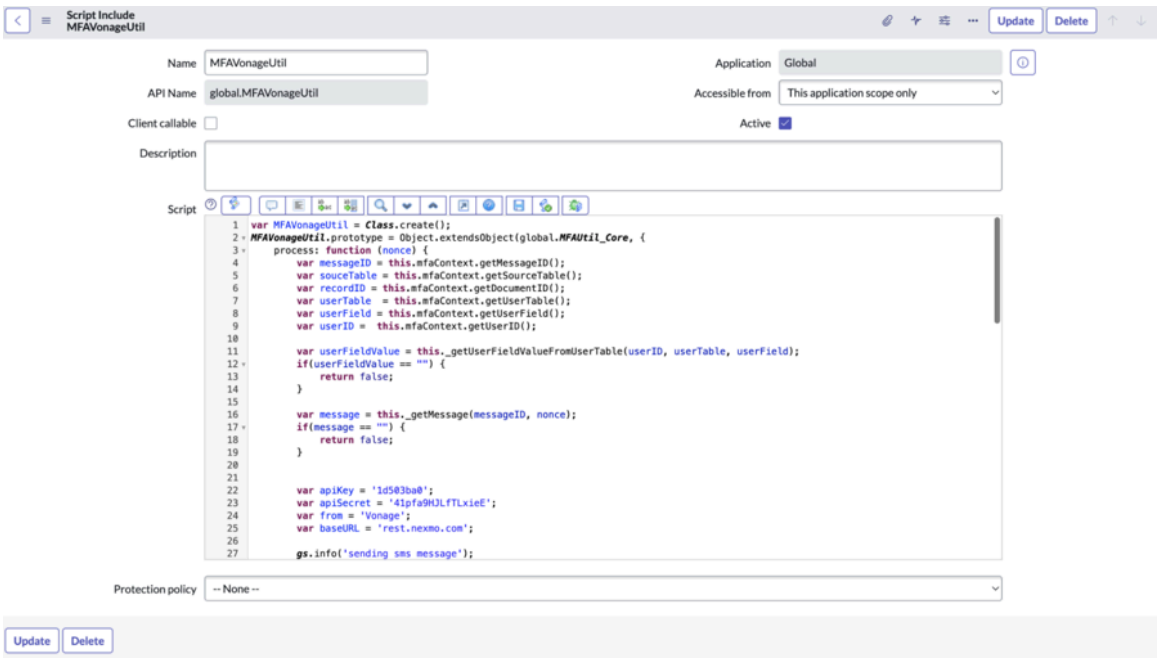
4. Clique em **Enviar**.
5. Abra o registro criado, na lista relacionada **Métodos HTTP** , clique em **Novo** e selecione o método HTTP como **POST**.
6. Preencha os seguintes campos:
   - Endpoint: `https://${baseURL}/sms/json`
   - Conteúdo:`api_key=${apiKey}&api_secret=${apiSecret}&text=${text}&from=${from}&to=${to}`
   - Tipo de conteúdo: `application/x-www-form-urlencoded`

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



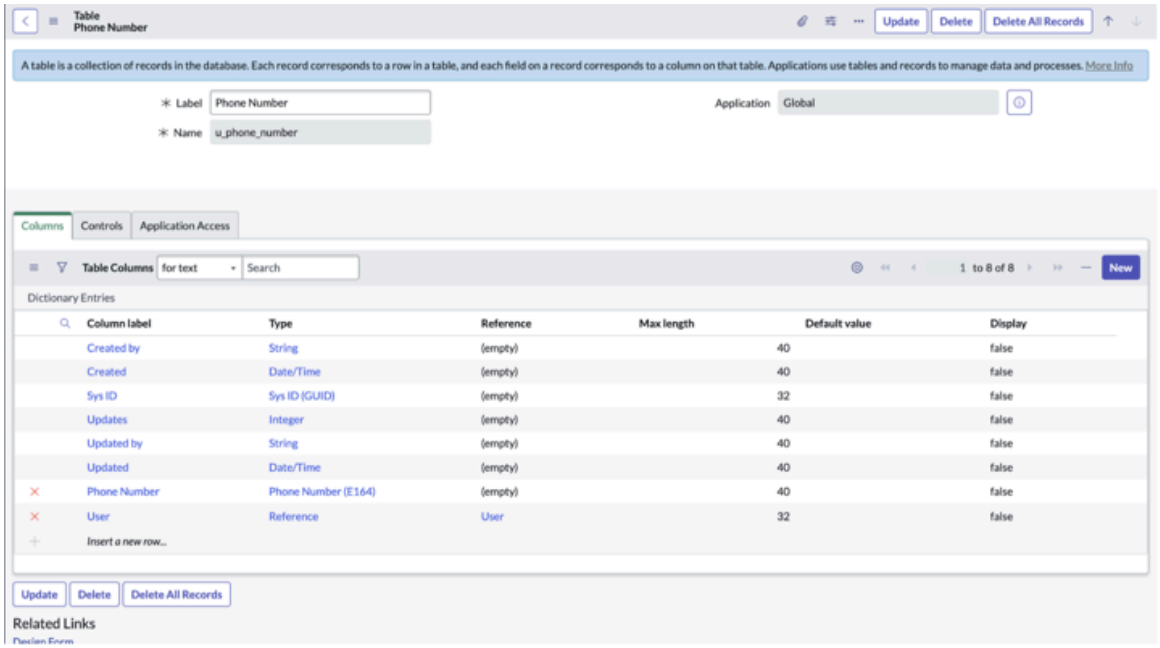
7. Atualize o registro.
8. Clique em **Gerar variáveis automaticamente** na seção **Links relacionados**.
9. Importe o SI compartilhado na pasta e copie a apiKey e o segredo do painel da API do Vonage.

> **Nota:**
>
> A apiKey e o segredo estão localizados nas configurações da sua conta do Vonage no Painel do Vonage.

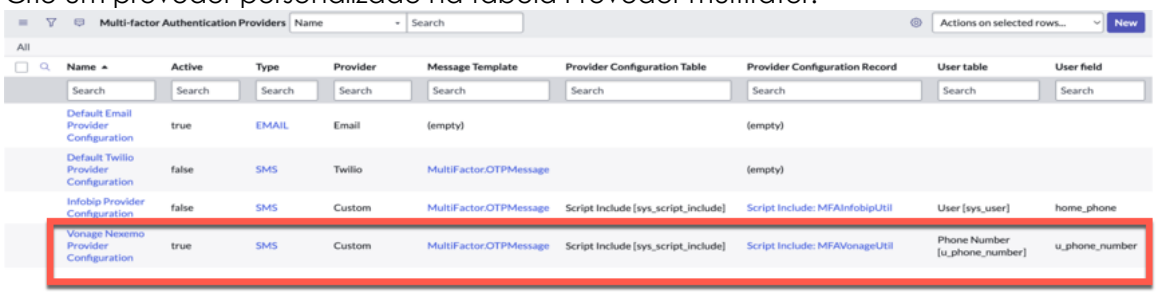


10. Crie uma tabela personalizada de Números de telefone com duas colunas, por exemplo:
    - **Rótulo da coluna**: Usuário, **Tipo**: referência, **Referência**: usuário (sys_user).
    - **Rótulo da coluna**: Número de telefone, **Tipo**: número de telefone (E164).

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



11. Crie um provedor personalizado na tabela Provedor multifator.



Para saber mais sobre a configuração de provedores, consulte Configuração de provedor MFA.

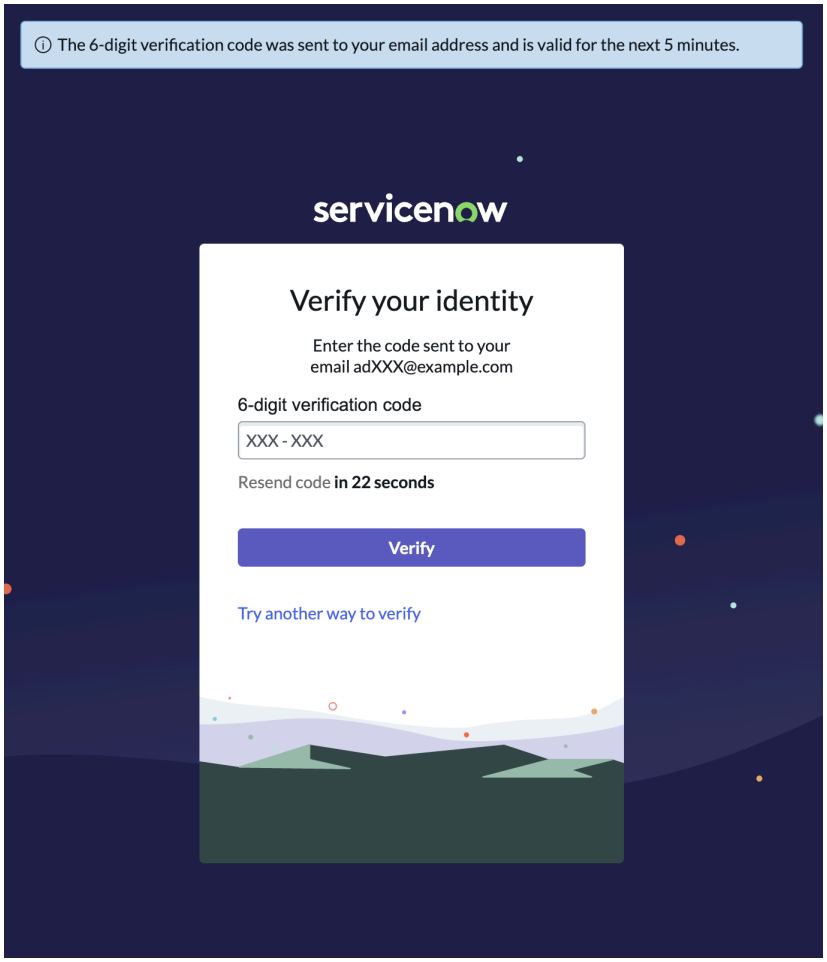
Autenticação multifator com e-mail

Autenticação multifator (MFA) com e-mail como um fator para a sua autenticação.

O administrador pode configurar a instância ServiceNow para exigir que os usuários tentem o login na instância usando OTP baseada em e-mail.

Nota: O MFA com e-mail é ativado com o plug-in Integração - Autenticação Multifator (`com.snc.integration.multifactor.authentication`) por padrão. É necessário configurar as entradas e condições da política.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Quando os usuários tentam fazer login em ServiceNow, a OTP do e-mail é enviada para o endereço de e-mail associado. Os usuários podem inserir o código de verificação de seis dígitos enviado para o endereço de e-mail para verificar sua identidade.

Configuração de e-mail como fator de MFA

Configure a entrada de política e a condição para exibir OTP de e-mail como uma política de fator de MFA para autenticação.

Antes de Iniciar

Função necessária: administrador

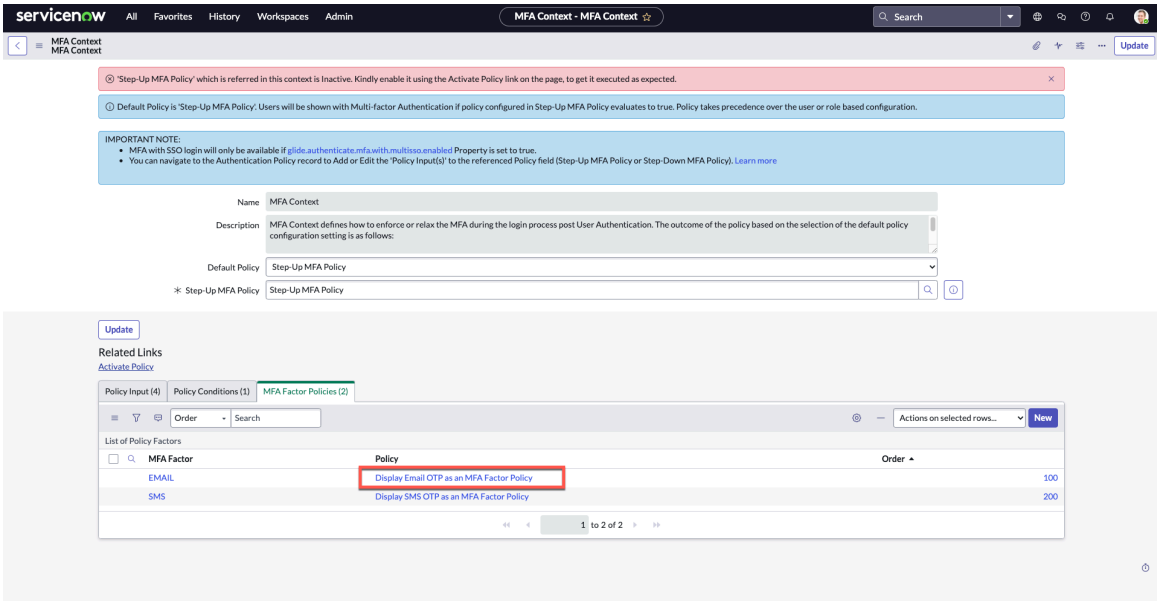
Procedimento

1. Navegue até **Todos** > **Autenticação multifator** > **Contexto de MFA**.
2. Clique na guia **Políticas do fator de MFA**.

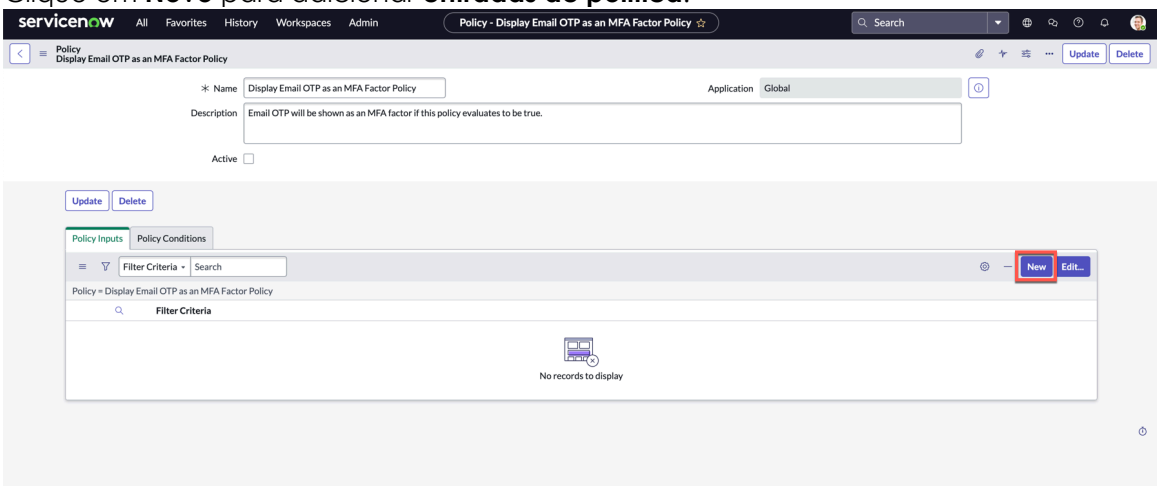
   Nota: O **E-MAIL** como **fator MFA com uma política** está disponível por padrão. É possível editar a política e especificar as entradas e condições.

3. Selecione **Exibir OTP do e-mail como uma política de fator de MFA**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Clique em **Novo** para adicionar **entradas de política**.

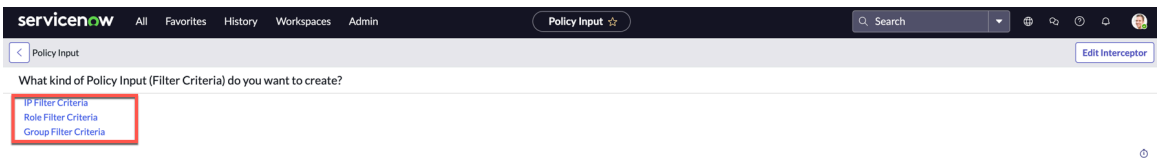


5. Selecione os critérios de filtro que deseja criar.

Estes são os tipos de critérios de filtro:

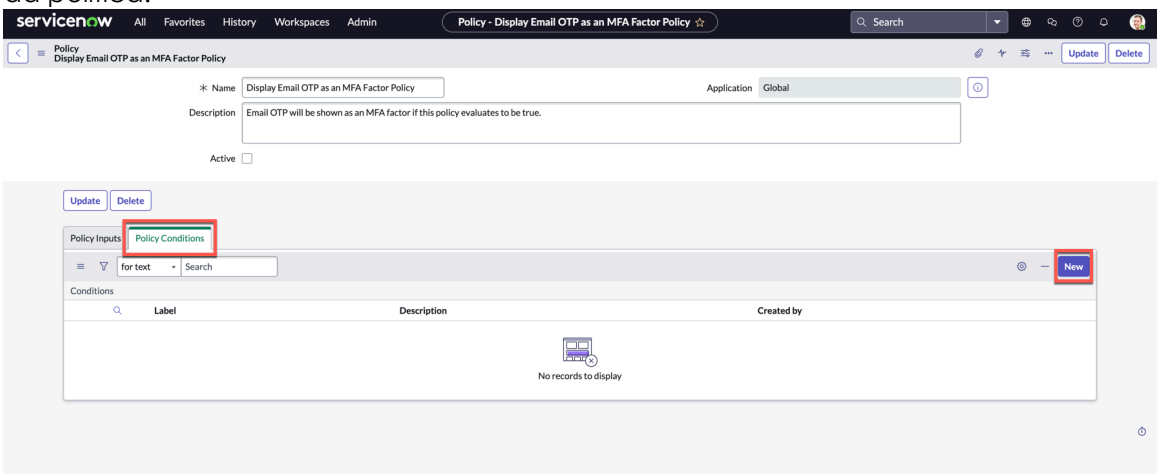
- Critérios de filtro por IP
- Critérios de filtro por função
- Critérios de filtro por grupo

Por exemplo, Critérios de filtro por função.



© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

6. Clique em **Critérios de filtro por função**, preencha os campos dos critérios de filtro por função e envie o registro. A nova política é criada. Para obter mais informações, consulte Critérios de filtro por função.
7. Na página Política — Exibir OTP de e-mail como um fator de MFA, clique em Condições da política.



8. Clique em **Novo** para adicionar **Condições da política**.
9. No formulário, preencha os campos:

Formulário de condições

Campo	Descrição
Rótulo	Nome para identificar a condição.
Descrição	Descrição da condição.
Condição	Combinação lógica de várias entradas de política (critérios de filtro) para avaliar solicitações de autenticação. Selecione a política de critérios de filtro baseada em função que foi criada para a condição.

10. Clique em **Enviar**.
11. Opcional: Repita a etapa 8 para criar condições de política adicionais.

> **Nota:** Se várias condições de política forem criadas, a saída final da política de acesso dependerá da lógica OU da saída de todas as condições de política. Isso significa que a política será avaliada como verdadeira se qualquer uma das condições de política for atendida.

Com base na política de filtro de função (usuários) e nas condições especificadas para a função, o fator de e-mail como MFA é mostrado como uma opção de autenticação para os usuários.

Redefinir a autenticação multifator (MFA) para usuários

Os administradores podem redefinir a MFA para usuários que excluíram o aplicativo, perderam o acesso ao dispositivo ou não têm nenhuma MFA alternativa associada ao dispositivo.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: admin

O procedimento a seguir descreve como um administrador da ServiceNow® pode redefinir a validação MFA para desbloquear usuários e permitir que eles registrem novamente a MFA.

Procedimento
1. Navegue até **Todos** > **Autenticação multifator** > **Configuração multifator do usuário**.
2. Na tabela de usuários, pesquise aquele que você deseja desbloquear.
3. Defina Validar como **falso**.
4. Navegue até **Todos** > **Autenticação multifator** > **Fatores recentes do usuário**.
5. Pesquise o mesmo usuário.
6. Defina "É fator recente" como **falso** para o tipo de MFA que você deseja redefinir para o usuário.
   Alterar o valor para **falso** desbloqueia o usuário e permite que ele registre novamente a MFA.
   Quando o usuário desbloqueado insere as credenciais e faz login, a página **Habilitar autenticação multifator (MFA)** é exibida. O usuário pode seguir as etapas na página para registrar novamente a MFA.

Tópico de referência: autenticação multifator

Tópico de referência relacionado à configuração da autenticação multifator.

Autenticações multifatores do usuário

Para acessar os detalhes sobre a autenticação multifator do usuário, navegue até **Todos** > **Autenticação multifator** > **Configuração multifator do usuário**.

Autenticações multifator do usuário

Campo	Descrição
Usuário	O nome de usuário
Desvio restante	O número total de desvios restantes para o usuário.
Segredo multifator	Os detalhes do segredo multifator.
Validado	Está validado com a autenticação multifator. Alterar o valor para **falso** invalida a configuração do app autenticador existente.

Nota: Os fatores de MFA usados recentemente pelos usuários estão disponíveis no módulo Fatores usados recentemente pelo usuário. Navegue até **Todos** > **Autenticação multifator** > **Fatores recentes do usuário**. Para obter mais informações, consulte Fatores usados recentemente pelo usuário.

Impressões digitais multifatores do navegador

Para acessar os detalhes sobre as impressões digitais do navegador do usuário, navegue até **Todos** > **Autenticação multifator** > **Impressões digitais multifatores do navegador**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Impressões digitais multifatores do navegador

Campo	Descrição
Usuário	O nome de usuário
Navegador	O navegador que o usuário utilizou.
Impressão Digital do Navegador	Os detalhes da impressão digital do navegador.
Cookie de Impressão Digital do Navegador	Os detalhes de cookies da impressão digital do navegador.
Validade do Cookie de Impressão Digital do Navegador	Os detalhes de validade dos cookies de impressão digital do navegador.

Fatores usados recentemente pelo usuário

Para acessar os detalhes sobre os fatores que o usuário utilizou recentemente, navegue até **Todos** > **Autenticação multifator** > **Fatores recentes do usuário**.

Usar Configurações Multifatores do Usuário

Campo	Descrição
Usuário	O nome de usuário
Tipo de Multifator	O tipo de multifator que o usuário utilizou para fazer login.
É Fator Recente	Os detalhes dos multifatores recentes do usuário.

Usar autenticação multifator (MFA)

Aprenda a usar ferramentas de autenticação multifator para acessar sua instância com segurança.

Login com MFA

ServiceNow requer aplicações autenticadoras que ofereçam suporte a senhas de uso único baseadas em tempo (TOTP). ServiceNow testa a MFA com os seguintes autenticadores:

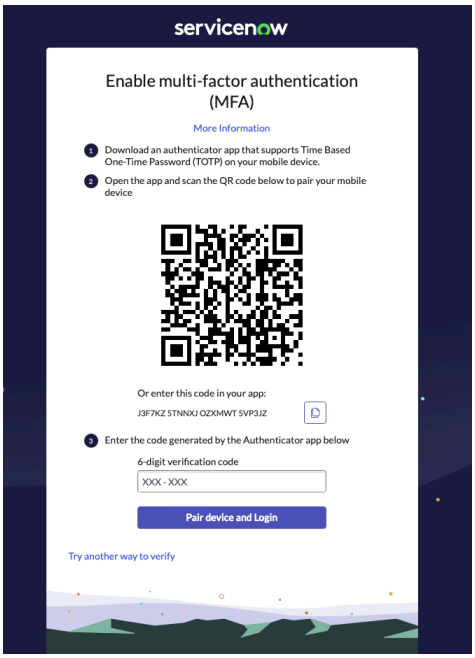
- Google Autenticador
- Microsoft Autenticador
- Autenticador LastPass
- Authy
- FreeOTP
- Duo
- Verificar Okta

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

- Outros autenticadores não listados também podem ser compatíveis, mas não foram testados pelo ServiceNow.
- Para informações relacionadas à mudança de comportamento específica do navegador, consulte este artigo da base de conhecimento.

Validação com aplicativo autenticador



Insira o código exibido no aplicativo autenticador para fazer login.

Se o administrador tiver habilitado a autenticação multifator (MFA) em sua instância, será solicitada uma segunda autenticação além do seu nome de usuário e senha. Para obter detalhes sobre o processo de login com MFA, consulte Login com autenticação multifator

Se você não tiver configurado uma segunda forma de autenticação, verá uma página de configuração após o login com orientações durante o processo de configuração de um aplicativo de autenticação. Para obter detalhes sobre esta configuração, consulte Como configurar a autenticação multifator pela primeira vez.

Registro de um dispositivo de autenticação

Depois de configurar um aplicativo de autenticação, é possível registrar outros métodos de autenticação.

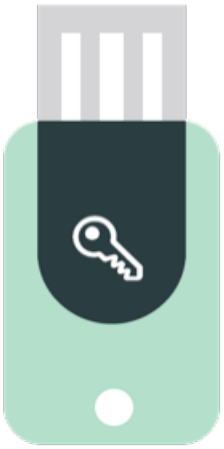
Autenticadores biométricos

É possível usar autenticadores biométricos, como impressão digital ou reconhecimento facial, como sua segunda autenticação de MFA. Se o seu administrador permitir esta opção, será possível configurar autenticadores biométricos usando as etapas em Registro de um autenticador biométrico.

Autenticadores de chave de hardware

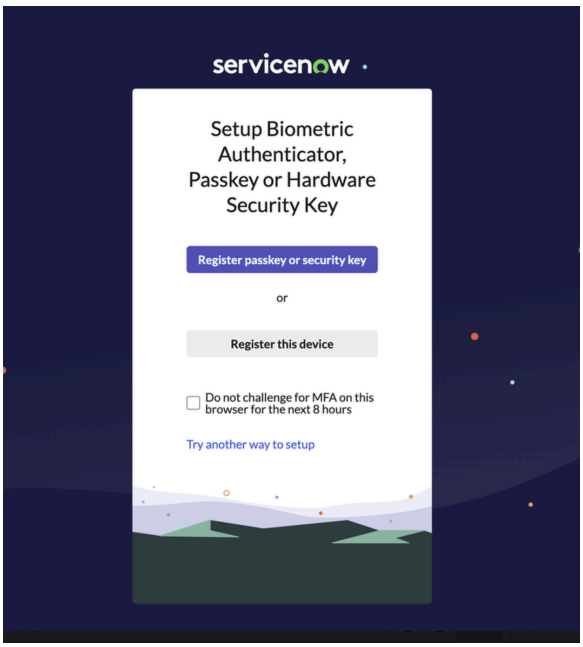
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

As chaves de hardware são dispositivos de segurança físicos que podem ser usados para autenticação. É possível registrar um dispositivo de hardware para uso com sua instância usando as etapas em Registro da chave de segurança de hardware.



Validação com chave biométrica ou de hardware

Use a chave biométrica ou de segurança para fazer login.

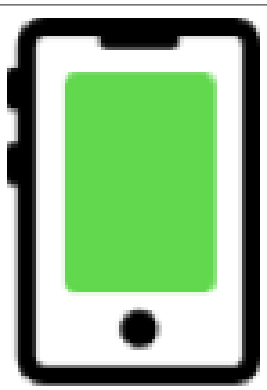


Registro de um número de telefone para OTP

SMS

O administrador configura a instância ServiceNow para exigir que os usuários tentem o login na instância usando OTP baseada em SMS.

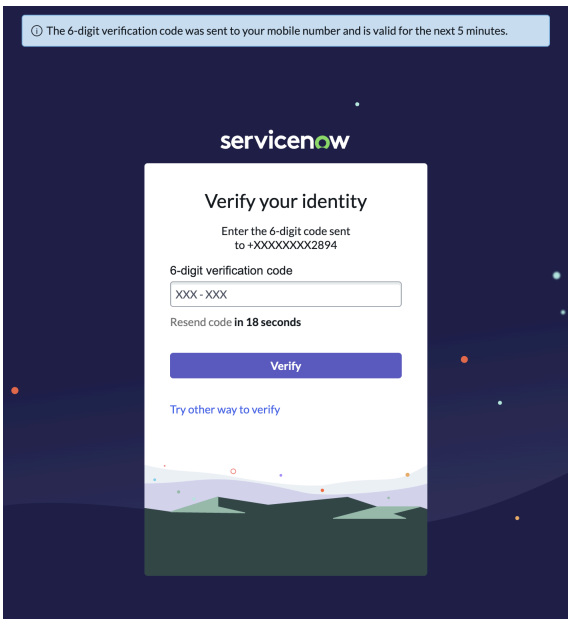
Quando os usuários tentam fazer login em ServiceNow, a OTP do SMS é enviada para o número do celular associado ao registro sys_user. Os usuários podem inserir o código de verificação de



© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

seis dígitos enviado para o dispositivo móvel para verificar sua identidade.

Validação com SMS



Insira o código de seis dígitos enviado para o seu número do celular para fazer login. O código enviado é válido pelos próximos 5 minutos. Use a opção "Reenviar código" para enviar o código novamente.

Registro de um endereço de e-mail para OTP

Endereço de e-mail

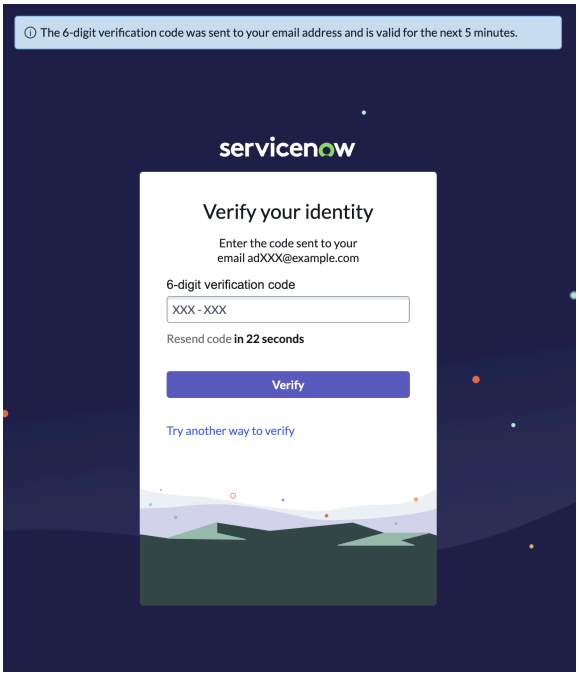
O administrador configura a instância ServiceNow para exigir que os usuários tentem o login na instância usando OTP baseada em e-mail.

Quando os usuários tentam fazer login em ServiceNow, a OTP do e-mail é enviada para o endereço de e-mail associado ao usuário. Os usuários podem inserir o código de verificação de seis dígitos enviado para o dispositivo móvel para verificar sua identidade.

Validação com e-mail

Insira o código de seis dígitos enviado para o seu endereço de e-mail para fazer login. O código enviado é válido pelos próximos 5 minutos. Use a opção "Reenviar código" para enviar o código novamente.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Como configurar a autenticação multifator pela primeira vez

Se o administrador tiver habilitado a autenticação multifator no seu perfil, mas você ainda não tiver feito a configuração da aplicação, será possível configurá-la após o login.

Antes de Iniciar

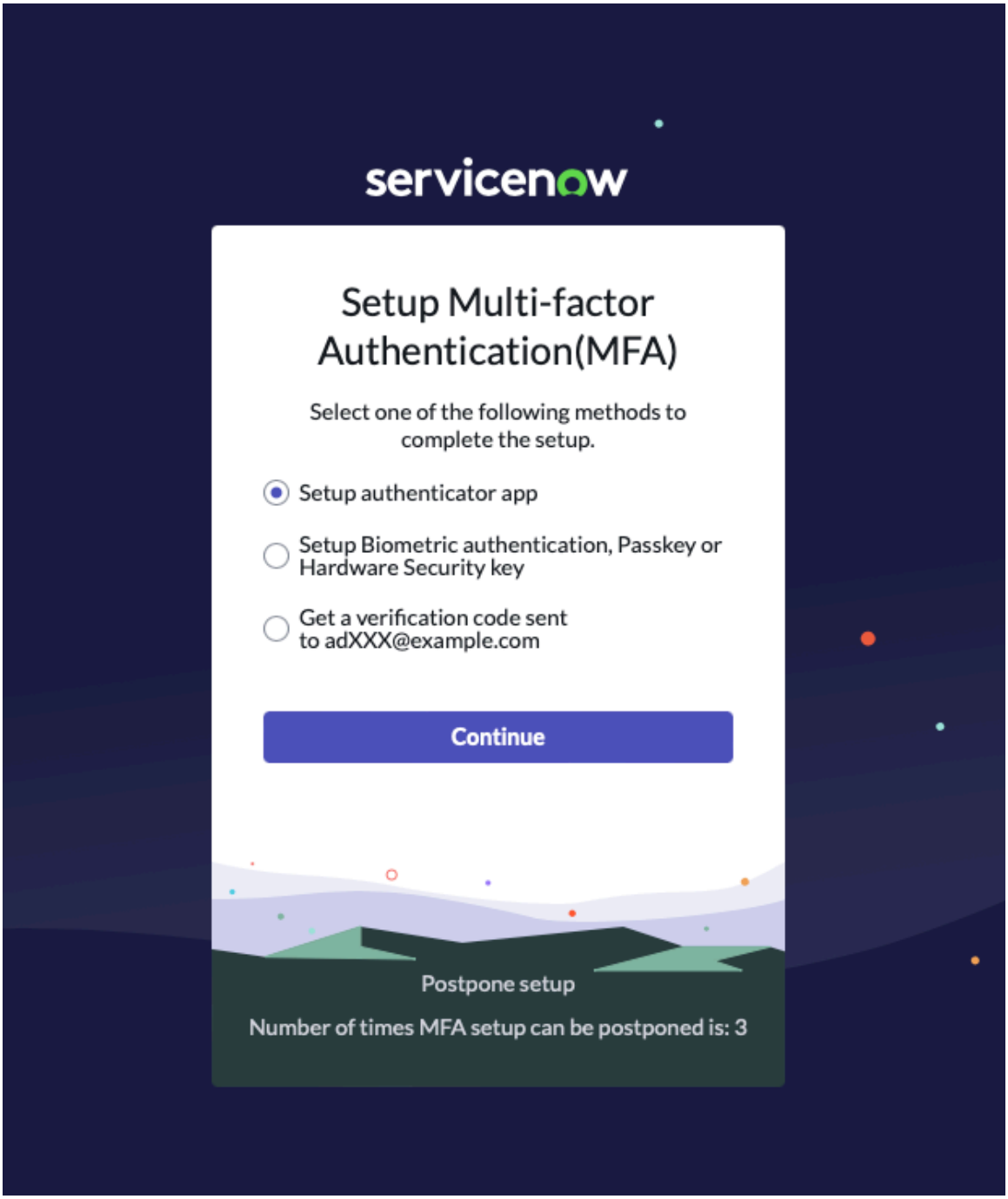
Função necessária: nenhuma

Procedimento

1. Faça login em sua instância usando seu nome de usuário e senha.

   A tela de configuração da autenticação multifator intercepta seu login.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



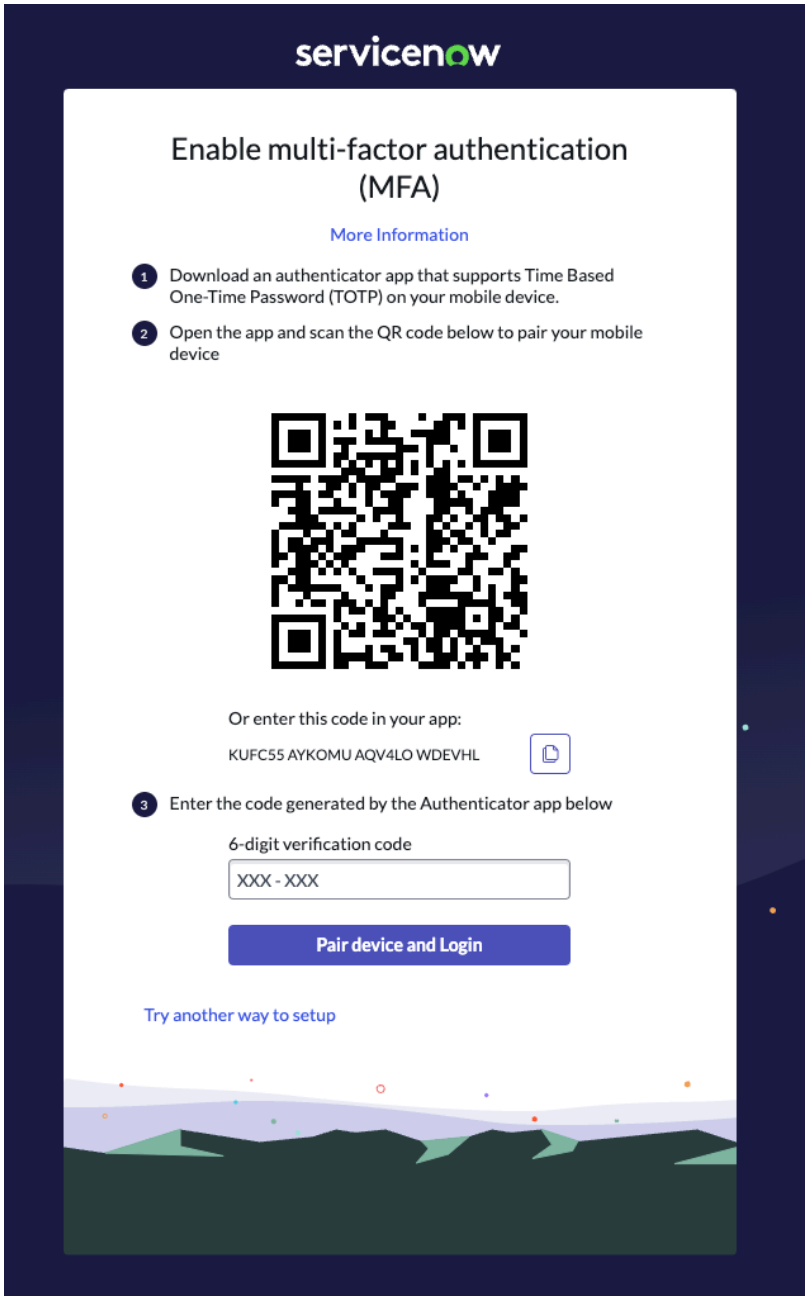
Nota: Se quiser ignorar a configuração da autenticação agora, clique em **Ignorar configuração**. É possível ignorar a autenticação multifator por um número limitado de vezes permitidas pelo administrador. Por fim, você deverá configurar a autenticação multifator.

2. Selecione um dos seguintes métodos para concluir a configuração da MFA.

a. Configurar app autenticador

Siga as instruções na tela para emparelhar o dispositivo e fazer login.

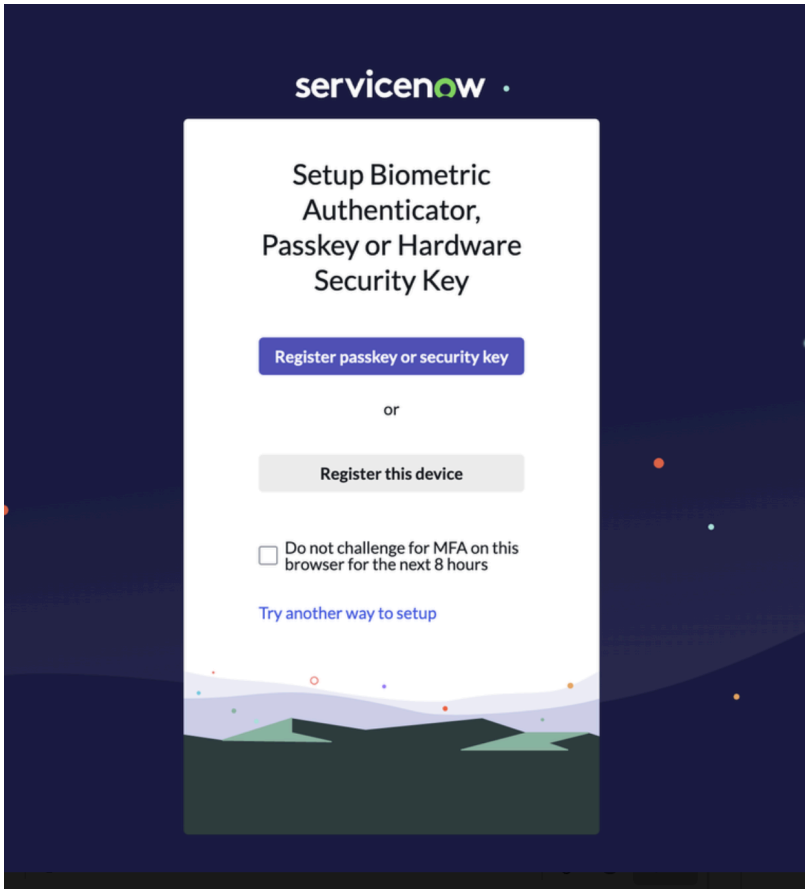
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



b. Configurar autenticação biométrica, senha ou chave de segurança de hardware

Selecione uma das opções para concluir a configuração.

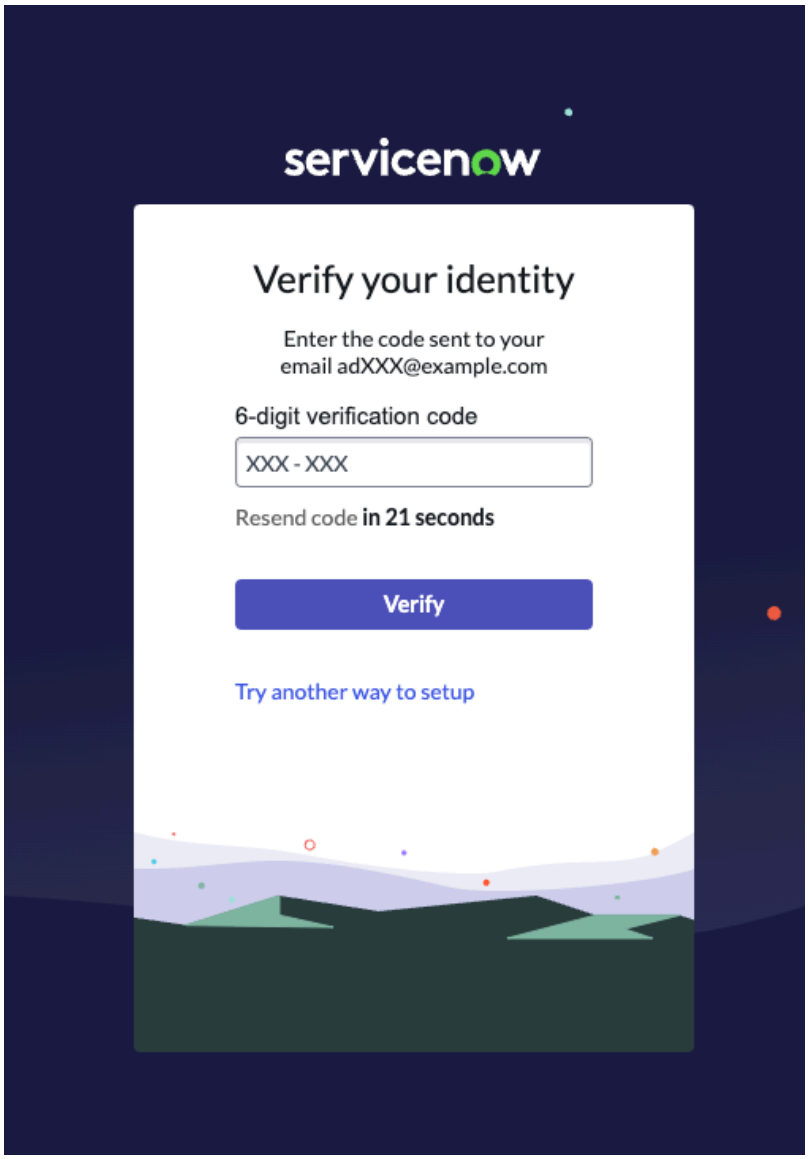
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



c. Receba um código de verificação em seu e-mail

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Digite o código de verificação enviado ao seu e-mail.



Após a conclusão com sucesso de qualquer uma das configurações, você será conectado à instância.

Configuração da autenticação multifator no seu perfil de usuário

Habilite a autenticação multifator para a sua conta nas configurações de perfil de usuário.

Antes de Iniciar
Função necessária: nenhuma

A autenticação multifator deve estar habilitada em sua instância.

Nota: Seu administrador pode exigir que você use a autenticação multifator. Nesse caso, você será avisado automaticamente ao fazer login. Consulte Como configurar a autenticação multifator pela primeira vez. Use o processo abaixo se o administrador permitir que você opte pela autenticação multifator.

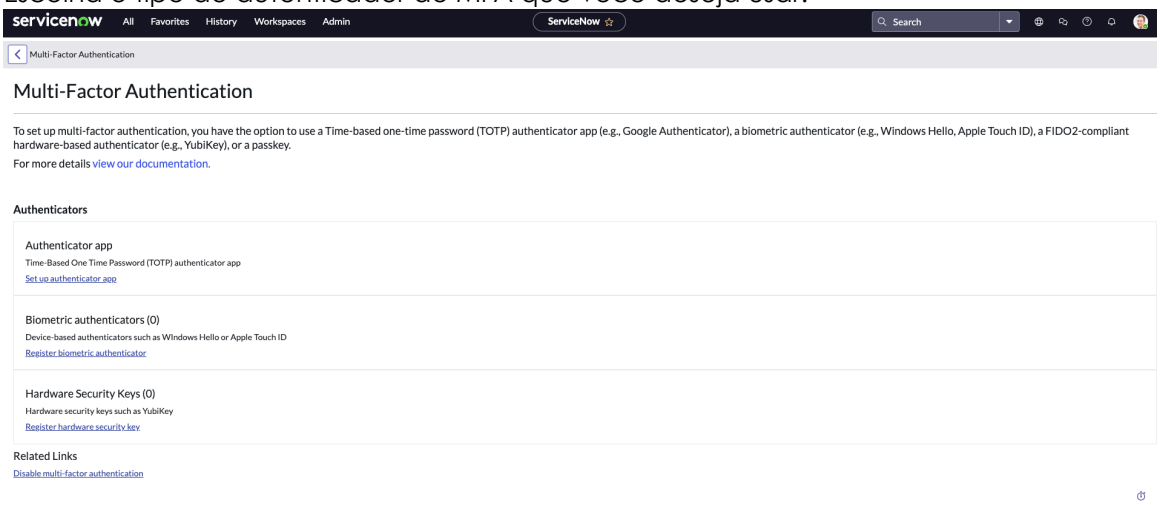
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

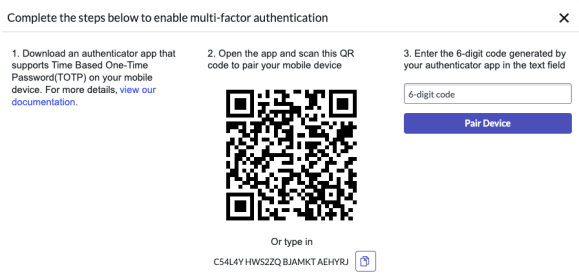
1. Navegue até **Todos** > **Autoatendimento** > **Meu perfil**.

   Nota: Você também pode acessar seu perfil clicando no seu nome de usuário no cabeçalho da instância.

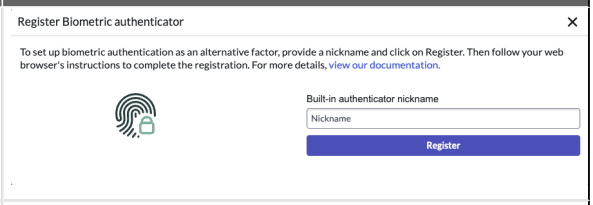
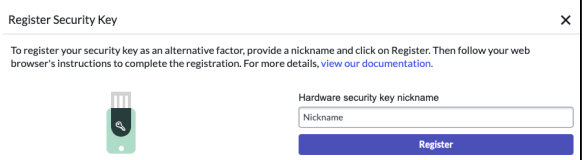
2. No seu perfil de usuário, clique em **Autenticação multifator** na seção **Links relacionados**.
3. Escolha o tipo de autenticador de MFA que você deseja usar.



Autenticadores de MFA

Autenticadores de MFA	Descrição
App autenticador	App autenticador baseado em TOTP (Time-Based One-Time Password, senha única baseada em tempo) Selecione **Configurar app autenticador** e siga as instruções na tela para registrar um app autenticador como o segundo fator de autenticação. 
Autenticadores biométricos	Autenticadores baseados em dispositivo, como Windows Hello ou Apple Touch ID Selecione **Registrar autenticação biométrica** e siga as instruções na tela para registrar um app autenticador como o segundo fator de autenticação.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Autenticadores de MFA	Descrição
	
Chaves de segurança de hardware	Chaves de segurança de hardware, como YubiKey Selecione **Registrar chaves de segurança de hardware** e siga as instruções na tela para registrar um app autenticador como o segundo fator de autenticação. 

Resultados

A autenticação multifator está habilitada para a sua conta de usuário. Você deverá usar a autenticação multifator na próxima vez que fizer login.

Nota: Você não poderá desabilitar a autenticação multifator na sua conta depois de habilitá-la. Se precisar desabilitar a autenticação multifator, entre em contato com o administrador.

Login com autenticação multifator

Faça login com a autenticação multifator quando ela for habilitada pelo administrador na sua instância.

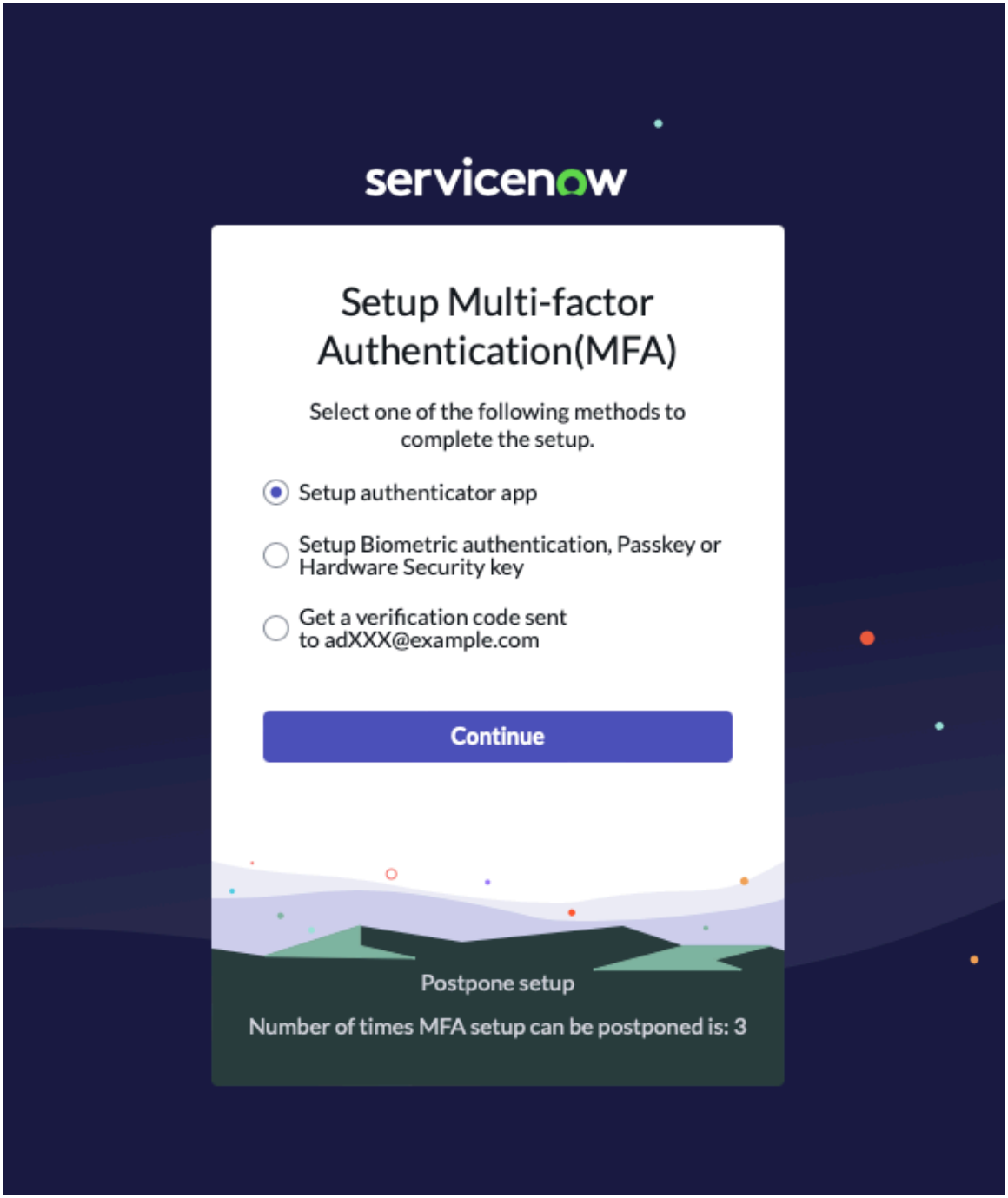
Antes de Iniciar

A autenticação multifator deve estar habilitada para o seu perfil. Você pode habilitá-la no seu perfil do usuário ou o administrador pode fazer isso para você.
Função necessária: none

Procedimento

1. Vá para o URL da sua instância para abrir a tela de login.
2. Insira seu nome de usuário e senha.
3. Clique em **Fazer login**.
   A tela de autenticação multifator é exibida.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Selecione um dos métodos para concluir a configuração da MFA.
   Para mais informações sobre cada configuração, consulte Como configurar a autenticação multifator pela primeira vez.

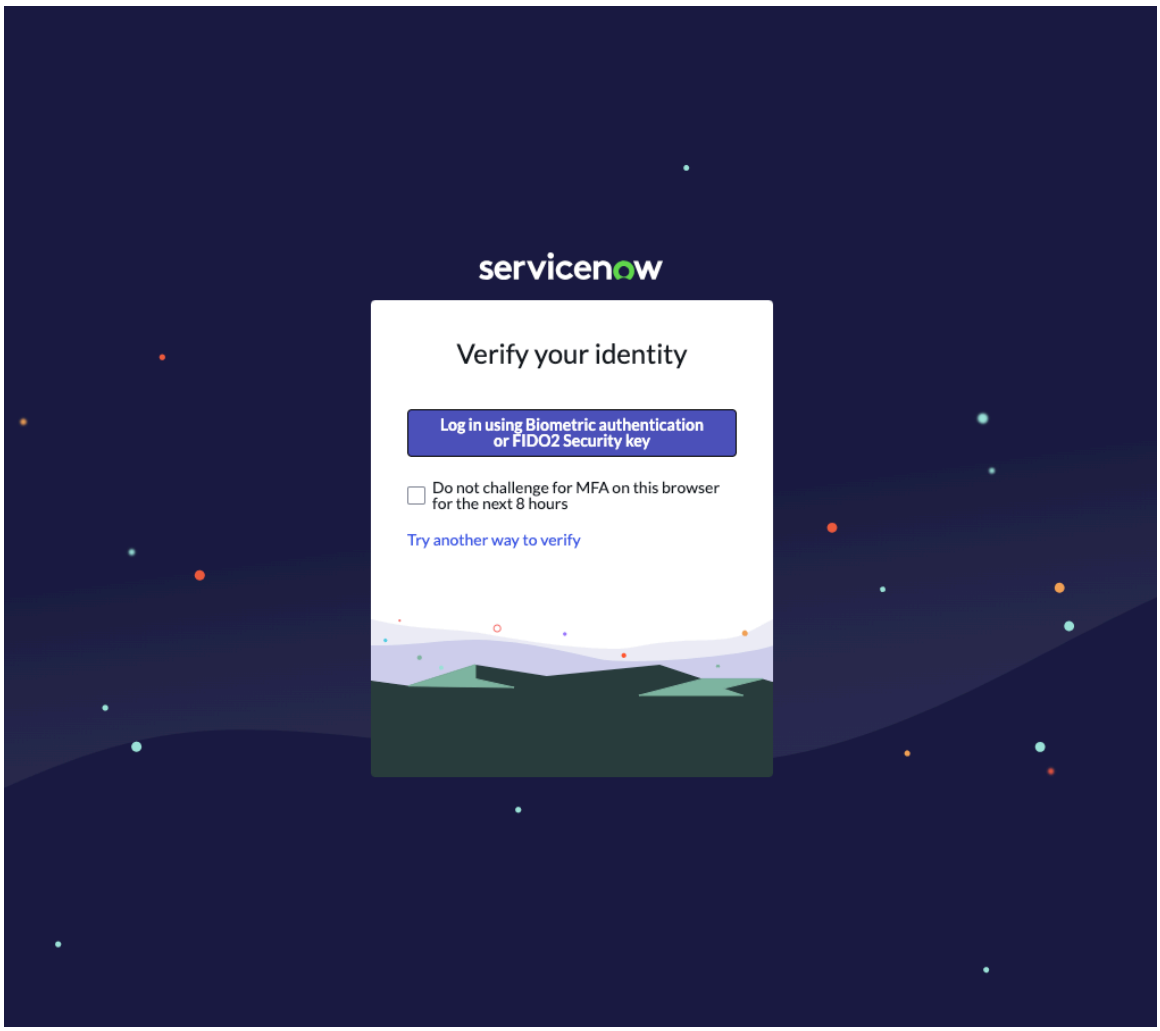
   Se você quiser adiar a configuração, selecione **Adiar configuração**. O número máximo de vezes que você pode adiar a configuração aparece na tela e este valor é configurado pelo administrador.

Resultados
Se você já configurou a MFA, o fator usado recentemente será exibido quando você fizer login na instância após inserir seu nome de usuário e senha.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Example: Fator de MFA usado recentemente

Se o fator usado recentemente tiver sido o login biométrico, ao fazer login usando seu nome de usuário e senha, ele será exibido diretamente com a tela de configuração da MFA biométrica.



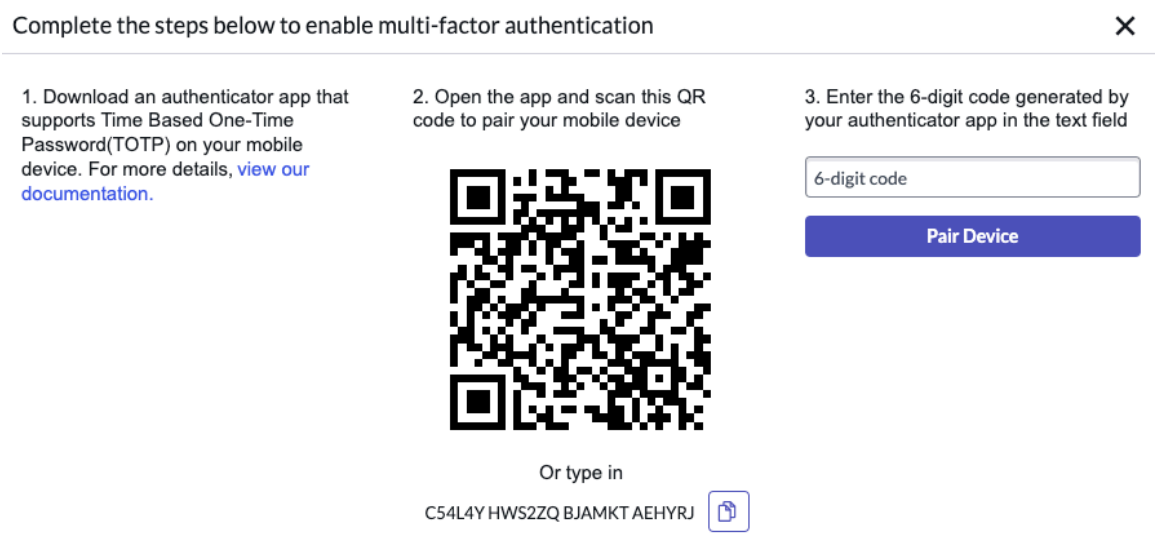
Aplicações autenticadoras

Use aplicações autenticadoras de terceiros para gerar senhas de MFA temporárias.

Uma aplicação autenticadora é um software de terceiros que gera senhas temporárias. Você pode usar essas senhas com a sua para fazer login em uma instância que requer autenticação multifator (MFA).

Se o administrador tiver habilitado a MFA em sua instância, você verá uma solicitação de senha após inserir seu usuário e senha durante o login.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



A ServiceNow requer aplicações autenticadoras que ofereçam suporte a TOTP (Time-based One-time Passwords, senhas de uso único baseadas em tempo).

A ServiceNow testa a MFA com os seguintes autenticadores:

- Google Authenticator
- Microsoft Autenticador
- Autenticador LastPass
- Authy
- FreeOTP
- Duo
- Verificar Okta

Nota: Outros autenticadores não listados também podem ser compatíveis, mas não foram testados pelo ServiceNow.

Mudança de Aplicativo autenticador

Gere um novo código para mudar o aplicativo autenticador no seu dispositivo.

Antes de Iniciar

A autenticação multifator deve estar habilitada para o seu perfil. Você pode habilitá-la no seu perfil do usuário ou o administrador pode fazer isso para você.
Função necessária: nenhuma

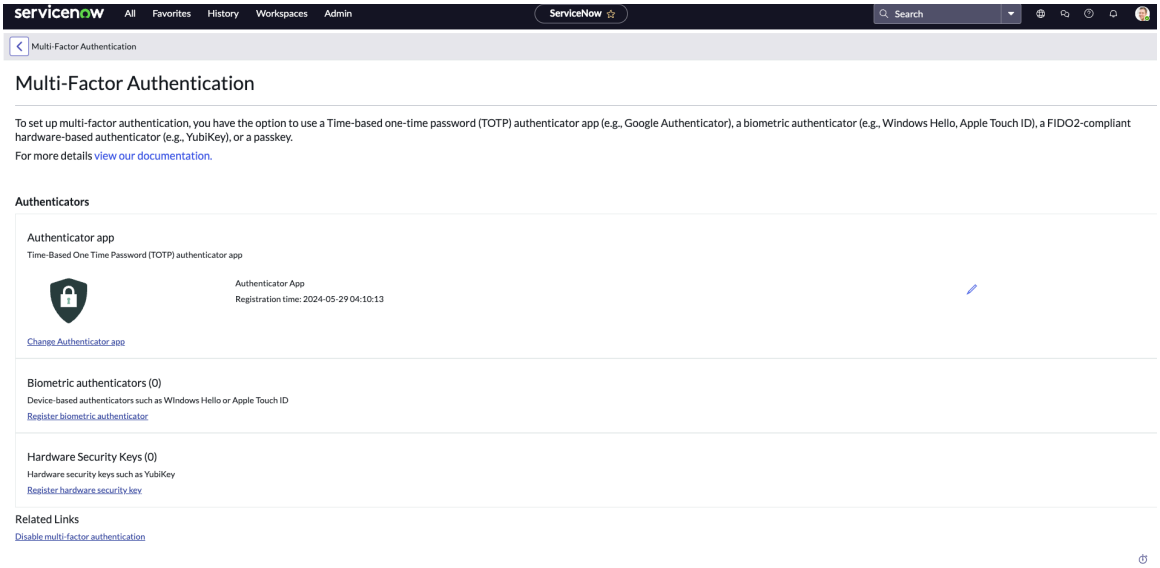
Procedimento

1. Navegue até **Todos** > **Autoatendimento** > **Meu perfil**.

   Nota: Você também pode acessar seu perfil clicando no seu nome de usuário no cabeçalho da instância.

2. No seu perfil de usuário, clique em **Autenticação multifator** na seção **Links relacionados**.
3. Em **App autenticador**, selecione o ícone de edição.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

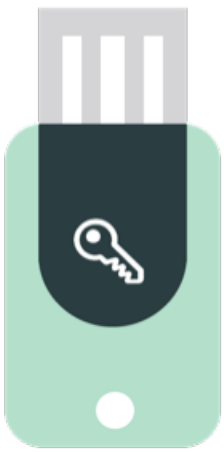


4. Na janela "Mudar código autenticador", clique em **Mudar**.
5. Siga as instruções na tela para registrar o app autenticador no dispositivo.

Autenticação da Web

Seus usuários podem usar chaves de hardware ou leitores biométricos do dispositivo (FIDO2) para a autenticação em uma instância.

Chaves de hardware



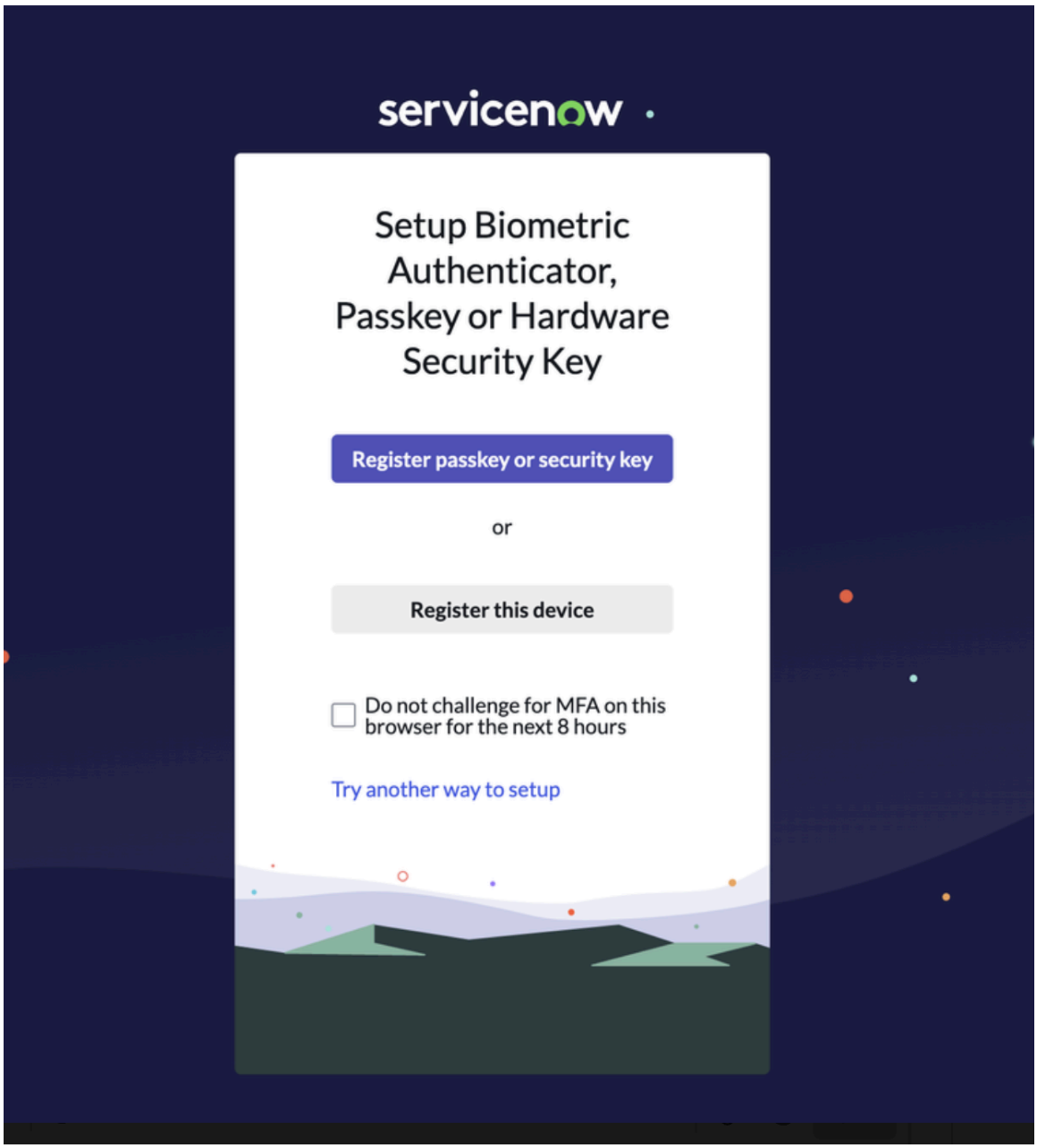
As chaves de hardware são hardware físico que pode ser usado para a autenticação. As chaves de hardware são inseridas em uma porta no seu dispositivo para fornecer autenticação. Para obter detalhes sobre como registrar chaves de hardware, consulte Registro da chave de segurança de hardware.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Biometria

Autenticadores biométricos usam impressão digital ou reconhecimento facial para identificar usuários. Seus usuários podem usar esses autenticadores em seus dispositivos como parte do processo de login multifator. Para obter detalhes sobre como registrar autenticadores biométricos, consulte Registro de um autenticador biométrico.

Escolha o segundo fator que deseja autenticar e faça a autenticação em sua instância.



© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para configurar o plug-in de autenticação da Web, consulte .

Registro de um autenticador biométrico

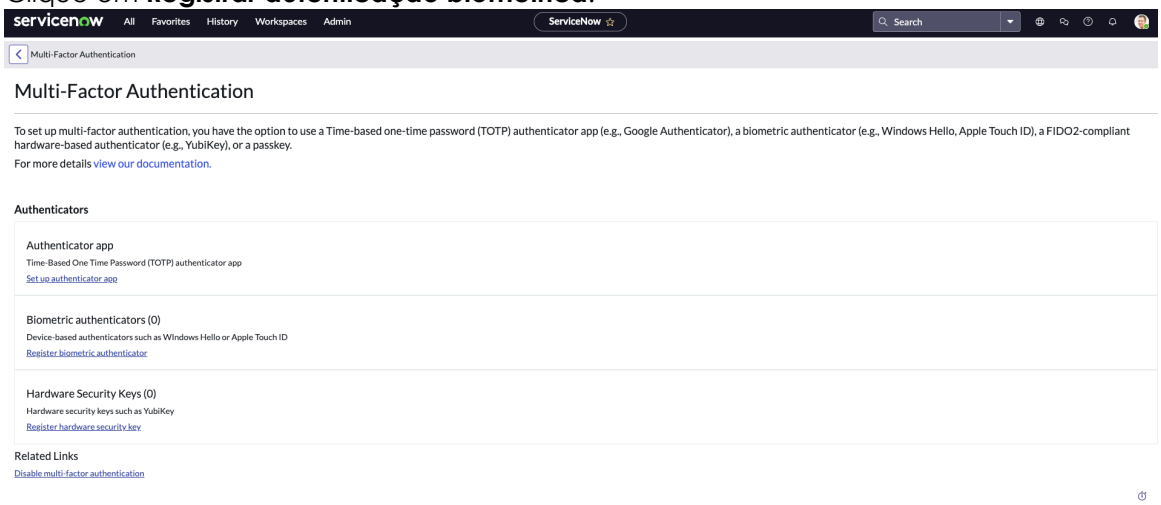
Registre um autenticador biométrico para usar como parte do login de autenticação multifator.

Antes de Iniciar

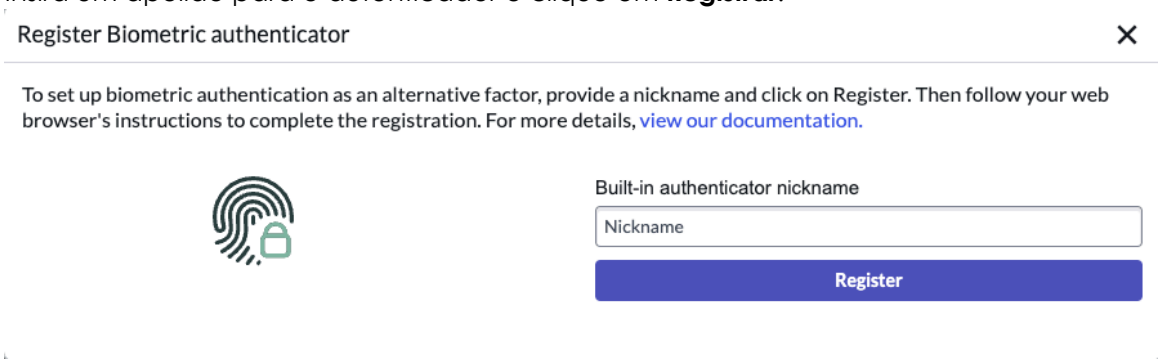
Função necessária: nenhuma

Procedimento

1. Navegue até **Todos** > **Autoatendimento** > **Meu perfil**.
2. Em **Links relacionados**, clique em **Autenticação multifator**.
   A página de autenticação multifator é aberta.
3. Clique em **Registrar autenticação biométrica**.



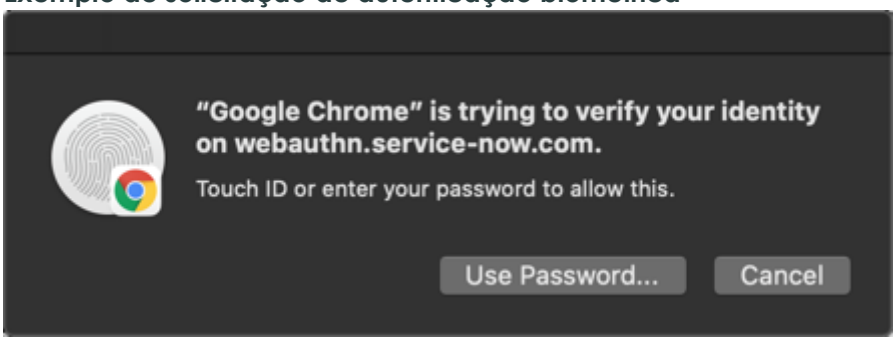
4. Insira um apelido para o autenticador e clique em **Registrar**.



5. Quando solicitado, siga as instruções na tela para autenticar com o autenticador biométrico.
   A mensagem varia de acordo com seu autenticador específico.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exemplo de solicitação de autenticação biométrica



Depois de fazer a autenticação com sucesso, uma janela de confirmação será exibida. Clique no X para fechar a confirmação.

Resultados

Seu autenticador biométrico foi registrado. É possível ver o autenticador biométrico listado na página "Autenticação multifator".

Registro da chave de segurança de hardware

Registre uma chave de hardware para usar como parte do login de autenticação multifator.

Antes de Iniciar

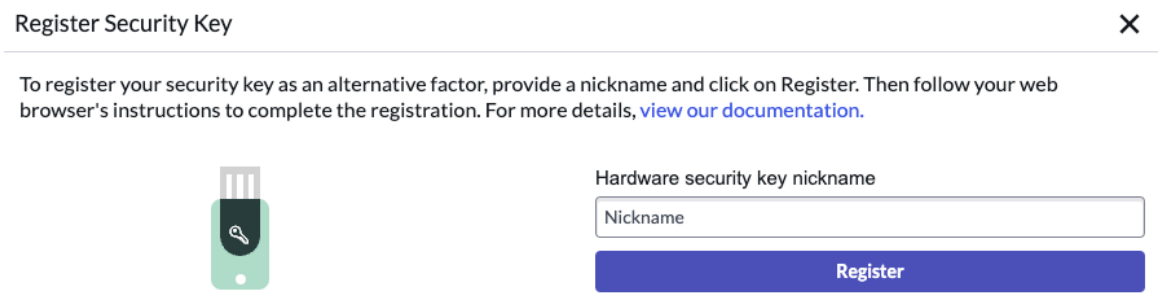
Função necessária: nenhuma

Procedimento

1. Navegue até **Todos** > **Autoatendimento** > **Meu perfil**.
2. Em **Links relacionados**, clique em **Autenticação multifator**.
   A página de autenticação multifator é aberta.
3. Clique em **Registrar chave de segurança de hardware**.

4. Insira um apelido para a chave de hardware e clique em **Registrar**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Quando solicitado, insira sua chave de segurança de hardware e ative-a.
   Depois de fazer a autenticação com sucesso, uma janela de confirmação será exibida. Clique no X para fechar a confirmação.

Resultados
Sua chave de hardware está registrada. É possível ver a chave de hardware listada na página "Autenticação multifator".

Autenticação multifator com Single Sign-On

Configure a autenticação multifator (MFA) com um provedor de Single Sign-On (SSO) para a sua instância ServiceNow.

Como muitos usuários em sua organização estão fazendo login em sua rede corporativa e acessando sua instânciaServiceNow, há uma necessidade maior de uma autenticação segura.

A MFA combinada com SSO fornece segurança aprimorada para a sua instância. Este recurso fornece flexibilidade para habilitar a MFA condicionalmente para os usuários.

Nota:

- ServiceNow A MFA é aplicada depois que o usuário é redirecionado após a autenticação bem-sucedida no provedor de identidade.
- A MFA não era aplicada com SSO antes da versão de San Diego.

Por exemplo, se quiser dar aos usuários externos um protocolo de segurança adicional, você poderá aplicar a MFA somente para esses usuários. Desta forma, é possível adicionar habilidades de autenticação adicionais e controlar o acesso dos usuários.

É possível impor a MFA para autenticação em logins baseados em SSO, como SAML, OpenID Connect e Digest.

A MFA com SSO pode ser configurada sob demanda, com base em seus requisitos. Com a ajuda de esquemas de autenticação e provedores de identidade, você pode impor a MFA a usuários específicos com um mecanismo de login específico.

É possível impor a MFA para as seguintes condições:

- Esquema de autenticação
- Provedor de identidade

A MFA com SSO é oferecida como parte do plug-in Adaptive Authentication (com.snc.adaptive_authentication) de autenticação adaptável. Para saber mais sobre como configurar a autenticação adaptável, consulte Autenticação adaptável.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configuração de MFA com SSO

Imponha MFA com SSO para usuários dentro ou fora da sua organização.

Antes de Iniciar

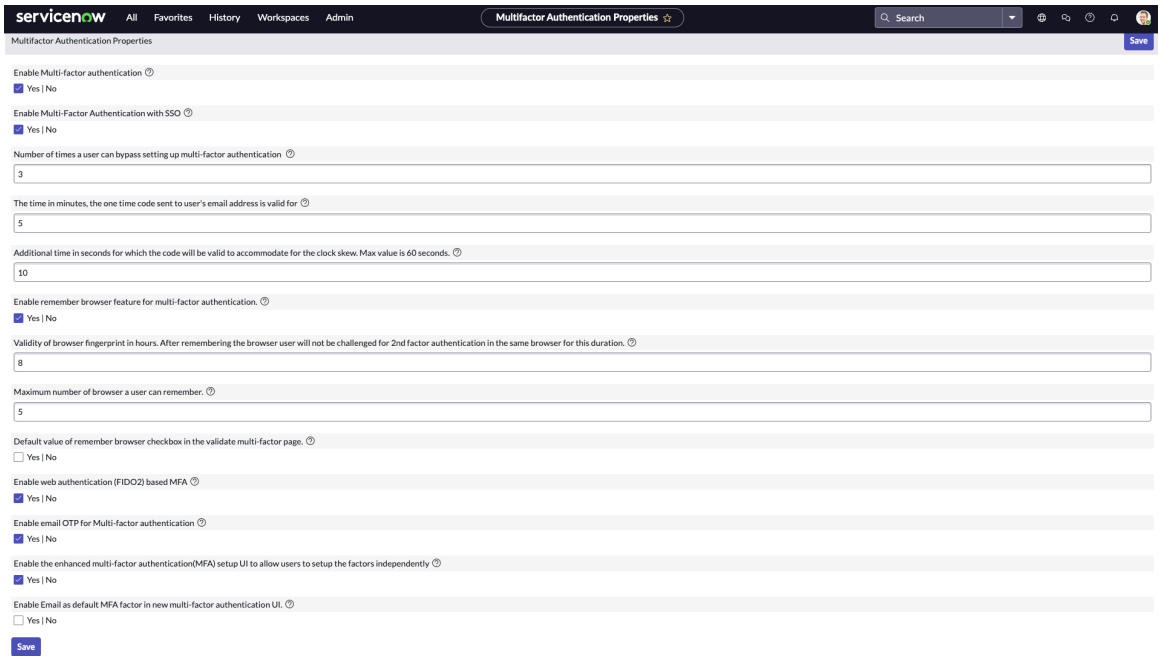
O recurso de MFA com SSO é oferecido como parte do plug-in Adaptive Authentication (com.snc.adaptive_authentication) de autenticação adaptável. Você deve habilitar a propriedade Autenticação adaptável para usar o recurso de MFA com SSO. Para saber mais sobre como configurar a Autenticação adaptável, consulte Autenticação adaptável.

Nota: O login por meio de MFA com SSO estará disponível se a propriedade *glide.authenticate.mfa.with.multisso.enabled* for definida como **verdadeira**.

Função necessária: administrador

Procedimento

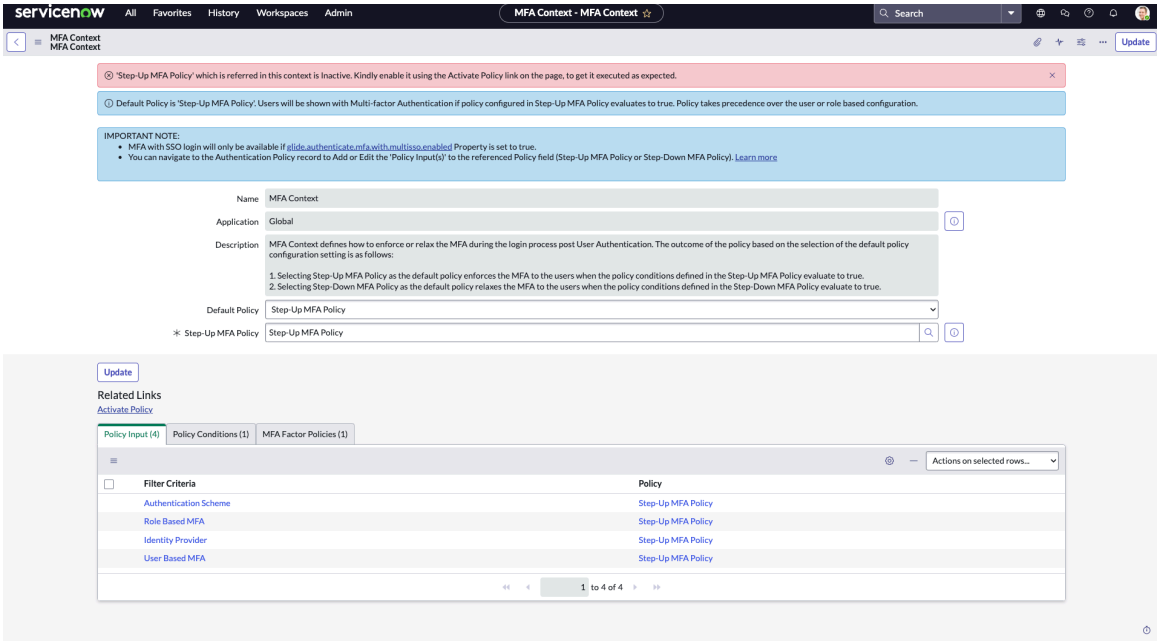
1. Navegue até **Todos** > **Autenticação multifator** > **Propriedades**.
2. Habilite as caixas de seleção **Habilitar autenticação multifator** e **Habilitar autenticação multifator com SSO**.



3. Clique em **Salvar**.
4. Navegue até **Autenticação multifator** > **Contexto de MFA**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O formulário Contexto de MFA é exibido.



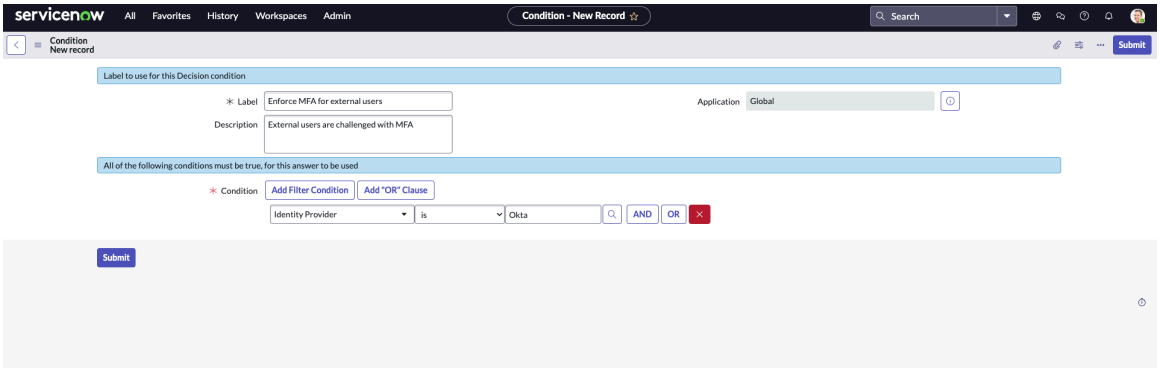
Nota: Por padrão, a política é a **Política de MFA em etapa crescente**. Os usuários serão exibidos com a autenticação multifator se uma condição configurada na **Política de MFA em etapa crescente** for avaliada como **verdadeira**. A política tem precedência sobre a configuração baseada em função ou usuário.

5. Opcional: Para editar uma política, volte para o registro da Política de autenticação, altere as condições e retorne até este ponto.
   Ao navegar até o registro da Política de autenticação, é possível adicionar ou editar as "Entradas de política" nos campos de política referenciados, **Política de MFA em etapa crescente** ou **Política de MFA em etapa decrescente**.
6. Para definir uma nova condição de política, clique em **Condições de política**.
7. Clique em **Nova**.
8. No formulário, preencha os campos.

Formulário Condições

Campos	Descrição
Rótulo	Nome exclusivo da condição que você deseja criar para o rótulo.
Descrição	A descrição da condição da política.
Condições	O tipo de condição que você deseja aplicar à política. Você pode adicionar condições do filtro e cláusulas "OU". **Nota:** Adicionar várias condições e cláusulas do filtro permite que você crie demandas de MFA para usuários específicos.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Example
Para configurar suas condições, considere o exemplo a seguir. Imagine que você deseja um esquema de autenticação com o provedor de identidade como sua condição para usuários externos. É possível definir as condições da seguinte forma:

a. Selecione **Esquema de autenticação** e defina os critérios como **Single Sign-On** ou **Nome de usuário e senha**.

Com base nesta seleção, o usuário recebe um login baseado em SSO ou um formulário de login para especificar o nome de usuário e a senha.

b. Selecione **Provedor de identidade** e especifique o provedor como o registro do IDP para o qual deseja habilitar a MFA. Por exemplo, **Okta**.

Com base nesta seleção, se o usuário fizer login com SSO, não será solicitado a usar a MFA. Por outro lado, se fizer login usando Okta, o usuário será solicitado a usar a MFA.

9. Clique em **Enviar**.

Informações relacionadas

Autenticação adaptável

Autenticação multifator com Single Sign-On

Single Sign-on (SSO) de vários provedores

O SSO externo permite que as organizações usem vários provedores de identidade (IdPs) de SSO para gerenciar a autenticação, bem como reter a autenticação do banco de dados local (básica).

A integração oferece suporte a qualquer combinação de métodos de autenticação local e externa em uma única instância:

- SAML 2.0
- Autenticação Digest
- OpenID Connect

Várias etapas são necessárias para o SSO de vários provedores, incluindo a configuração de propriedades, a criação de provedores de identidade (IdPs) e a configuração de usuários para usar o SSO.

Por exemplo, uma empresa com presença global pode exigir um provedor de SSO para seus funcionários, um diferente para seus fornecedores e autenticação de banco de dados

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

local para seus administradores. Como alternativa, uma empresa pode implementar SAML 2.0 e soluções de autenticação de token resumido na mesma instância.

Ativar plug-in Multi-Provider SSO

Esta integração requer o plug-in Integration - Multiple Provider Single Sign-On (com.snc.integration.sso.multi.installer).

Antes de Iniciar

Função necessária: administrador

O plug-in com.snc.integration.sso.multi.installer também pode ser usado para OIDC, SAML e Digest.

Função necessária: admin

Procedimento

1. Navegue até **Todos** > **Aplicações do sistema** > **Todas as aplicações disponíveis** > **Todas**.
2. Encontre o plug-in Integration - Multiple Provider Single Sign-On Installer (com.snc.integration.sso.multi.installer) usando os critérios de filtro e a barra de pesquisa.

   Pesquise o plug-in pelo nome ou ID. Se não conseguir encontrar um plug-in, talvez seja necessário solicitá-lo ao pessoal ServiceNow.
3. Selecione **Instalar** para iniciar o processo de instalação.

   Nota: Quando a separação de domínio e o administrador delegado estão habilitados em uma instância, o usuário administrativo deve estar no domínio **global**. Caso contrário, será exibido o seguinte erro: `A instalação da aplicação não está disponível porque há outra operação em execução: ativação de plug-in para <plugin name>.`

   Você verá uma mensagem após a conclusão da instalação.

Propriedades, tabelas e scripts de SSO de vários provedores

O plug-in Integration - Multiple Provider Single Sign-On inclui as seguintes propriedades do sistema, tabelas e scripts.

Propriedades

O SSO de vários provedores adiciona as seguintes propriedades do sistema.

Propriedades de SSO de vários provedores

Nome	Descrição
glide.authenticate.multisso.debug	Habilita (verdadeiro) ou desabilita (falso) o registro em log de depuração para a integração SSO de vários provedores. • Tipo: verdadeiro | falso • Valor padrão: falso

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Propriedades de SSO de vários provedores

Nome	Descrição
glide.authenticate.multisso.enabled	Habilita (verdadeiro) ou desabilita (falso) o SSO de vários provedores. • Tipo: verdadeiro | falso • Valor padrão: falso **Nota:** Definir esta propriedade como falsa não desabilitará o SSO de vários provedores se a recuperação de conta (ACR) também estiver habilitada na instância. Para fazer login com nome de usuário e senha, a ACR também deve ser desabilitada por meio da propriedade *glide.sso.acr.enabled*. Para obter detalhes sobre esta propriedade, consulte Propriedades de recuperação de conta.
glide.authenticate.multissov2_feature.enabled	Esta propriedade determina se a versão do MultiSSOv2 está habilitada na instância.

Tabelas

O SSO de vários provedores adiciona as seguintes tabelas.

Tabelas do SSO de vários provedores

Nome	Descrição
Propriedades do SSO `[sso_properties]`	Armazena dados para cada IdP, esquema, dados genéricos de SSO e assim por diante.
Propriedades da atualização 1 do SAML 2 `[saml2_update1_properties]`	Armazena dados para configurações da atualização 1 do SAML 2.0, como certificados SAML.
Propriedades `de resumo` `[digest_properties]`	Armazena dados para configurações de autenticação de token resumido.
Federação de SSO `[sso_federation]`	Armazena dados para cada federação de SSO.
Provedor de identidade OIDC `[oidc_identity_provider]`	Armazena dados para provedores de identidade baseados em Open ID Connect.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Scripts

O SSO de vários provedores adiciona os seguintes scripts.

Scripts do SSO de vários provedores

Nome	Descrição
MultiSSO	Permite que um cliente tenha um tipo de SSO definido por empresa.
MultiSSOLogin	Permite que cada domínio tenha seu próprio script de login.
MultiSSOLogout	Permite que cada domínio tenha seu próprio script de logout.
MultiSSO_OIDC_custom	Permite que um usuário defina um script de Single Sign-on personalizado para a conexão OIDC.
MultiSSO_OIDC_logout_custom	Permite que um usuário defina um script de logout personalizado para a conexão OIDC.
MultiSSO_Abstract_Core	Fornece uma classe base para todas as classes de SSO de vários provedores.
MultiSSO_ClientHelper	Fornece funções de utilitário de cliente chamável para SSO de vários provedores.
MultiSSO_DigestedToken	Fornece uma lógica de sistema base para autenticação de token resumido.
MultiSSO_SAML2_Update1	Fornece lógica para o processamento da atualização 1 do SAML 2.0 para um Single Sign-on de vários locatários.

Configurações de SSO de vários provedores

Várias etapas são necessárias para o SSO de vários provedores, incluindo a configuração de propriedades, a criação de provedores de identidade (IdPs) e a configuração de usuários para usar o SSO.

Consulte os tópicos a seguir para saber mais sobre cada uma das configurações.

- Fluxo de autenticação de IdP SSO (SAML) de vários provedores
- Configure as propriedades de SSO de vários provedores
- Criação de um provedor de identidade externo
- Configuração de usuários para SSO de vários provedores

Configure as propriedades de SSO de vários provedores

Configure as propriedades de SSO e também adicione uma propriedade à tabela Propriedades do sistema para configurar uma lista de inclusão de IdP.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Navegue até **Todos** > **SSO de vários provedores** > **Administração** > **Propriedades**.
2. Marque a caixa de seleção **Habilitar SSO de vários provedores**.

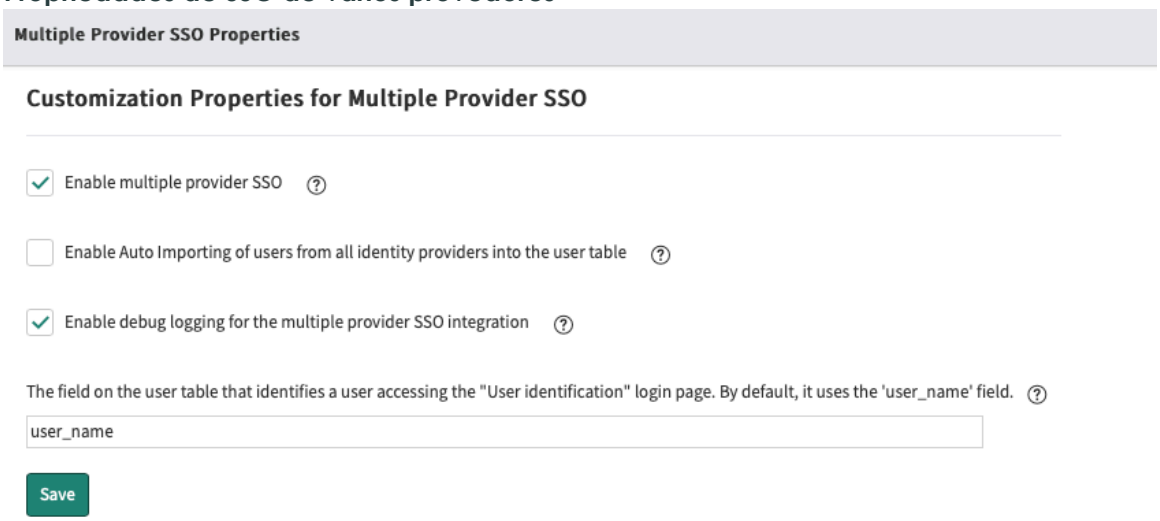
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Esta seleção adiciona o link Usar login externo à página de login.

3. Para atualizar a tabela Usuário com os usuários no IdP, selecione a opção **Habilitar importação automática**.
4. Para habilitar as mensagens de depuração para serem exibidas na parte inferior do quadro de conteúdo, marque a caixa de seleção **Habilitar log de depuração para a integração SSO de vários provedores**.
   Se habilitado, o recurso de registro em log de depuração tornará o desempenho mais lento e usará espaço em disco para gerar registros em log.
5. Na propriedade **O campo na tabela do usuário que identifica um usuário que acessa a página de login de identificação do usuário**, insira o campo na tabela Usuário que contém o valor usado pelo IdP para identificar o usuário. O valor padrão é **user_name**.

   O valor padrão é **user_name**.

Propriedades de SSO de vários provedores



6. Clique em **Salvar**.
7. Instrua os usuários a clicarem no link **Usar login externo** ao fazer login na instância.

Informações relacionadas

Provisionamento de usuário do SAML

Criação de um provedor de identidade externo

Depois de configurar as propriedades de SSO de vários provedores, você poderá atualizar ou criar um novo provedor de identidade de token resumido de SAML 2.0.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Navegue até **Todos** > **SSO de vários provedores** > **Provedores de identidade**.
2. Para editar um registro de provedor de identidade, clique no registro.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Para configurações de token resumido, atualize manualmente as propriedades.
- Para configurações da atualização 1 do SAML2, atualize automaticamente os metadados do provedor de identidade com o link relacionado **Importar metadados do provedor de identidade** ou atualize as propriedades manualmente.
- Para configurações do OpenID Connect, atualize as propriedades manualmente.

3. Para criar um novo provedor de identidade, clique em **Novo**.
   - Para configurações de token resumido: clique em **Resumo do SSO** e insira as propriedades de resumo do Single Sign-on de vários provedores.
   - Para configurações de SAML2: clique em **MultiSSOV2_SAML2_custom** e importe os metadados do provedor de identidade de um URL, como XML, ou insira manualmente as informações do provedor de identidade.

   - Para OpenID Connect: clique em **Conexão OpenID** e insira a ID de cliente, o segredo do cliente e o URL de configuração amplamente conhecido.

4. Para transformar um IdP no IdP de failover a ser usado quando o IdP padrão não estiver disponível, marque a caixa de seleção **Padrão**.

   Se você tiver a atualização 1 do SAML 2 ativa e fizer upgrade para a versão Fuji, o IdP da atualização 1 do SAML 2 será selecionado como o failover padrão. Nenhum IdP de failover padrão será selecionado para novas instâncias ou se você estiver atualizando de uma versão na qual a atualização 1 do SAML 2 não estiver ativa.

   Nota: O processo de importação de metadados cria automaticamente um registro de certificado para o provedor de identidade. Navegue até o módulo **Certificado x509** para ver o certificado.

   Nota: Os certificados de logon único devem estar sempre no formato PEM para funcionar com certificados SAML.

5. Se a assinatura eletrônica estiver ativa, configure o formulário do provedor de identidade e adicione o **URL de estipulação do cliente, para autenticação da assinatura eletrônica**. Na maioria dos casos, esse URL é: `https://YOURINSTANCE.service-now.com/consumer.do`. No entanto, se empregar um método personalizado para lidar com a autenticação SAML para assinatura eletrônica, você poderá configurar seu próprio

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

URL de consumidor. Se estiver usando somente a atualização 1 do SAML 2.0, não o Single Sign-on de vários provedores, configure o URL do consumidor de estipulação com propriedades SAML de assinatura eletrônica.

Como gerar metadados do provedor de serviço de instância (SP) para SAML

Como parte da configuração do SSO, você pode gerar os metadados SP da instância para fornecer ao IdP.

Antes de Iniciar
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa
O IdP precisa dos metadados do SP da instância para autenticar e encaminhar solicitações.

Procedimento

1. Escolha o plug-in SSO instalado:

Opção	Descrição
SSO Multiprovedor	Navegue até **SSO de vários provedores** > **Provedores de identidade**. Escolha um IdP e clique no botão **Gerar metadados**. A integração gera automaticamente os metadados do SP da instância a partir das configurações de propriedade do sistema.
SAML 2 SSO	Navegue até **SAML 2 Single Sign-on** > **Metadados**. A integração gera automaticamente os metadados do SP da instância a partir das configurações de propriedade do sistema.

2. Copie os metadados do SP na caixa de texto.

Por exemplo:

```
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
 entityID="https://yourinstance.service-now.com">
  <SPSSODescriptor AuthnRequestsSigned="false"
 WantAssertionsSigned="true"
 protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
  <SingleLogoutService
 Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
 Location="https://yourinstance.service-now.com/navpage.do" />

 <NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddres
s</NameIDFormat>
  <AssertionConsumerService isDefault="true" index="0"
 Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
 Location="https://yourinstance.service-now.com/navpage.do" />
  <AssertionConsumerService index="1"
 Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
 Location="https://yourinstance.service-now.com/consumer.do"/>
 </SPSSODescriptor>
</EntityDescriptor>
```

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Forneça os metadados do SP da instância para o IdP.
   Por exemplo, SSOCircle permite que um usuário forneça os metadados do SP online.

Configuração de usuários para SSO de vários provedores

Os administradores podem configurar o SSO de vários provedores para usuários individuais ou para todos os usuários que pertencem a uma empresa. Não é possível configurar SSO de vários provedores para grupos.

Antes de Iniciar
Função necessária: administrador

Procedimento

1. Navegue até **Todos** > **SSO de vários provedores** > **Provedores de identidade**.
2. Clique com o botão direito em um registro de provedor de identidade e selecione **Copiar sys_id**.
3. Copie os dados para a área de transferência.
4. Navegue até um registro de usuário ou um registro de empresa.
5. Configure o formulário e adicione o campo **Fonte do SSO**.
6. No campo **Fonte do SSO**, insira um dos seguintes:
   - **Usuários do SAML**: digite **sso:** seguido pelo sys_id do registro do provedor de identidade.
   - **Usuários da federação do SSO**: digite **federation:** seguido pelo sys_id do registro de federação.
7. Clique em **Atualizar**.

Teste de conexões IdP

Testar a conexão com um IdP valida as configurações antes da habilitação da autenticação externa.

Antes de Iniciar
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa
A versão Jakarta oferece suporte ao teste de conexão em uma janela pop-up. Se o seu IdP não funcionar corretamente com esta opção, será possível desativar esta configuração-padrão.
O trabalho de atualização de metadados do IDP Multi-SSO busca e atualiza o certificado do IDP ao criar, atualizar ou testar a conexão.

Nota: Para alguns casos, se o teste de conexão falhar, os IdPs precisarão criar glide.authenticate.multisso.test.connection.mandatory com o valor como falso, e você poderá ativar o idp sem a conexão de teste.

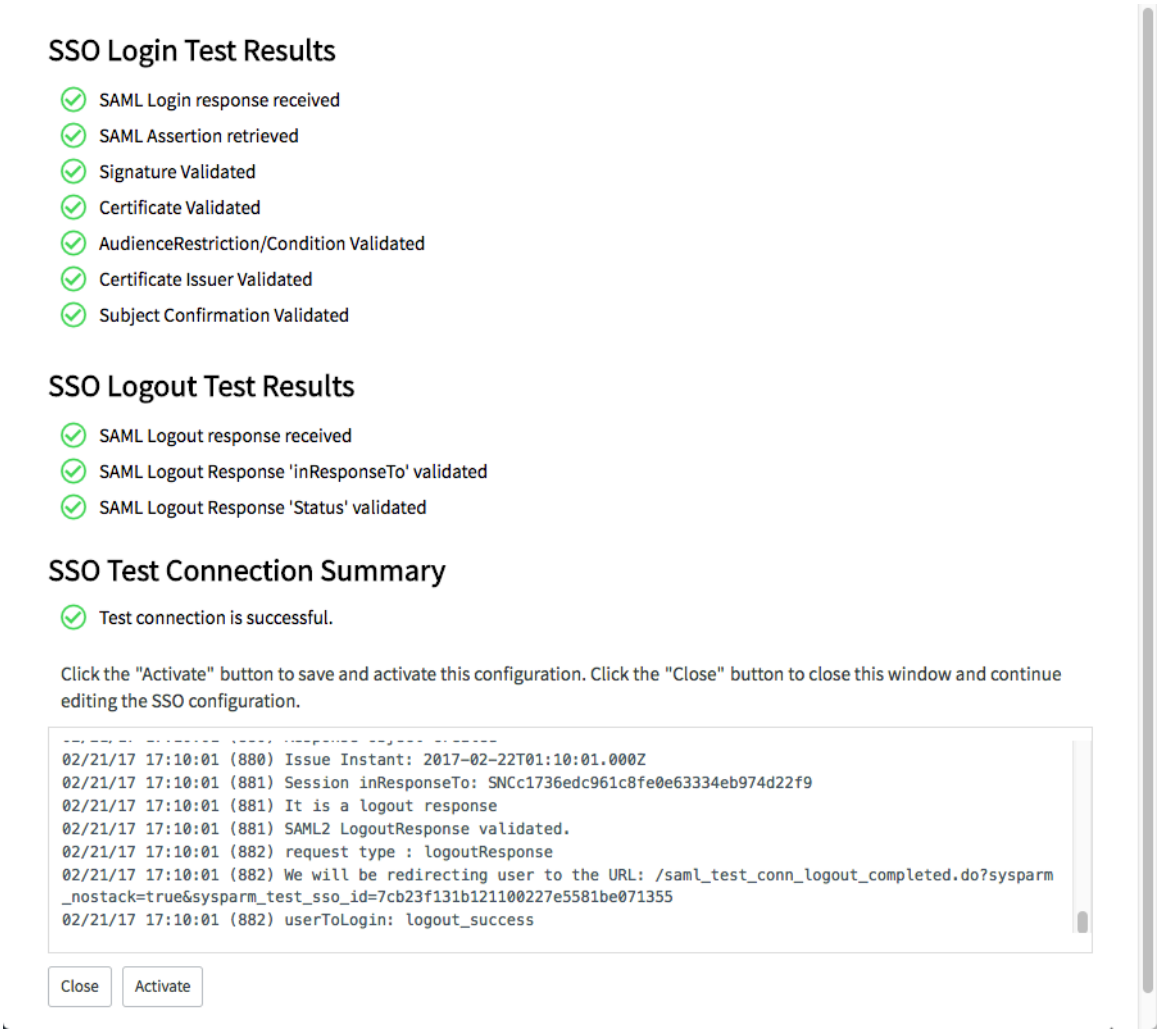
Procedimento

1. Navegue até **Todos** > **SSO de vários provedores** > **Provedores de identidade**.
2. Selecione um IdP definido ou clique em **Novo** para definir um novo IdP.
3. Opcional: Configure um provedor de identidade se estiver configurando um novo IdP.
4. Clique em **Testar conexão**e insira as credenciais de login do IdP para verificar o login.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Não é possível ativar o IdP até obter uma conexão de teste bem-sucedida. Se o teste falhar, será possível atualizar para salvar as informações de configuração, mas a configuração não poderá ser ativada.

5. Verifique os resultados usando os **Resumo/resultados de testes de SSO** ou a seção **Logs de teste de SSO** para ver as mensagens do registro em log.
   Se houver erros, consulte Correções e erros de Multi-SSO (SAML 2.0)
6. Clique em **Cancelar** quando o teste estiver concluído.



Erros comuns de conexão de IdP

A tabela a seguir descreve alguns dos erros comuns de conexão de IdP e suas soluções.

Solução de problemas de conexões de teste de IdP

Mensagens de erro	Solução
Falha na validação do campo de usuário. Campo de usuário inválido '<field name>' não é um campo na tabela sys_user.	Verifique se o conteúdo do campo selecionado da tabela Usuário corresponde ao token NameID do SAML.
O emissor da estipulação é inválido.	Verifique se o **URL do provedor de identidade** contém um URL válido para o seu IdP. Cada URL de IdP deve ser exclusivo.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Solução de problemas de conexões de teste de IdP

Mensagens de erro	Solução
Falha na validação de AudienceRestriction.	Verifique se o **URI do público** contém um URL válido para sua instância.
Não é possível sair da sessão do IdP.	Verifique se o URL **SingleLogoutRequest** contém um URL válido para o serviço de logout do IdP.
A assinatura não foi validada em relação à chave da credencial.	Verifique se o IdP tem um certificado válido instalado.

Solução de problemas de script com SAML

Solucione problemas de script com SAML. É possível que ocorram problemas de script se o SAML já estiver ativo no momento em que você ativar várias instâncias de Single Sign-on e se já tiver personalizado as saídas de instalação.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Backup da saída de instalação modificada SAML2SingleSignon_update1 e da inclusão de script SAML2_update1.
2. Reverta a saída da instalação e a inclusão de script para a versão que está disponível com o sistema de linha de base.
3. Ative ou faça upgrade do plug-in **Integration - Multiple Provider Single Sign-On**.
   O sistema faz upgrade do SAML e de todos os arquivos necessários para o Update 1 do SAML 2.
4. Abra a página de propriedades de SSO múltiplo e marque a caixa de seleção **Habilitar SSO de vários provedores** para habilitá-lo.
5. Coloque as mudanças de saída de instalação SAML2SingleSignon_update1 na inclusão de script de linha de base **MultiSSO_SAML2_Update1 e as mudanças de inclusão de script SAML2_update1 na** inclusão de script SAML2_update1 de linha de base.

Login usando SSO de vários provedores

O método recomendado e mais eficiente para login de usuários usando SSO de vários provedores é usando um URL configurado especificamente.

Antes de Iniciar

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

Depois que o SSO de vários provedores for configurado, você poderá enviar um URL aos usuários com o IdP correto na cadeia de caracteres do parâmetro. Por exemplo:

```
/login_with_sso.do?glide_sso_id=<sys_id of the sso configuration>
```

Depois que um usuário faz login com êxito na página do IdP, um cookie contendo o sys_id do IdP é adicionado ao navegador. Na próxima vez que o usuário tentar fazer login, o sistema o redirecionará para fazer login no servidor IdP, que faz login na instância automaticamente.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Se um parâmetro de URL não estiver definido ou o cache do navegador tiver sido excluído, os usuários também poderão fazer o seguinte:

Procedimento

1. Clique no link **Usar login externo** na página de login.

   A página de login externo é exibida. Os usuários podem clicar em **Usar login local** para retornar à página de login padrão.

2. Insira o valor do campo especificado na tabela Usuário configurada por você nas propriedades de SSO de vários provedores.

   O usuário é redirecionado para o servidor IdP, onde pode fazer login.

Resultados

Depois que fazem login com sucesso em um IdP, os usuários são redirecionados automaticamente para esse IdP sempre que tentam acessar a instância. Para que um usuário acesse um IdP diferente, envie a ele um URL com as novas informações de IdP no parâmetro. Se o usuário fizer login com êxito, o novo IdP substitui o IdP antigo no cookie. Se o usuário não fizer login com êxito, as informações do IdP antigo serão mantidas no cookie.

Permitir que os usuários escolham o provedor de identidade para login

O suporte à federação de SSO permite que os usuários escolham em qual IdP fazer login.

Antes de Iniciar

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

As federações de SSO agregam metadados de vários IdPs e provedores de serviços, incluindo sua instância. As federações publicam os metadados como um arquivo XML, que inclui informações como nomes de IdP e certificados de IdP. Os administradores podem instruir a instância a ler o arquivo XML e preencher automaticamente a tabela Propriedades do SSO com todas as informações de IdP necessárias.

Procedimento

1. Navegue até **Todos** > **SSO de vários provedores** > **Federação**.
2. Clique em **Nova**.
3. Preencha os campos conforme apropriado (consulte a tabela).
4. Clique em **Enviar**.
5. Depois de configurar uma federação, habilite a tarefa programada Atualizar metadados do SSO e configure os usuários que você deseja que acessem os IdPs de federação. Use o sys_ID do registro de federação que você acabou de criar.

   Use o sys_ID do registro de federação que você acabou de criar.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A instância preenche a tabela de propriedades do SSO com as informações do IdP. Quando os usuários configurados para usar a federação fazem login, eles são redirecionados para o URL do serviço de descoberta configurado por você. Em seguida, eles selecionam o IdP e fornecem as credenciais necessárias. Como alternativa, é possível enviar aos usuários um URL com o IdP no parâmetro.

Como permitir que os usuários escolham o provedor de identidade para login

Campo	Descrição
Nome	Insira um nome descritivo para a federação.
Ativo	Marque a caixa de seleção para permitir que a instância extraia o arquivo XML da federação.
Tipo	Selecione o tipo de autenticação compatível com esta federação.
Descoberta URL do serviço	Insira o URL do serviço de descoberta para esta federação. Este é o site para onde os usuários são direcionados para selecionar um IdP e fazer login.
URL de metadados	Insira o URL do arquivo XML que contém os metadados da federação.
Certificado x509	Selecione o certificado da federação.
Domínio	Selecione o domínio ao qual os dados pertencerão.

Nota: O IdP de gerenciamento de identidade federada InCommon é pré-configurado.

Uso de Portal de serviços com SSO de vários provedores para redirecionar um URL

Portal de serviços usa uma combinação de propriedades do sistema e inclusões de script para determinar como o sistema lida com redirecionamentos de URL para usuários que fazem login no portal.

Antes de Iniciar
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa
Se você estiver usando a propriedade do sistema para redirecionar automaticamente para o seu Provedor de identidade (IdP) primário, Portal de serviços redirecionará automaticamente para esse IdP. Se vários IdPs estiverem disponíveis, Portal de serviços exibirá um link na página de login para **Usar login externo**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Configurar a página de login do Portal de serviços
2. Redirecionar para o Portal de serviços após o login

Recuperação de conta (ACR)

Os administradores podem configurar a recuperação de conta (ACR) para executar atividades de recuperação, como lidar com erros de configuração de SSO ou certificados expirados.

Nota: Habilitar a ACR desabilita os logins interativos locais (com base em nome de usuário ou senha) quando o SSO está habilitado para suas instâncias.

A ACR fornece os seguintes recursos:

- Ignore o Single Sign-on (SSO) para solucionar problemas com a configuração do SSO como administrador.
- Faça login usando o SSO para executar tarefas com uma conta de administrador configurada como uma recuperação de conta.
- Os fluxos de ACR permitem que os administradores usem recursos de autoatendimento para lidar com a recuperação de conta quando houver necessidade de recuperação, por exemplo, configuração incorreta de SSO ou certificados expirados.
- Reduza o acesso não autorizado às instâncias e forneça uma base sólida para o uso da ACR fora dos casos de uso do SSO.

Nova instância

Para que uma nova instância use a ACR, você deve fazer o seguinte:

- Ativar o plug-in Multi-SSO (`com.snc.integration.sso.multi.installer`)
- Habilitar a ACR (`glide.sso.acr.enabled`) — Habilitado por padrão no caso de novas instâncias.
- Antes de habilitar a propriedade SSO (`glide.authenticate.multisso.enabled`), o administrador deve se inscrever como um usuário da ACR.

  Nota: Definir esta propriedade como falsa não desabilitará o SSO de vários provedores se a recuperação de conta (ACR) também estiver habilitada na instância. Para fazer login com nome de usuário e senha, a ACR também deve ser desabilitada por meio da propriedade *`glide.sso.acr.enabled`*. Para obter detalhes sobre esta propriedade, consulte Propriedades de recuperação de conta.

- Antes de se inscrever como um usuário da ACR, o administrador deve definir uma senha para login local e registrar a MFA.

Instância com upgrade

Para que uma instância com upgrade use a ACR, você deve fazer o seguinte:

- Ativar o plug-in Multi-SSO (`com.snc.integration.sso.multi.installer`)
- Habilitar a ACR (`glide.sso.acr.enabled`)

Nota: No caso de uma instância atualizada, o administrador deve habilitar a ACR.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Antes de habilitar a propriedade SSO (`glide.authenticate.multisso.enabled`), o administrador deve se inscrever como um usuário da ACR.
- Antes de se inscrever como um usuário da ACR, o administrador deve definir uma senha para login local e registrar a MFA.

Configuração de usuários de recuperação de conta

Para usar a recuperação de conta, registre pelo menos uma conta de administrador como um usuário de recuperação de conta. O Single Sign-on não pode ser ativado em sua instância até que pelo menos uma conta seja configurada. Para obter detalhes sobre este processo, consulte Configuração de um usuário de recuperação de conta na página Propriedades de recuperação de conta.

Nota: Se você estiver atualizando uma instância que já utilize o Single Sign-on para Rome ou uma versão posterior, o Single Sign-on continuará a funcionar sem um usuário de recuperação configurado.

Configuração de recuperação de conta

O recurso de recuperação de conta está incluso nos plug-ins **Integration - Multiple Provider Single Sign-On Installer (com.snc.integration.sso.multi.installer)**. O recurso está habilitado por padrão. É possível alterar esta e outras configurações de recuperação de conta usando as propriedades do sistema. Para obter detalhes sobre estas propriedades, consulte Propriedades de recuperação de conta.

Contexto da política de recuperação de conta

Depois de registrar um usuário de recuperação de conta e habilitar o Single Sign-on (SSO), sua instância restringirá todos os logins locais. Essa restrição é definida no contexto da política de autenticação **SSO — Contexto de ACR**. Para obter mais informações sobre o contexto, consulte Contexto de recuperação de conta.

Para obter detalhes sobre como as políticas de autenticação e contextos de política, e como eles funcionam em sua instância, consulte Autenticação adaptável.

Configuração de um usuário de recuperação de conta

Configure um usuário de recuperação de conta para executar atividades de recuperação de conta em sua instância.

Um usuário de recuperação de conta é uma conta de usuário que os administradores podem usar para executar tarefas de recuperação de conta, como lidar com uma configuração incorreta de SSO ou lidar com certificados expirados.

Nota: Se estiver usando a recuperação de conta em sua instância, será necessário configurar um usuário de recuperação de conta. Esta etapa é necessária antes de habilitar o Single Sign-on de vários provedores em uma instância.

Configuração de um usuário de recuperação de conta na página Propriedades de recuperação de conta

Configure uma recuperação de conta na página Propriedades de recuperação de conta.

Antes de Iniciar

Função necessária: administrador

Para que uma nova instância configure a ACR, você deve fazer o seguinte:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Ativar o plug-in Multi-SSO (`com.snc.integration.sso.multi.installer`)
- Habilitar a ACR (`glide.sso.acr.enabled`) — Habilitado por padrão no caso de novas instâncias.
- Antes de habilitar a propriedade SSO (`glide.authenticate.multisso.enabled`), o administrador deve se inscrever como um usuário da ACR.
- Antes de se inscrever como um usuário da ACR, o administrador deve definir uma senha para login local e registrar a MFA.

Para que uma instância atualizada use a ACR, você deve fazer o seguinte:

- Ativar o plug-in Multi-SSO (`com.snc.integration.sso.multi.installer`)
- Habilitar a ACR (`glide.sso.acr.enabled`)

  Nota: No caso de uma instância atualizada, o administrador deve habilitar a ACR.

- Antes de habilitar a propriedade SSO (`glide.authenticate.multisso.enabled`), o administrador deve se inscrever como um usuário da ACR.

  Nota: Definir esta propriedade como falsa não desabilitará o SSO de vários provedores se a recuperação de conta (ACR) também estiver habilitada na instância. Para fazer login com nome de usuário e senha, a ACR também deve ser desabilitada por meio da propriedade *`glide.sso.acr.enabled`*. Para obter detalhes sobre esta propriedade, consulte Propriedades de recuperação de conta.

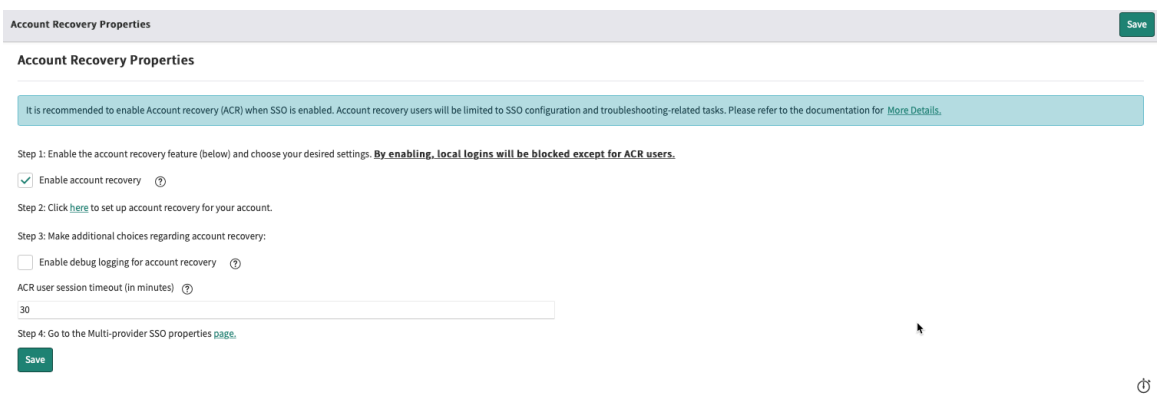
- Antes de se inscrever como um usuário da ACR, o administrador deve definir uma senha para login local e registrar a MFA.

Procedimento

1. Navegue até **Todos** > **Recuperação de conta** > **Propriedades**.
2. Clique em **Habilitar recuperação de conta**.

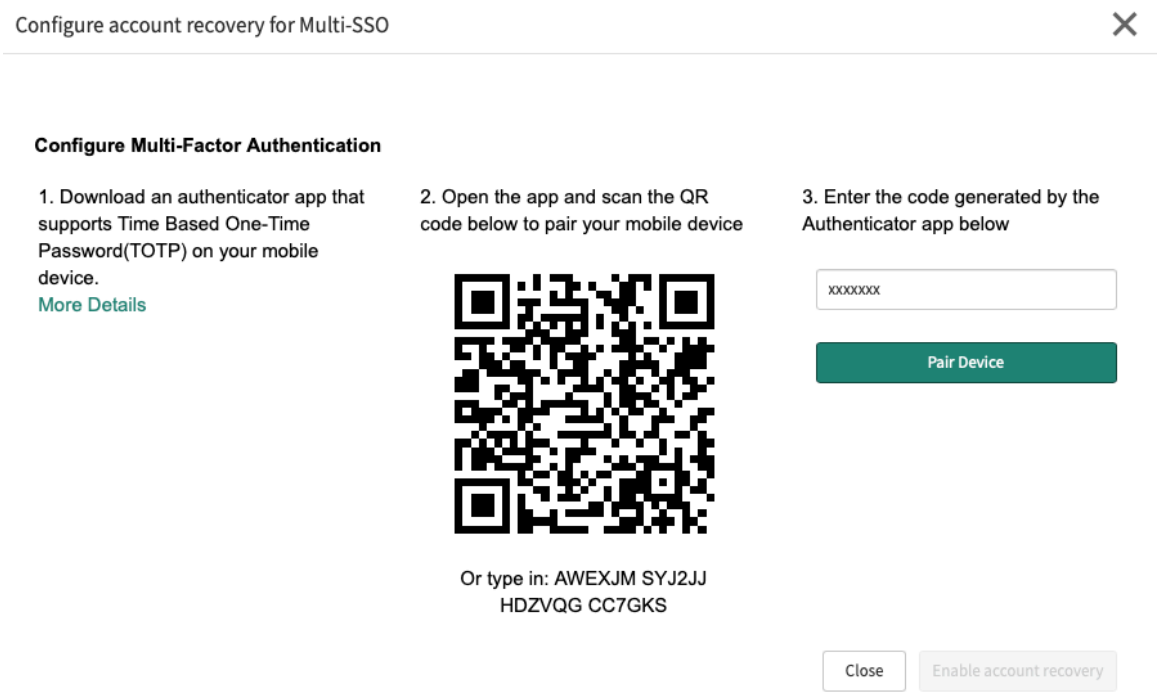
   Nota: É necessário habilitar a recuperação de conta quando o SSO estiver habilitado. Os usuários da recuperação de conta estarão limitados à configuração do SSO e tarefas relacionadas à solução de problemas.

3. Clique no texto **aqui** na Etapa 2.



© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Seguindo as instruções na tela em **Configurar recuperação de conta para o modal Multi-SSO**.



Habilitar recuperação de conta será habilitado depois que as etapas na tela forem concluídas.

5. Clique em **Habilitar recuperação de conta**.

Resultados

Você configurou sua conta de usuário como um usuário de recuperação de conta. É possível verificar esta conta e ver todos os outros usuários de recuperação de conta configurados, navegando até **SSO de vários provedores** > **Recuperação de conta** > **Usuários**.

Configuração de um usuário de recuperação de conta a partir de um perfil do usuário administrador

Configure um administrador como um usuário de recuperação de conta do perfil do usuário administrador.

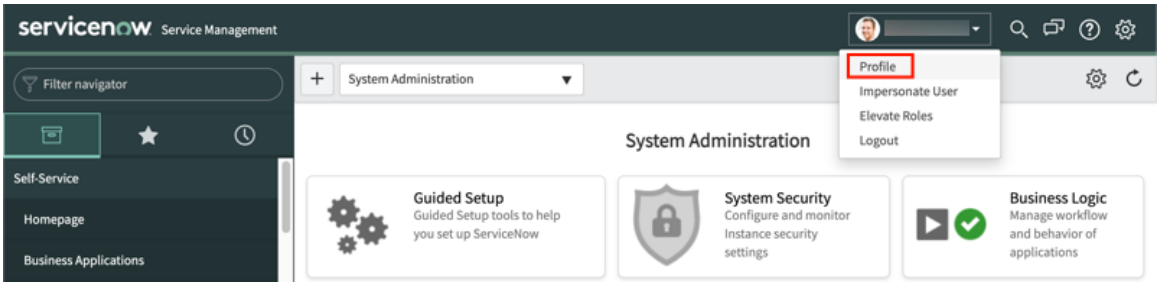
Antes de Iniciar

Função necessária: administrador

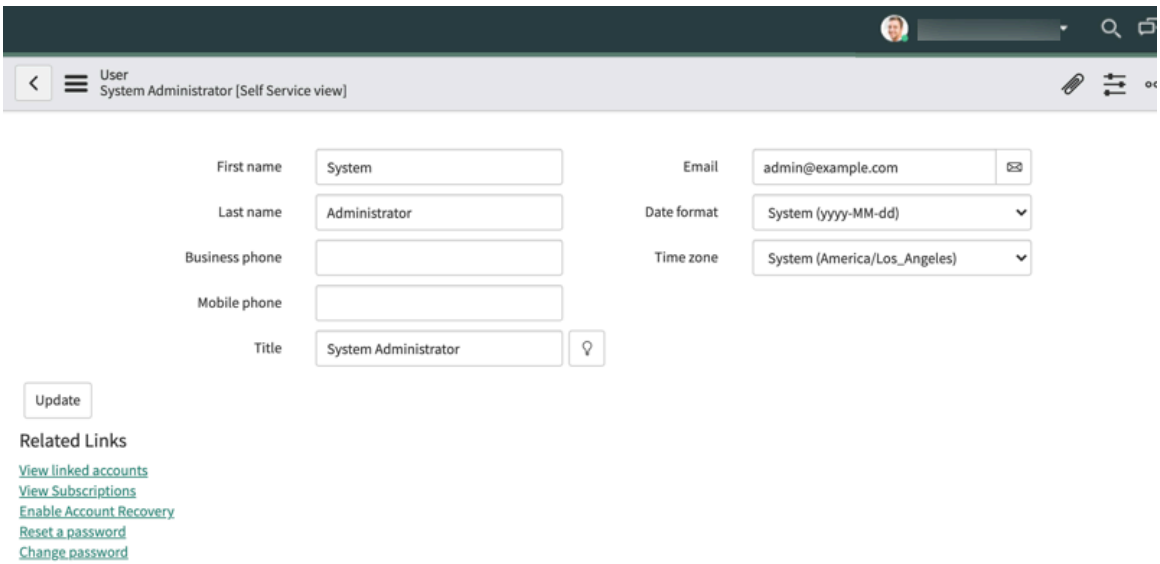
Procedimento

1. Faça login em sua instância usando uma conta de administrador.
2. Clique no nome do usuário no cabeçalho da instância e selecione **Perfil**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. No formulário **Usuário**, clique em **Habilitar recuperação de conta** na seção **Links relacionados**.

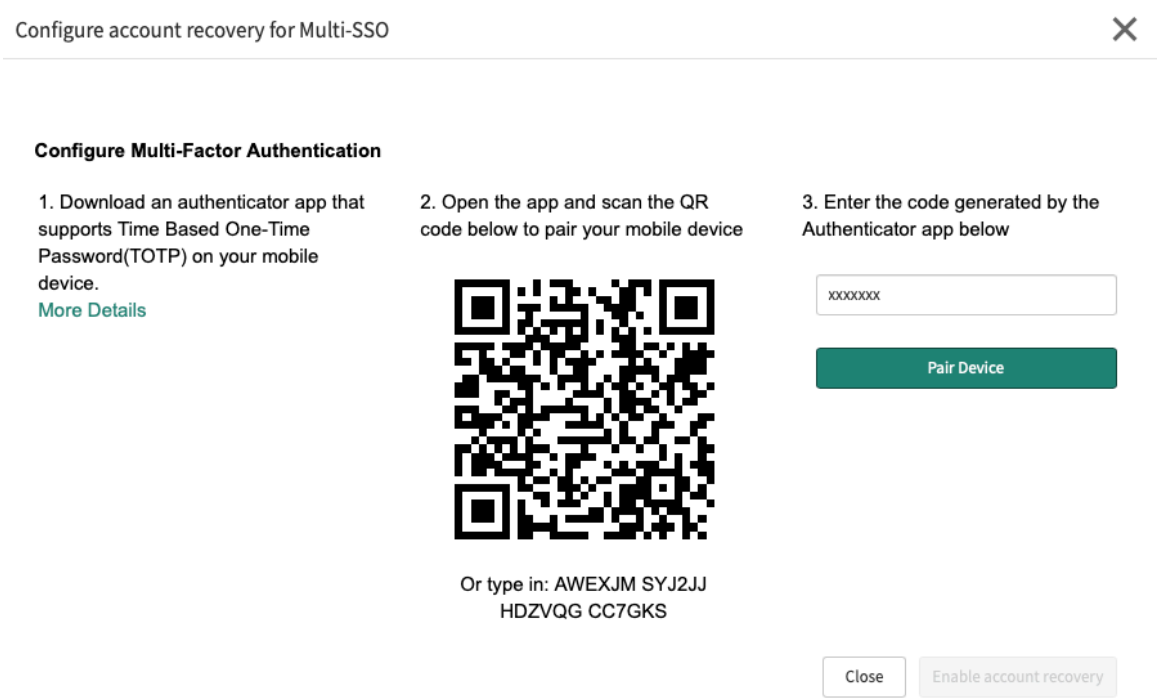


Nota:

Se o usuário selecionado já tiver a recuperação de conta habilitada, **Habilitar recuperação de conta** não será exibido nos links relacionados. Em vez disso, a opção **Desabilitar recuperação de conta** será exibida.

4. Seguindo as instruções na tela em **Configurar recuperação de conta para o modal Multi-SSO**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Habilitar recuperação de conta será habilitado depois que as etapas na tela forem concluídas.

5. Clique em **Habilitar recuperação de conta**.

Resultados

Você configurou sua conta de usuário como um usuário de recuperação de conta. É possível verificar esta conta e ver todos os outros usuários de recuperação de conta configurados, navegando até **SSO de vários provedores** > **Recuperação de conta** > **Usuários**.

Propriedades de recuperação de conta

Use as propriedades do sistema para configurar a recuperação de conta (ACR) em sua instância.

Acesse as propriedades de recuperação de conta em sua instância navegando até **SSO de vários provedores** > **Recuperação de conta** > **Propriedades**.

Propriedades do sistema de recuperação de conta

Propriedade	Descrição
Habilitar recurso de recuperação de conta [glide.sso.acr.enabled]	Se o recurso de recuperação de conta está habilitado em sua instância. Esta propriedade está habilitada por padrão.
Habilitar registro em log de depuração para recuperação de conta [glide.sso.acr.debug.log.enabled]	Se sua instância inclui informações de recuperação de conta no registro log de depuração. Esta propriedade está desabilitada por padrão.
Tempo limite da sessão do usuário da ACR (em minutos) [glide.sso.acr.ui.session.timeout]	Minutos de inatividade antes de sua instância encerrar uma sessão de usuário de

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Propriedades do sistema de recuperação de conta

Propriedade	Descrição
	recuperação de conta. Esta propriedade tem um valor padrão de 30.

Assinatura eletrônica com SSO para vários provedores

A assinatura eletrônica com SSO para vários provedores permite que você use as propriedades de assinatura eletrônica em vez das propriedades do SAML ou do OIDC para autenticação.

Para verificação de single sign-on (SSO) durante a autenticação e para exigir que os usuários forneçam credenciais antes de enviar sua assinatura eletrônica, você pode configurar a autenticação para solicitar credenciais do usuário antes de enviar uma assinatura.

Você pode instalar o plug-in Aprovações com assinatura eletrônica (`com.glide.e_signature_approvals`) para ter a configuração de assinatura eletrônica para logins por SSO.

Nota: Você deve instalar as assinaturas da Assinatura de código (`com.glide.code_signing.signatures`) para instalar o plug-in de assinatura eletrônica.

Ativação do plug-in Approval with e-Signature

O plug-in Approval with e-Signature (com.glide.e_signature_approvals) permite que os usuários aprovem solicitações ao reinserir suas credenciais de login.

Antes de Iniciar

Função necessária: admin

Nota: Você deve instalar as assinaturas da Assinatura de código (`com.glide.code_signing.signatures`) para instalar o plug-in de assinatura eletrônica.

Procedimento

1. Navegue até **Todos** > **Aplicações do sistema** > **Todas as aplicações disponíveis** > **Todas**.
2. Encontre o plug-in usando os critérios de filtro e a barra de pesquisa.

   Pesquise o plug-in pelo nome ou ID. Se não conseguir encontrar um plug-in, talvez seja necessário solicitá-lo ao pessoal ServiceNow.

3. Selecione **Instalar** para iniciar o processo de instalação.

   Nota: Quando a separação de domínio e o administrador delegado estão habilitados em uma instância, o usuário administrativo deve estar no domínio **global.** Caso contrário, será exibido o seguinte erro: `A instalação da aplicação não está disponível porque há outra operação em execução: ativação de plug-in para <plugin name>.`

   Você verá uma mensagem após a conclusão da instalação.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Use o SSO de vários provedores para configurar uma aprovação de SSO para uma autenticação SAML 2.0

Uma aprovação de SSO com assinatura eletrônica requer configuração no IdP SAML e na instância ServiceNow.

Antes de Iniciar
Função necessária: admin

Por Que e Quando Desempenhar Esta Tarefa
O IdP do SAML deve oferecer suporte e honrar o atributo forceAuthn nas solicitações de asserção do SAML. A assinatura eletrônica não funciona sem esta configuração de IdP. Configure uma aprovação com assinatura eletrônica usando as credenciais de uma autenticação SAML 2.0.

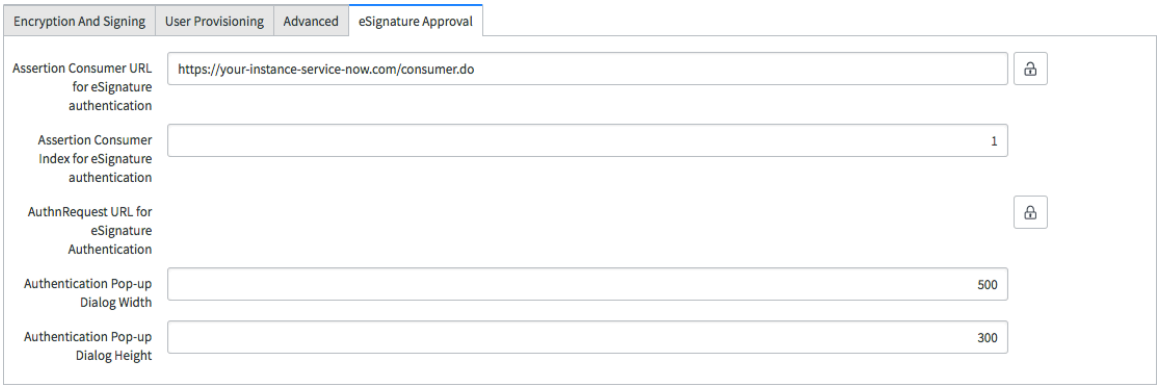
Procedimento

1. Ative ou faça upgrade para SAML 2.0 com o plug-in Activate Multi-Provider SSO.
2. Ative o plug-in Approval with e-Signature.
3. Navegue até **SSO de vários provedores** > **Provedores de identidade** e verifique se a guia Avançado da configuração de 2.0 SAML IdP mostra o atributo **Forçar AuthnRequest** verificado.
   Seu IdP SAML 2.0 deve oferecer suporte ao atributo **Forçar AuthnRequest**, ou a assinatura eletrônica não será compatível.
4. Na guia Aprovação com assinatura eletrônica, insira as propriedades SAML de assinatura eletrônica a seguir.

Opção	Descrição
URL de estipulação do cliente, para autenticação da assinatura eletrônica	Esta propriedade é padronizada para o URL apropriado. Para configurar esta propriedade, clique no ícone de cadeado para tornar este campo editável. Após as edições, selecione o ícone para bloquear o campo.
Índice de estipulação do cliente, para autenticação da assinatura eletrônica	Se seu provedor de serviço tiver mais de um URL definido para o AssertionConsumerURL, você poderá definir o índice a ser usado para a assinatura eletrônica, começando com o índice 1 ou mais.
URL AuthnRequest para autenticação com assinatura eletrônica	Você pode inserir o URL que aponta para o URL de AuthnRequest do IdP do SAML 2.0 para autenticação com assinatura eletrônica. Se o URL for o mesmo URL do consumidor de estipulação, você poderá deixar essa configuração vazia.
Largura da caixa de diálogo de autenticação	Quando um usuário aprova uma solicitação usando a assinatura eletrônica, uma caixa de diálogo é aberta e um usuário pode inserir credenciais. Esta configuração controla a largura da caixa de diálogo. O padrão é 500.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
Altura da caixa de diálogo de autenticação	Quando um usuário aprova uma solicitação usando a assinatura eletrônica, uma caixa de diálogo é aberta e um usuário pode inserir credenciais. Essa configuração controla a altura da caixa de diálogo. O padrão é 300.



5. Selecione o botão **Gerar metadados** abaixo das guias para gerar novamente os metadados do provedor de serviços.
6. Copie os metadados do provedor de serviços e atualize-os no IdP SAML.

Uso de um SSO de vários provedores para configurar uma aprovação de SSO para uma autenticação OIDC

Uma aprovação de SSO com assinatura eletrônica requer configuração no IdP SAML e na instância ServiceNow.

Antes de Iniciar
Função necessária: admin

Por Que e Quando Desempenhar Esta Tarefa
O IdP do SAML deve oferecer suporte e honrar o atributo forceAuthn nas solicitações de asserção do SAML. A assinatura eletrônica não funciona sem esta configuração de IdP. Configure uma aprovação com assinatura eletrônica usando as credenciais de uma autenticação SAML 2.0.

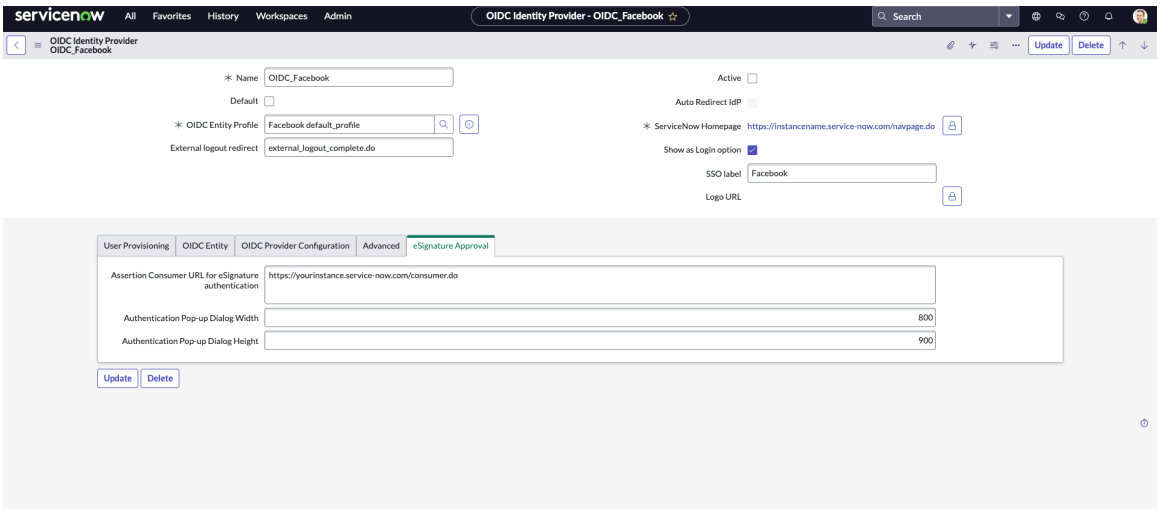
Procedimento

1. Ative o plug-in Approval with e-Signature.
2. Navegue até **SSO de vários provedores** > **Provedor de identidade** e verifique as configurações do seu provedor OIDC
3. Na guia Aprovação com assinatura eletrônica, insira as propriedades SAML de assinatura eletrônica a seguir.

Opção	Descrição
URL de estipulação do cliente, para autenticação da assinatura eletrônica	Esta propriedade é padronizada para o URL apropriado. Para configurar esta propriedade, clique no ícone de cadeado para tornar este campo editável. Após as edições, selecione o ícone para bloquear o campo.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
Largura da caixa de diálogo de autenticação	Quando um usuário aprova uma solicitação usando a assinatura eletrônica, uma caixa de diálogo é aberta e um usuário pode inserir credenciais. Esta configuração controla a largura da caixa de diálogo. O padrão é 800.
Altura da caixa de diálogo de autenticação	Quando um usuário aprova uma solicitação usando a assinatura eletrônica, uma caixa de diálogo é aberta e um usuário pode inserir credenciais. Essa configuração controla a altura da caixa de diálogo. O padrão é 900.



4. Selecione **Enviar** se você estiver configurando a assinatura eletrônica durante a configuração inicial do OIDC ou **Atualizar** se quiser atualizar os detalhes na assinatura eletrônica.

OpenID Connect (OIDC) como um provedor de identidade (IdP) de Single Sign-on (SSO)

O OpenID Connect (OIDC) é uma camada de identidade criada na parte superior do protocolo OAuth e que fornece uma experiência de Single Sign-on (SSO) moderna e intuitiva para você e seus usuários finais. A OIDC também melhora a experiência de login para aplicações móveis, permitindo que os usuários façam login em ServiceNow aplicações usando seu provedor de identidade social. Por exemplo, os administradores podem configurar o Single Sign-on com um provedor de identidade de terceiros que ofereça suporte ao OpenID Connect. Os usuários têm a opção de fazer login na sua aplicação personalizada ServiceNow usando as credenciais do provedor de identidade.

Você pode escolher usar provedores de identidade social como Google para seus usuários de empresa para cliente (B2C) e provedores de identidade corporativa como Okta , Microsoft Azure AD para seus usuários de empresa para empresa.

Criação de uma configuração OpenID Connect (OIDC) para Single Sign-On (SSO)

Crie ou atualize uma configuração de OpenID Connect (OIDC) usando o plug-in Multi-Provider SSO.

Configuração do OpenID Connect (OIDC) para Single Sign-On (SSO)

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

- Registre uma aplicação OIDC com seu provedor de identidade (IdP) e anote a ID de cliente, o segredo do cliente e o URL de configuração amplamente conhecido.
- Ativar plug-in Multi-Provider SSO
- Configure as propriedades de SSO de vários provedores
- Ative a aprovação com o plug-in Approval with E-Signature para habilitar a assinatura eletrônica para o IdP OIDC.
- Função necessária: administrador

Se você tiver a ID de cliente, o segredo do cliente e o URL de configuração amplamente conhecido do provedor de identidade, poderá importar diretamente a configuração da OIDC para o SSO.

Nota: A opção de login com IdP OIDC não será compatível se o plug-in Domain Separation estiver instalado.

Se as informações necessárias sobre o provedor de identidade não estiverem disponíveis, será possível configurar manualmente a OIDC para SSO. Depois de concluir a configuração, os usuários podem fazer login nas aplicações do ServiceNow usando provedores de identidade social de terceiros, como Google Okta.

Procedimento

1. Navegue até **Todos** > **SSO de vários provedores** > **Provedores de identidade**.
2. Escolha uma das opções a seguir.
   - Para atualizar uma configuração existente, clique em um registro de provedor de identidade OIDC.
   - Para criar uma nova configuração, clique em **Novo** e selecione **OpenID Connect**.
3. Para uma nova configuração, insira as informações de configuração da OIDC usando um dos seguintes métodos:

Opção	Descrição
Importar configuração conhecida da OpenID Connect	Se você tiver o URL de configuração amplamente conhecido com suas credenciais de cliente associadas, poderá importar uma configuração diretamente da OIDC. **Nota:** Se você importar a configuração conhecida da OIDC, todos os campos relacionados serão preenchidos automaticamente.
Configurar o formulário do provedor de identidade de OIDC manualmente	Se você não tiver uma entidade OAuth OIDC existente, feche o pop-up Importar configuração conhecida da OpenID Connect e preencha os campos no formulário do provedor de identidade OIDC manualmente.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Importação de campos de configuração conhecida da OpenID Connect

Propriedade	Descrição
Nome	Nome exclusivo para a configuração do provedor de identidade OIDC.
ID de cliente	ID de cliente da aplicação registrada no provedor de identidade OIDC de terceiros.
Segredo do cliente	Segredo do cliente da aplicação registrado no provedor de identidade OIDC de terceiros.
URL de configuração amplamente conhecido	URL que contém metadados sobre o provedor de identidade OIDC de terceiros.

Todos os campos obrigatórios devem ser preenchidos no formulário do provedor de identidade OIDC.

Antes de preencher manualmente o formulário do provedor de identidade OIDC, verifique se você já possui um perfil de entidade OAuth para o IdP OIDC.

Se não tiver um perfil de entidade OAuth, você poderá criá-lo usando os modelos-padrão de provedor OIDC externo, como Okta, Azure e outros.

O tipo de concessão do perfil de entidade OAuth deve conter um código de autorização. Para obter mais informações, consulte Configurar um provedor OAuth OIDC na Now Platform.

Nota: É possível usar os modelos de provedores de identidade de terceiros, Auth0, Azure AD, Google e Okta que estão disponíveis nos dados de demonstração do plug-in Multiple Provider Single Sign-On Installer.

Campos de Provedor de identidade OIDC

Propriedade	Descrição
Nome	Nome do registro do provedor de identidade OIDC.
Ativo	Opção para ativar a configuração do IdP OIDC. **Nota:** Esta opção pode ser definida como ativa somente após um teste de conexão bem-sucedido.
Padrão	Opção para definir a configuração IdP OIDC como padrão quando mais de uma configuração OIDC estiver disponível.
Redirecionar IdP automaticamente	Opção para habilitar o redirecionamento automático dos usuários para a página de login do provedor de identidade. Este campo mostra quando a opção **Definir como IdP de redirecionamento automático** está definida na seção Links relacionados.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Propriedade	Descrição
	Nota: Se uma nova configuração Redirecionar IdP automaticamente for ativada, o cookie *glide_sso_id* será atualizado automaticamente com o novo IdP de redirecionamento automático. A propriedade do sistema *glide.authenticate.sso.update.idp.cookie* controla este recurso.
Perfil de entidade de OIDC	Perfil de entidade OAuth para a configuração de OIDC.
ServiceNow Página inicial	O URL da página de login usada para autenticação. Este campo é definido automaticamente como o URL da sua instância. O formato da URL é `https://yourinstance.service-now.com/navpage.do`
Redirecionamento de logout externo	O URL para onde a integração redireciona os usuários após o logout. Normalmente, o portal que é usado para SSO. Este campo é definido automaticamente como `external_logout_complete.do` Por exemplo, `https://yourinstance.service-now.com/external_logout_complete.do`
Mostrar como opção de login	Opção para exibir o IdP OIDC como uma opção de login na página de login. A opção de login aparece como o botão **login com o Provedor de identidade**.
Rótulo de SSO	Rótulo do IdP OIDC exibido na página de login. Este campo é exibido somente quando **Mostrar como opção de login** está habilitada.
URL do logotipo	URL publicamente disponível que contém o logotipo do provedor IdP OIDC. Este campo é exibido somente quando **Mostrar como opção de login** está habilitada.

4. Opcional: Habilite o provisionamento automático de usuário na guia Provisionamento de usuário>guia Provisionamento de usuário.

   (Optional) Você pode optar por habilitar o provisionamento automático de usuários durante o login do usuário. Quando o provisionamento automático de usuário está habilitado, um registro de usuário é criado automaticamente na instância da ServiceNow se ainda não existir.

Campos de Provisionamento de usuário

Propriedade	Descrição
Provisionar usuários automaticamente	Opção para habilitar o provisionamento automático de usuários. Esta propriedade cria um usuário na tabela Usuário (sys_user) da instância quando o usuário faz a saída do IdP, mas não existe na tabela Usuário.
Provisionar usando	Fonte de dados a ser usada para transformar um `token de ID`, um endpoint de `informações do usuário` ou um `token de ID e informações de usuário` em um usuário ServiceNow. Use a lista de pesquisa para selecionar o modelo de fonte de dados predefinido e abra o registro para configurar o mapeamento da tabela de transformações.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Propriedade	Descrição
Provisionar fonte de dados	Fonte de dados do token de ID usada para provisionamento de usuário.
Fonte de dados de informações do usuário	A fonte de dados do endpoint de informações do usuário usada para provisionamento de usuários. Este campo é exibido quando `Informações do usuário` ou `Token de ID e informações do usuário` são selecionados para o campo **Provisionar usando**.
Atualizar usuário no próximo login	Opção para habilitar a atualização do usuário durante o próximo login.
Atualizar tempo de intervalo do usuário (segundos)	Intervalo de tempo mínimo em segundos para atualizar o registro de usuário entre os logins subsequentes. Este campo é definido automaticamente para 3.600 segundos. Por exemplo, depois que um usuário faz login, o registro do usuário será atualizado após 3.600 segundos até o próximo login. Este campo está disponível somente quando o campo **Atualizar usuário no próximo login** está habilitado.
Funções de usuário aplicadas aos usuários provisionados	Lista de funções aplicadas aos usuários recém-provisionados.

5. Guia Entidade OIDC
   É possível exibir e modificar a configuração do cliente OIDC e o fluxo de conexão da OIDC usando o registro da entidade.
6. Guia Configuração de provedor OIDC
   Você pode exibir e modificar o URL de configuração amplamente conhecido do IdP OIDC ou da validação da declaração do token de ID.
7. Opcional: Guia Avançado

   (Optional) Scripts que são executados durante o Single Sign-on e o logout.

   Campos de Avançado

Propriedade	Descrição
Script de Single Sign-on	Script que é executado durante o Single Sign-On. Esse campo é definido automaticamente como `MultiSSO_OIDC_custom`.
Script de logout	Script que é executado depois que o usuário faz logout. Esse campo é definido automaticamente como `MultiSSO_OIDC_logout_custom`.

8. Opcional: Na guia Aprovação de assinatura eletrônica, configure a assinatura eletrônica para o Idp OIDC.

   Nota: A guia Aprovação de assinatura eletrônica é exibida somente quando o plug-in **Approval with e-Signature** (com.glide.e_signature_approvals) está instalado.

   Campos de aprovação de assinatura eletrônica

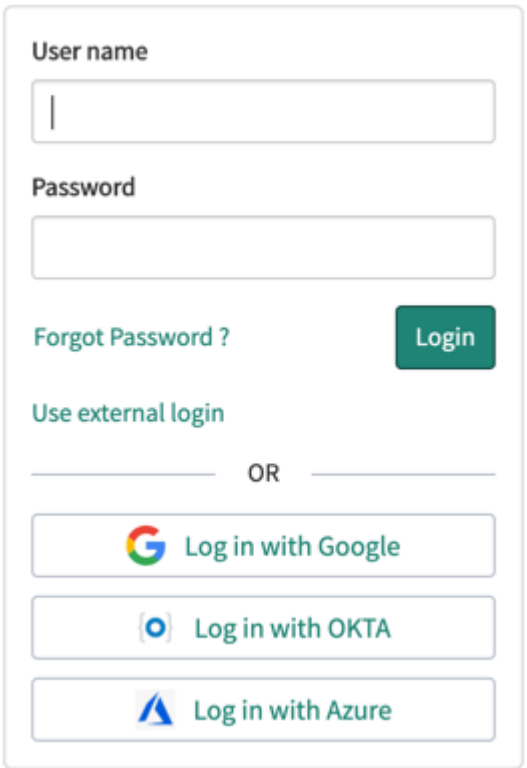
Propriedade	Descrição
URL de estipulação do cliente, para autenticação da assinatura eletrônica	Se empregar um método personalizado para lidar com a autenticação OIDC

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Propriedade	Descrição
	para assinatura eletrônica, você poderá configurar seu próprio URL de consumidor. Por exemplo, se estiver usando o SSO de vários provedores, você não precisará usar esta propriedade. Este formato da URL é `https://yourinstance.service-now.com/consumer.do`
Largura da caixa de diálogo de autenticação	Largura da caixa de diálogo de autenticação. Esse campo é definido automaticamente para `800`.
Altura da caixa de diálogo de autenticação	Altura da caixa de diálogo de autenticação. Esse campo é definido automaticamente para `900`.

9. Opcional: Navegue até a página de login da instância para verificar se o IdP aparece como uma opção de login.
   O URL deve estar no seguinte formato: `https://yourinstance/login_with_sso.do?glide_sso_id=sysId_IdP`

   Nota: Se a opção **Selecionado como opção de login** estiver habilitada, você poderá acessar o URL de login da instância.



Uso do SSO (Single Sign-On) baseado no Facebook

Faça login em sua instância ServiceNow usando suas credenciais Facebook no SSO baseado no Facebook.

Antes de Iniciar

O SSO baseado no Facebook é enviado junto com sua instância ServiceNow.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

É possível definir as configurações do provedor de identidade (Idp) para o IdP **OIDC_Facebook** como seus **provedores de identidade**. Para obter mais informações sobre configurações de Idp, consulte Configuração de um Single Sign-on (SSO) baseado no Facebook.

Função necessária: administrador

Procedimento

1. Navegue até **Todos** > **SSO de vários provedores** > **Provedores de identidade**.
2. Selecione **OIDC_Facebook**.
3. Na página OIDC_Facebook, especifique os seguintes campos:

Nota:

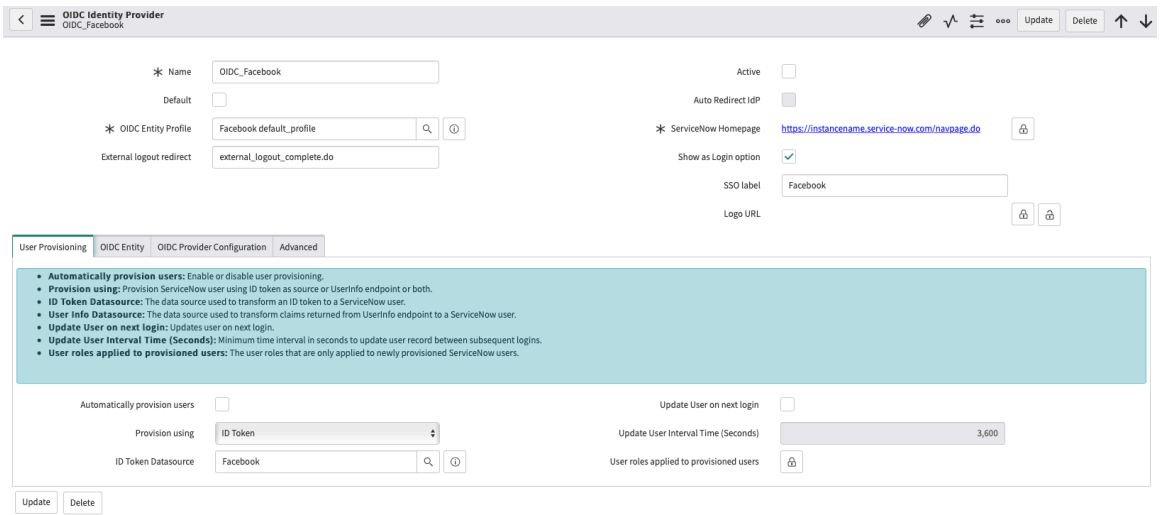
- A maioria dos campos é preenchida automaticamente se o IdP padrão estiver em uso.
- Detalhes da página inicial ServiceNow devem ser fornecidos.
- Detalhes relacionados ao usuário, como ID de cliente e segredo do cliente de Facebook, devem ser fornecidos no IdP.

Detalhes do provedor de identidade de OIDC_Facebook

Campo	Descrição
Nome	Nome do registro IdP OIDC. Insira `OIDC_Facebook`.
Padrão	Opção para definir a configuração IdP OIDC como padrão.
Perfil de entidade de OIDC	Perfil de entidade OAuth para a configuração de OIDC. Insira `o default_profile do Facebook`.
Redirecionamento de logout externo	O URL para onde a integração redireciona os usuários após o logout. Normalmente, esse URL é o portal usado para o SSO. Este campo é definido automaticamente como **external_logout_complete.do**. Por exemplo, `https://<yourinstance>.service-now.com/external_logout_complete.do`.
Ativo	Opção para ativar a configuração do IdP OIDC. **Nota:** Esta opção pode ser definida como ativa somente após um teste de conexão bem-sucedido.
Redirecionar IdP automaticamente	Opção para habilitar o redirecionamento automático dos usuários para a página de login do provedor de identidade.
ServiceNow Página inicial	O URL da página de login que é usada para autenticação. Este campo é definido automaticamente como o URL da sua instância. O formato do URL é `https://`

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	`<yourinstance>.service-now.com/navpage.do`
Mostrar como Opção de login	Opção para exibir o IdP OIDC como uma opção de login na página de login. Nesse caso, a opção de login é exibida como o botão **Login com Facebook**.
Rótulo de SSO	Rótulo do IdP OIDC exibido na página de login. Este campo é exibido somente quando **Mostrar como opção de login** está habilitada.
URL de logotipo	URL publicamente disponível que contém o logotipo do provedor IdP OIDC. Este campo é exibido somente quando **Mostrar como opção de login** está habilitada.



4. Opcional: Abra a guia **Provisionamento do usuário** e preencha os campos.

Nota: Você deve configurar as informações relacionadas à OIDC, como ID de cliente e segredo do cliente dos seus usuários de Facebook.

Guia Provisionamento de usuário

Campo	Descrição
Provisionar usuários automaticamente	Opção para habilitar o provisionamento automático de usuários. Esta propriedade cria um usuário na tabela Usuário [sys_user] da instância quando o usuário existe no IdP, mas não existe na tabela Usuário. **Nota:** Você pode optar por habilitar o provisionamento automático de usuários durante o login do usuário. Quando o provisionamento automático de usuários está habilitado, um registro de usuário será criado automaticamente na instância ServiceNow se esse registro de usuário não existir.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Provisionar usando	A origem de dados a ser usada para transformar em um usuário ServiceNow. Estas são as opções: ◦ **Um token de ID** ◦ **Endpoint de informações do usuário** ◦ **Informações de usuário e token de ID** Use a lista de pesquisa para selecionar o modelo de origem de dados predefinido e abra o registro para configurar o mapeamento da tabela de transformações.
Provisionar origem de dados	A origem de dados do token de ID usada para o provisionamento de usuários.
Origem de dados de informações do usuário	A origem de dados do endpoint de informações do usuário usada para o provisionamento de usuários. Este campo é exibido somente quando **Informações do usuário** ou **Token de ID e informações do usuário** são selecionados no campo **Provisionar usando**.
Atualizar usuário no próximo login	Opção para habilitar atualizações do usuário durante o próximo login.
Atualizar tempo de intervalo do usuário (segundos)	Intervalo de tempo mínimo (em segundos) para atualizar o registro de usuário entre os logins subsequentes. Este campo é definido automaticamente para 3.600 segundos. Por exemplo, depois que um usuário faz login, o registro do usuário será atualizado após 3.600 segundos até o próximo login. Este campo está disponível somente quando o campo **Atualizar usuário no próximo login** está habilitado.
Funções de usuário aplicadas aos usuários provisionados	Lista de funções aplicadas aos usuários recém-provisionados.

5. Na guia **Entidade OIDC**, exiba e modifique a configuração do cliente OIDC e o fluxo de conexão OIDC usando o registro da entidade.
   Para obter mais informações relacionadas à configuração baseada em OIDC, consulte Como configurar um provedor de OAuth e OIDC para aceitar token de terceiros
6. Na guia **Configuração do provedor OIDC**, exiba e modifique o URL de configuração amplamente conhecido do IdP OIDC.
7. Opcional: Abra a guia **Avançado** e preencha os campos.

Guia Avançado

Propriedade	Descrição
Script de Single Sign-on	O script que é executado durante o Single Sign-On.
Script de logout	O script que é executado depois que o usuário faz logout.

Nota: Scripts são executados durante o Single Sign-on e o logout.

8. Para habilitar e testar a configuração, clique em **Ativar**.
9. Para atualizar o registro, clique em **Atualizar**.
   A opção de login baseado no Facebook é exibida no formulário de login.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

10. Ao fazer login no formulário de login, faça o seguinte:
    a. Selecione a opção Facebook.
    b. Para fazer login na instância ServiceNow, especifique suas credenciais Facebook.

Configuração de um Single Sign-on (SSO) baseado no Facebook

Configure um SSO baseado no Facebook para sua instância ServiceNow.

Antes de Iniciar

Tenha uma ID de cliente válida que esteja configurada como um IdP de Facebook.

Habilite as seguintes propriedades:

- Habilitar SSOs de vários provedores
- Habilitar registro em log de depuração para integrações de SSO de vários provedores.

Função necessária: administrador

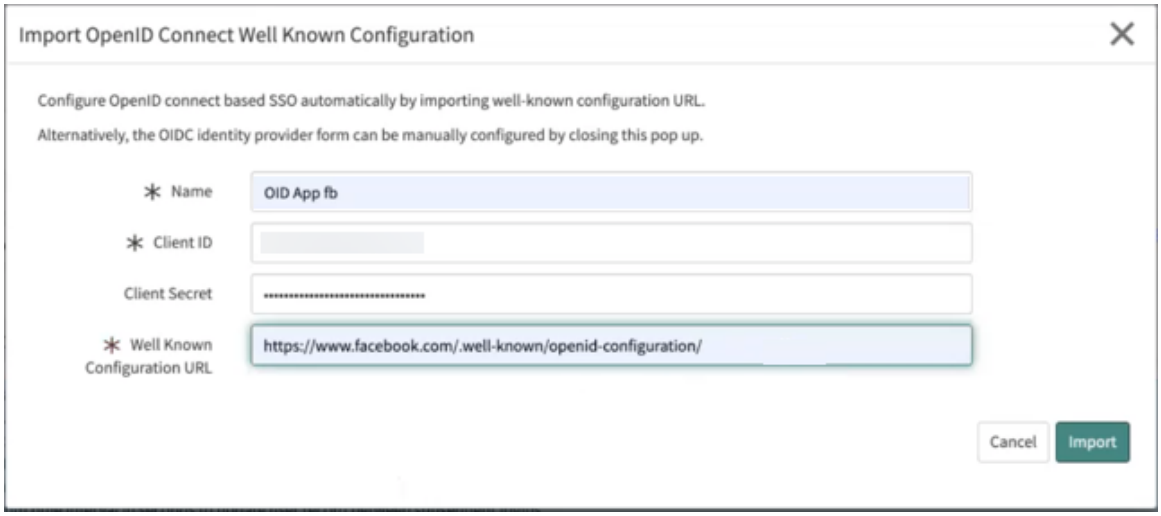
Procedimento

1. Navegue até **Todos** > **SSO de vários provedores** > **Provedores de identidade**.
2. Para criar um novo provedor de identidade Facebook, clique em **Novo**.
3. Clique em **OpenID Connect**.
4. No formulário, preencha os campos.

Importação do formulário de configuração conhecida da OpenID Connect

Campos	Descrição
Nome	Nome exclusivo para a configuração do provedor de identidade OIDC.
ID de cliente	A ID de cliente da aplicação registrada no provedor de identidade OIDC de terceiros.
Segredo do cliente	O segredo do cliente da aplicação registrado no provedor de identidade OIDC de terceiros.
URL de configuração amplamente conhecido	O URL que contém metadados sobre o provedor de identidade OIDC de terceiros.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

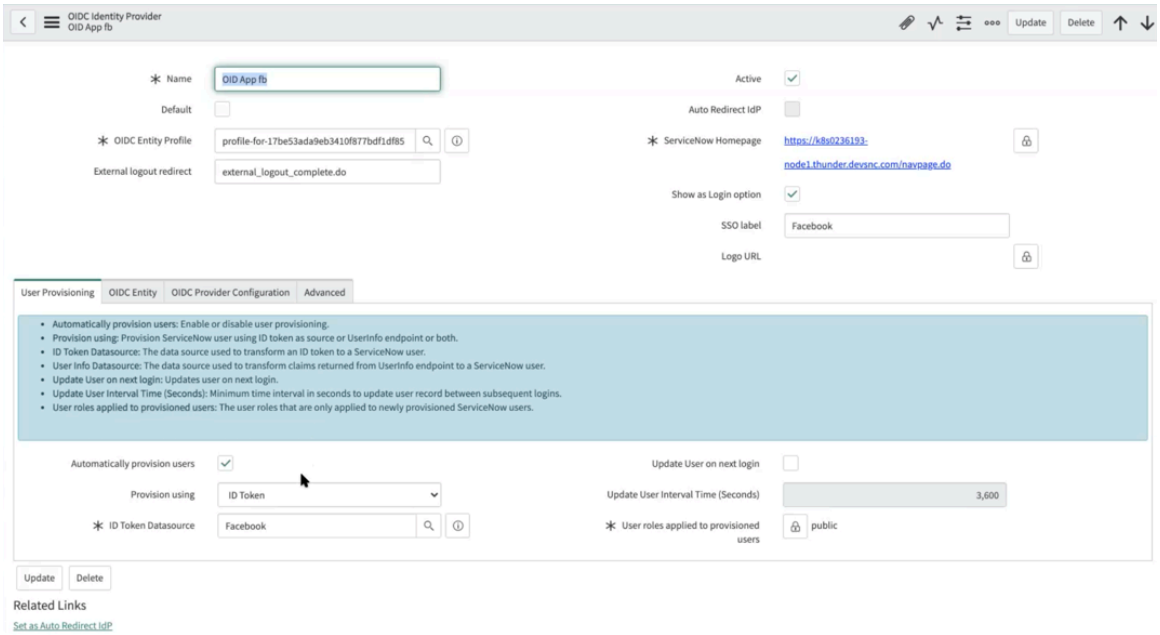


5. Clique em **Importar**.
   O IdP baseado no Facebook foi criado.

6. Selecione o IdP Facebook.
7. No IdP Facebook, faça o seguinte:
   a. Valide todos os campos, como **Nome**, **Perfil de entidade de OIDC**, **Redirecionamento de logout externo**e **Página inicial da ServiceNow**.
   b. Forneça seu **rótulo de SSO**.
8. Na guia **Provisionamento de usuário**, especifique os campos de que você precisa para configurar o provisionamento de usuário e funções específicas.

   Somente os campos obrigatórios são obrigatórios. É possível especificar os campos restantes, dependendo do que você precisa.

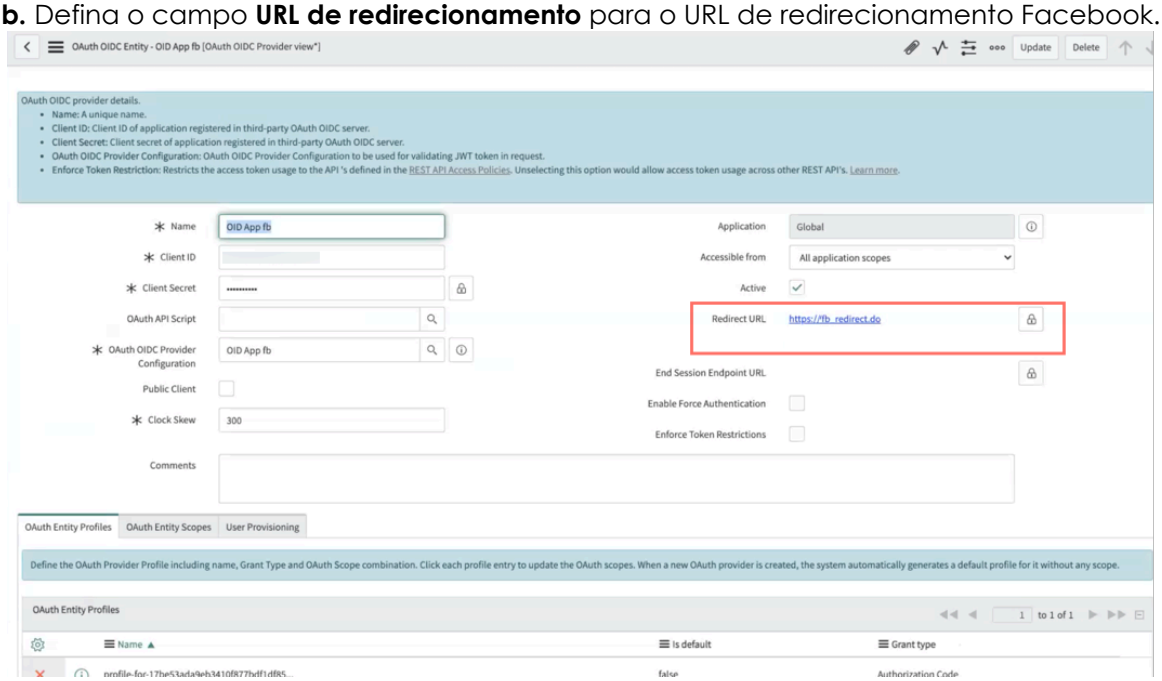
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



9. Na guia **Entidade OIDC**, faça o seguinte:

   a. Clique na entidade.

   b. Defina o campo **URL de redirecionamento** para o URL de redirecionamento Facebook.

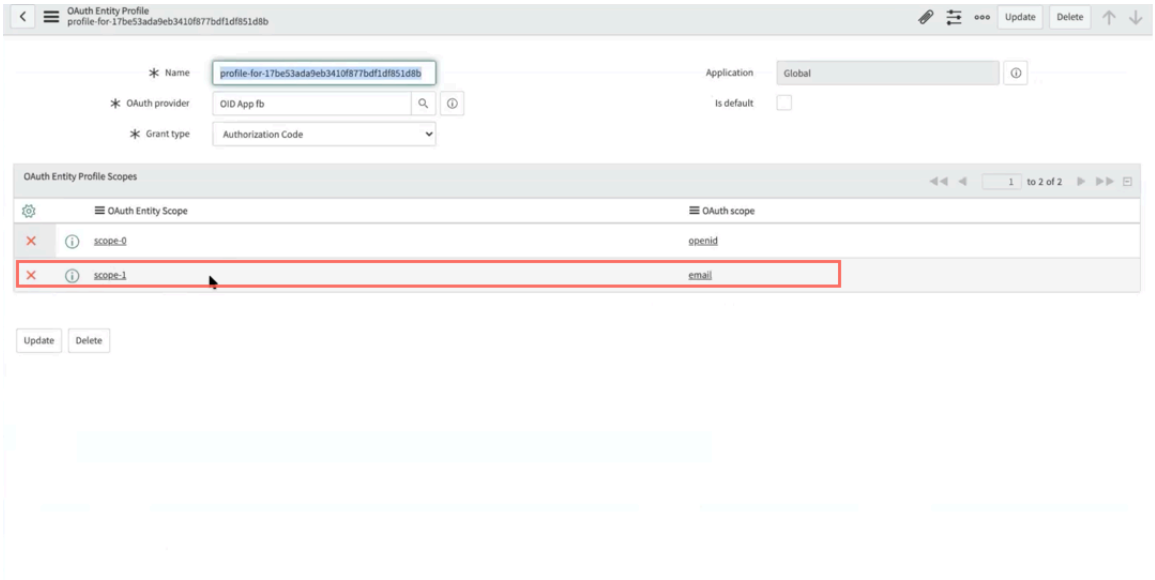


10. Na guia **Perfis de entidade OAuth**, faça o seguinte:

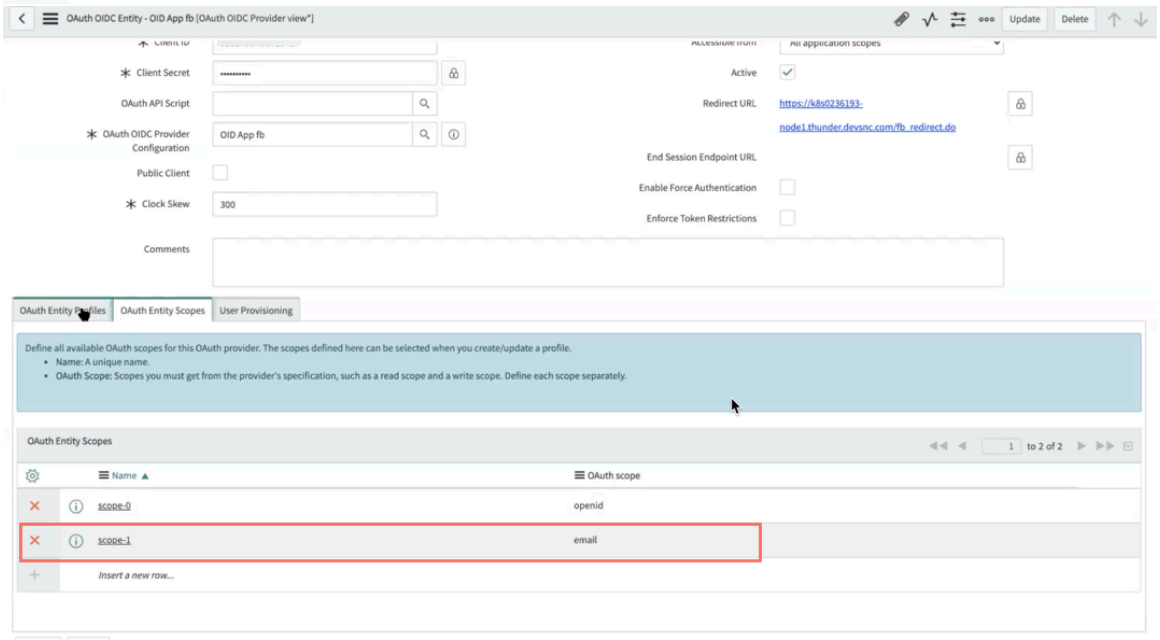
    a. Nos detalhes de perfil, clique em um perfil.

    b. Selecione um escopo e verifique os detalhes.
    Por exemplo, selecione **scope-1**

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



11. Na guia **Escopos da entidade OAuth**, clique no link **scope-1** e adicione o escopo como `e-mail`.

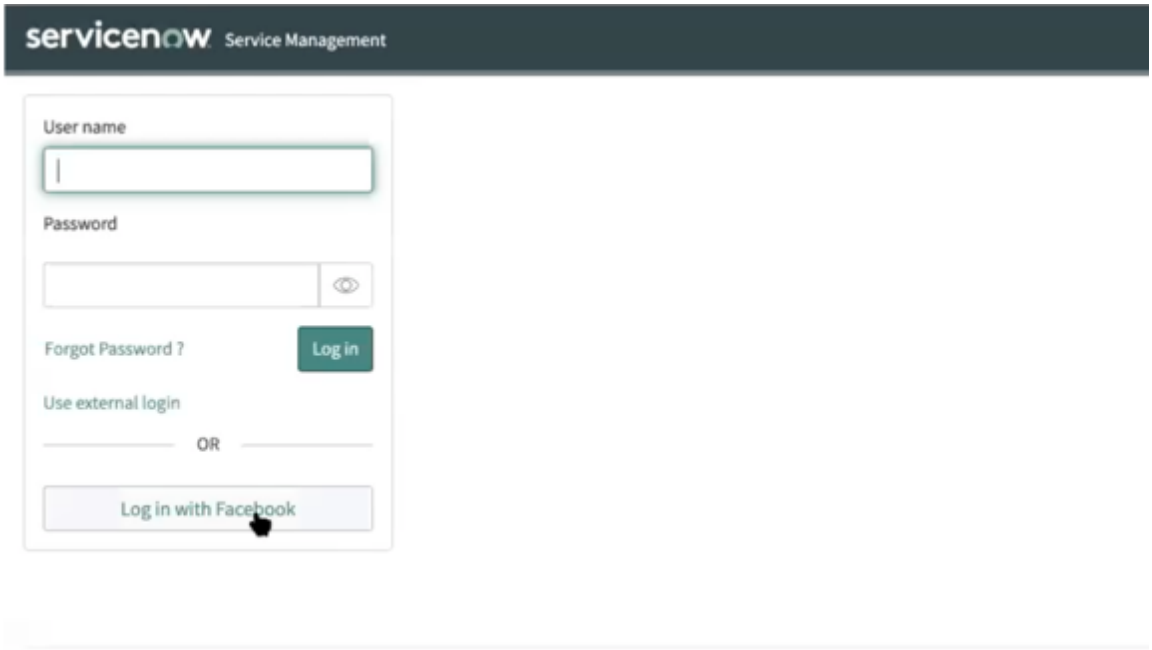


12. Para salvar a configuração, clique com o botão direito do mouse no cabeçalho e clique em **Salvar**.
13. Para definir a configuração como ativa, selecione **Ativo**.

Resultados

Os usuários são exibidos com a opção SSO Facebook no formulário de login.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



SAML

A Linguagem de marcação de segurança (Security Assertion Markup Language, SAML) é um padrão baseado em XML para a troca de dados de autenticação e autorização entre domínios de segurança.

O SAML troca informações de segurança entre um provedor de identidade (um produtor de asserções) e um provedor de serviço (um consumidor de asserções). SAML é um produto do Comitê Técnico de Serviços de Segurança OASIS. Quando implementado corretamente, o SAML é um dos métodos mais seguros de Single Sign-on (SSO) disponíveis.

A integração do SAML 2.0 permite o SSO trocando tokens XML com um Provedor de identidade (IdP) externo. O IdP autentica o usuário e passa um token NameID para o sistema. Se o sistema encontrar um usuário com um token NameID correspondente (por exemplo, o endereço de e-mail), a instância fará login nesse usuário.

Se você estiver usando o plug-in SAML 2.0 para autenticação SSO, deverá definir a propriedade "glide.ui.rotate_sessions" como "falsa". Caso contrário, ele interferirá no compartilhamento de informações da sessão que ocorre entre a instância e o Provedor de identidade. Usuários com o privilégio elevado "security_admin" podem acessar essa propriedade.

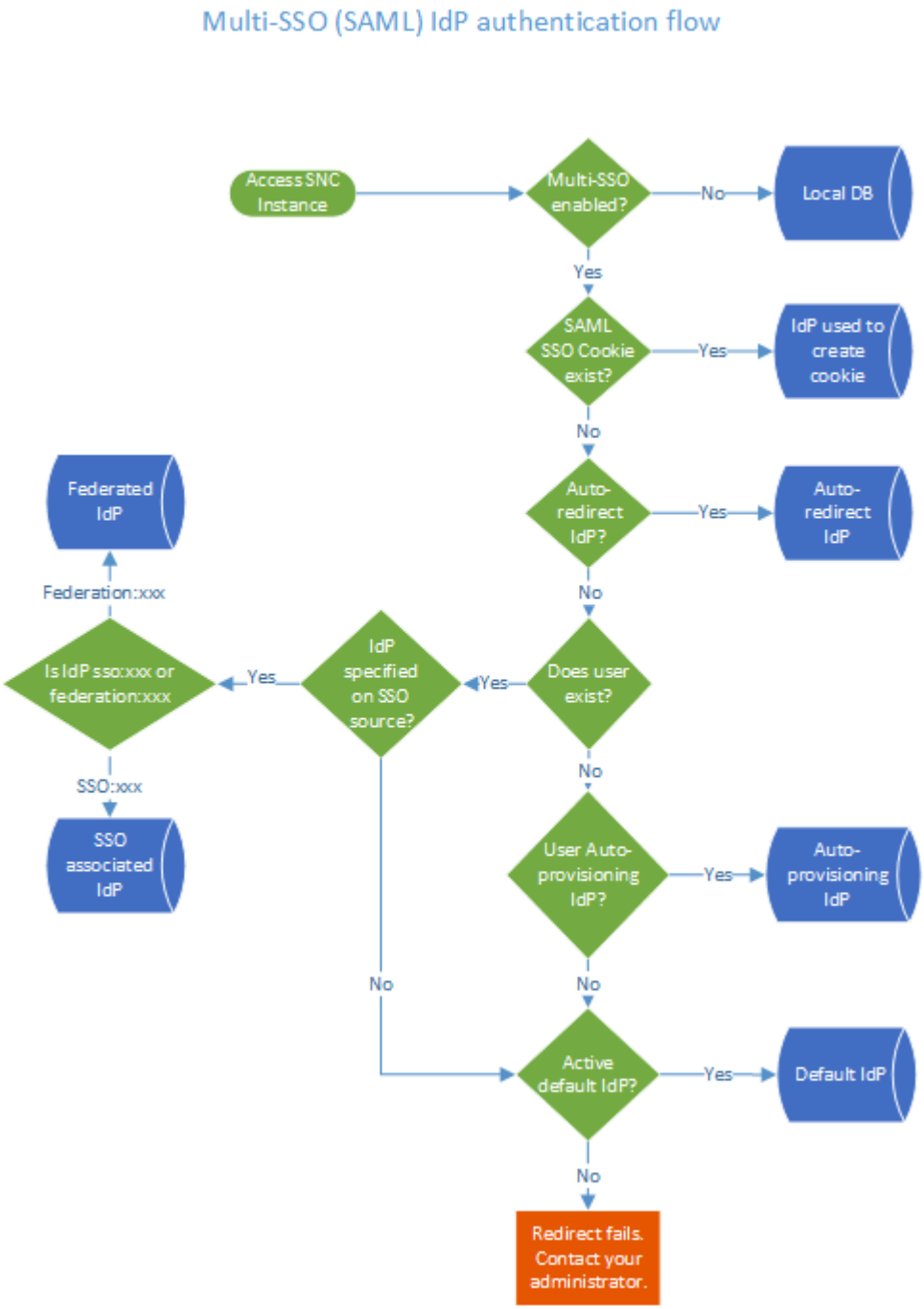
Nota: É recomendável que os clientes que usam uma integração SAML 2.0 existente atualizem para o plug-in Multi-Provider SSO.

Fluxo de autenticação de IdP SSO (SAML) de vários provedores

Descreve as diferentes entidades com permissão para autenticar um usuário por meio do Multi-SSO do SAML.

É possível seguir o fluxo de autenticação para entender quando uma entidade autentica um usuário usando o Multi-SSO.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Banco de dados local

Se o Multi-SSO não estiver habilitado, a autenticação será direcionada para um banco de dados local.

IdP do Cookie SSO do SAML

Se houver um cookie de SSO do SAML, o IdP especificado com o cookie autenticará o usuário.

IdP de redirecionamento automático

Se o IdP de redirecionamento automático estiver habilitado, ele autenticará o usuário.

IdP federado

Se o navegador do usuário for redirecionado para a tela de login de autorização externa (login_locate_sso.do) e o usuário existir na tabela do

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

usuário com o IdP definido no campo **Fonte do SSO** como federation: xxx, o IdP federado autenticará o usuário.

IdP associado

Se o navegador do usuário for redirecionado para a tela de login de autorização externa (login_locate_sso.do) e o usuário existir na tabela do usuário com o IdP definido no campo **Fonte do SSO** como sso: xxx, o IdP associado autenticará o usuário.

Provisionamento automático de IdP

Se o navegador do usuário for redirecionado para a tela de login de autorização externa (login_locate_sso.do) e o usuário não existir na tabela Usuário, mas o provisionamento automático estiver ativado, o provisionamento automático de IdP autenticará o usuário.

Nota: Se mais de um provisionamento automático de IdP estiver habilitado, o usuário poderá escolher aquele que deseja usar.

IdP padrão

Se o navegador do usuário for redirecionado para a tela de login de autorização externa (login_locate_sso.do) e o usuário:

- Não existir na tabela Usuário, o provisionamento automático não estará habilitado e um IdP padrão estará ativo
- Existir na tabela Usuário, um IdP não estará especificado no usuário de fonte do SSO ou no registro da empresa e um IdP padrão estará ativo

então, o IdP padrão autenticará o usuário.

Propriedades do sistema do Provedor de identidade (IdP)

Um IdP geralmente oferece um documento XML que contém metadados de autenticação e logout.

Por exemplo, o SSOCircle publica os metadados online.

Pesquise os metadados do IdP para encontrar estas entradas:

- O elemento `SingleSignOnService` com um atributo `Binding` que contém um valor `Redirecionamento HTTP`. O atributo `Location` lista o URL que a integração requer para o serviço "AuthnRequest".
- O elemento `SingleLogoutService` com um atributo `Binding` que contém um valor de `Redirecionamento HTTP`. O atributo `Location` lista o URL que a integração requer para o serviço "SingleLogoutRequest".

Nota: A integração de SAML 2.0 só oferece suporte à vinculação a serviços IdP por Redirecionamento HTTP.

Por exemplo:

```
<SingleSignOnServiceBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"Location="https://
idp.ssocircle.com:443/sso/SSORedirect/metaAlias/ssocircle"/>
```

```
<SingleLogoutServiceBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"Location="https://
idp.ssocircle.com:443/sso/IDPSloRedirect/metaAlias/ssocircle"ResponseLoca
```

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

```
tion="https://
idp.ssocircle.com:443/sso/IDPSloRedirect/metaAlias/ssocircle"/>
```

Como definir o URL do emissor do IdP

Forneça o URL para os IdPs que emitirão o token de segurança.

Antes de Iniciar
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa
A integração verifica se cada resposta SAML contém o mesmo URL listado nessa propriedade do sistema que o URL listado no elemento *Issuer*. Por exemplo:

```
<samlp:Responsexmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
  Destination="https://demoi2.service-now.com/navpage.do"
  ID="s28da6774c88ae1eab292bf25fe625db81919d8e1e"
 InResponseTo="SNC841720c227c81948cfd68cadcad235c6"
 IssueInstant="2012-01-30T20:07:10Z"  Version="2.0"><saml:Issuer
 xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">http://
idp.ssocircle.com</saml:Issuer>
   ...
   <saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
     ID="s2f347f973c063836cf70ea38302d94976f9c5b851"
     IssueInstant="2012-01-30T20:07:10Z"
 Version="2.0"><saml:Issuer>http://idp.ssocircle.com</saml:Issuer>
      ...
   </saml:Assertion></samlp:Response>
```

Procedimento

1. Navegue até **Todos** > **SAML 2 Single Sign-on** > **Propriedades**.
2. Na propriedade *O URL Provedor de identidade que irá emitir o token de segurança SAML2 com a informação do usuário*, insira o URL de sua IdP.

   Cada URL de IdP deve ser exclusivo. Por padrão, a integração contém o URL para SSOCircle. Para obter mais informações, consulte http://idp.ssocircle.com.

Como definir o URL do serviço AuthnRequest

Usando os metadados do IdP, defina as URLs de serviço de solicitação para o IdP da integração.

Antes de Iniciar
Função necessária: administrador

Procedimento

1. Na propriedade *O URL base para o serviço AuthnRequest do Provedor de identidade. A AuthnRequest será publicada nesse URL como o parâmetro SAMLRequest*, insira o URL para a vinculação Redirecionamento HTTP obtida do elemento `SingleSignOnService`.
2. Marque a caixa de seleção próxima ao *Assinar AuthnRequest* para habilitar o serviço de logon único do Provedor de identidade para receber um AuthnRequest assinado.
3. Na propriedade *Quando o logon único do SAML 2.0 falhar porque a sessão não foi autenticada ou este é o primeiro login, redirecione para este URL. Esse é o URL base pelo qual o AuthnRequest do SAML 2.0 será enviado por meio do parâmetro*

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

SAMLRequest, insira o URL para a vinculação Redirecionamento HTTP obtida do elemento `SingleSignOnService`.

Por padrão, a integração contém o URL para o serviço "SSOCircle".

Como definir o URL do serviço SingleLogoutRequest

Usando os metadados do IdP, defina URLs de serviço de solicitação para o IdP da integração.

Antes de Iniciar
Função necessária: administrador

Procedimento

1. Na propriedade *O URL base para o serviço SingleLogoutRequest do Provedor de identidade. O LogoutRequest será publicado nesse URL como o parâmetro SAMLRequest*; insira o URL obtido do elemento `SingleLogoutService`.
   O "LogoutRequest" será publicado nesse URL como o parâmetro "SAMLRequest". Por padrão, a integração contém o URL para o serviço "SSOCircle".
2. Na propriedade *URL para redirecionar usuários após o logout, normalmente de volta ao portal que habilitou o SSO (por exemplo, http://portal.companya.com/logout)*, insira o URL para o qual você deseja redirecionar os usuários após o logout bem-sucedido.

   Se o seu IdP usa autenticação baseada em formulário, insira o URL do formulário de login do IdP. Se o seu IdP usa um método de autenticação não baseado em formulário, como o Kerberos, você deve definir o URL como uma página de logout estática. Dessa forma, os usuários que fazem logout não serão redirecionados imediatamente para o IdP e poderão fazer login novamente. Por padrão, a integração contém o URL para a página de IU estática `external_logout_complete.do`.

(Opcional) Como habilitar solicitações de logout assinadas

Alguns IdPs exigem que o Provedor de serviço assine as solicitações de logout com um certificado.

Antes de Iniciar
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa
Se o seu IdP requer solicitações de logout assinadas, use os metadados do IdP para definir as seguintes propriedades do sistema.

Procedimento

1. Na guia **Avançado**, na propriedade *Assinar LogoutRequest. Defina esta propriedade como verdadeira se o serviço "SingleLogoutRequest" do Provedor de identidade solicitar a LogoutRequest assinada*, selecione **Sim** para especificar que seu IdP exige solicitação de logout assinada ou **Não** para utilizar solicitações de logout não assinadas.
2. Se você selecionou **Sim** para *Assinar LogoutRequest*, na propriedade *A vinculação de protocolo para o serviço "SingleLogoutRequest" do Provedor de identidade. (O valor pode ser "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" ou "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST".)*, insira um dos valores compatíveis listados no atributo `Binding` do elemento `SingleLogoutService`.

   Por padrão, a integração usa uma vinculação "Redirecionamento HTTP".

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Clique em **Atualizar**.
4. Instale um armazenamento de chaves do Provedor de serviço (SP).

Propriedades do sistema do Provedor de serviço (SP)

Essas propriedades do sistema definem como a instância interage com o IdP como um Provedor de serviços.

Siga o processo sequencial para definir o IdP como Provedor de serviço.

Definição do URL da instância para SAML

Defina os URLs específicos da instância para que o IdP possa autenticar os usuários.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Na propriedade *O URL para a instância do Service-now (geralmente esta instância)*, insira o URL (incluindo a página de login) da instância para a qual o IdP será autenticado.
   Por exemplo: https://yourinstance.service-now.com/navpage.do
2. Na propriedade *A identificação da entidade ou o emissor*, insira o URL base (excluindo a página de login) da instância para a qual o IdP fará a autenticação.
   Por exemplo: https://yourinstance.service-now.com/

Definição do URL do público-alvo para SAML

Usando a propriedade "Público", habilite sua instância para verificar se esse é o destinatário pretendido de uma resposta SAML.

Antes de Iniciar

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

A integração verifica se cada resposta SAML contém o mesmo URL listado nessa propriedade do sistema que o URL listado no elemento *Audience*. Por exemplo:

```
<samlp:Responsexmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
  ID="s2cdc74f37f923e26fe1aeec42b70a93d24230334f"
  InResponseTo="90AA6073F01567BFB0DF194F596314E2"
 Version="2.0"  IssueInstant="2010-04-29T23:21:51Z"
 Destination="https://dloomac.service-now.com/navpage.do">
...
<saml:Conditions NotBefore="2012-01-30T19:57:10Z"
 NotOnOrAfter="2012-01-30T20:17:10Z"><saml:AudienceRestriction><saml:Audi
ence>https://
demoi2.service-now.com</saml:Audience></saml:AudienceRestriction></saml:C
onditions>
...
</samlp:Response>
```

Procedimento

1. Navegue até **Todos** > **SAML 2 Single Sign-on** > **Propriedades**.
2. Na propriedade *O URI do público-alvo que aceita o token SAML2. (Normalmente, é o URI da sua instância. Por exemplo: https://<instance name>.service-now.com.)*, insira o URL da sua instância.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por exemplo, https://demoi2.service-now.com. Este URL deve corresponder ao valor do elemento *Audience* na resposta SAML.

3. Clique em **Atualizar**.

Configuração de uma política NameID para SAML

Configure uma política NameID para SAML. O SAML 2.0 requer que o IdP troque um token NameID com o provedor de serviços.

Antes de Iniciar
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa
Para a integração do SAML 2.0, o token NameID deve ser mapeado para um campo específico na tabela "Usuário". A integração usa o valor do token NameID para determinar qual usuário o IdP autentica.

Procedimento

1. Pesquise os metadados do IdP para encontrar o elemento `NameIDFormat` que contém um valor de `emailAddress`.
   O valor desse elemento é o formato padrão que a integração utiliza.
2. Analise outros elementos `NameIDFormat` para determinar se há formatos que correspondem a outros campos na tabela Usuário.

Como determinar qual campo da tabela Usuário corresponde ao token NameID

Os provedores de identidade especificam o formato do token `NameID`.

Antes de Iniciar
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa
A configuração do SAML 2.0 requer a seleção de um campo na tabela Usuário que corresponda ao formato do token `NameID`. Normalmente, os IdPs oferecem a opção de usar um endereço de e-mail como token `NameID`. Como a tabela Usuário contém um campo de e-mail, esse campo é uma opção lógica para uso como um token `NameID`. Para usar outro campo dessa tabela como token `NameID`, primeiro verifique se o IdP oferece um formato `NameID` que corresponda ao valor de um campo da tabela Usuário. Isso pode exigir a adição do campo à tabela.

Procedimento

1. Compare os formatos disponíveis no elemento `NameIDFormat` do IdP com os campos da tabela Usuário.
2. Selecione um formato `NameID` em que haja um valor correspondente na tabela Usuário.
3. No campo *O campo da tabela Usuário que deve corresponder ao elemento NameID do Assunto em SAMLResponse*, insira o nome do campo da tabela Usuário para pesquisar valores correspondentes no token `NameID`.

   Por padrão, a integração usa o campo de e-mail.

Como definir a política do IdP NameID

Especifique qual formato o IdP usa para o token `NameID`.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa
Este formato está listado como parte dos metadados do IdP.

Procedimento
1. Na propriedade *A política NameID a ser usada para retornar o NameID do Assunto no SAMLResponse. Seu provedor de identidade SAML deve oferecer suporte a isso declarando a política em seus metadados. O valor NameID será usado para fazer uma correspondência com o campo especificado na tabela Usuário para pesquisar o usuário.*, insira o valor do elemento `NameIDFormat` que a integração usa.

   Por padrão, a integração usa o SSOCircle `NameIDFormat` para endereços de e-mail.

2. Clique em **Salvar**.

Valores no campo da tabela Usuário para SAML
Certifique-se de que o campo da tabela Usuário da integração contenha valores correspondentes apropriados.

Por exemplo, se a integração usar o campo de e-mail como o token `NameID`, certifique-se de que a instância liste o mesmo endereço de e-mail que o IdP. A integração falha ao autenticar qualquer usuário que não tenha um valor correspondente para o token `NameID`.

(Opcional) Como habilitar o fornecimento de uma classe de contexto de autenticação para SAML
Você pode habilitar a instância para enviar uma solicitação de classe de contexto de autenticação ao IdP que contém o formato de solicitação de autenticação preferencial da sua instância.

Antes de Iniciar
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa
Se habilitar a criação de uma mensagem AuthContextClass, você também deverá especificar um formato de referência de classe de contexto de autenticação.

Nota: Alguns IdPs não permitem que o Provedor de serviços defina a classe de contexto de autenticação. Desabilitar esta configuração permite que o IdP escolha a classe de contexto de autenticação.

Procedimento
1. Na propriedade *Criar uma solicitação AuthnContextClass na declaração AuthnRequest*, selecione **Sim** para especificar uma classe de contexto específica, como Transporte protegido por senha ou **Não** para que o IdP selecione a classe de contexto mais apropriada.
2. Se você selecionou **Sim** em *Criar uma solicitação AuthnContextClass na declaração AuthnRequest*, na propriedade *O método AuthnContextClassRef que solicitaremos em nosso SAML 2.0 AuthnRequest para o Provedor de identidade* insira o URN da classe de contexto que você deseja usar para autenticação (consulte a tabela).

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opções de URN de AuthnContextClass

Tipo de autenticação	Classe de contexto de autenticação URN
Autenticação baseada em formulários	`urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport`
Autenticação baseada em Kerberos	`urn:federation:authentication:windows`

Por padrão, a integração usa um método de autenticação de Transporte protegido por senha.

3. Clique em **Atualizar**.

(Opcional) Como definir propriedades de armazenamento de chaves para assinar solicitações de logout para SAML

Defina as propriedades do armazenamento de chaves para habilitar a integração a fim de assinar solicitações de logout usando o servidor assinado e os certificados de CA assinados.

Antes de Iniciar
Função necessária: admin

Procedimento

1. Na propriedade *O alias da entrada de chave armazenada no armazenamento de chaves SAML 2.0 SP usado para assinar solicitações SAML 2*, insira o nome do alias que você criou para o armazenamento de chaves SAML 2.0.
   Por padrão, a integração procura o alias *saml2sp*.
2. Na propriedade *A senha da chave de entrada armazenada no armazenamento de chaves SAML 2.0 SP usado para assinar solicitações SAML 2*, insira a senha para o seu armazenamento de chaves SAML 2.0.
   Por padrão, a senha é igual ao nome do alias padrão.
3. Clique em **Atualizar**.
4. Gere novamente seus metadados de SP.
   Para obter mais informações, consulte Metadados de SP.

Como criar um armazenamento de chaves de provedor de serviços para SAML

Crie um armazenamento de chaves Java que contenha os seguintes itens para que sua instância assine solicitações de logout.

Antes de Iniciar
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

- Certificado do servidor assinado para a instância
- Certificado CA assinado
- Par de chaves públicas e privadas

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você pode criar seu próprio certificado assinado com uma autoridade de certificação privada ou comprar um de uma autoridade de certificação pública.

As etapas a seguir ilustram como gerar um novo arquivo de armazenamento de chaves Java Keytool, criar uma solicitação de assinatura de certificado (CSR) e importar certificados. Quaisquer certificados raiz ou intermediários precisam ser importados antes da importação do certificado primário para o seu domínio. Digite esses comandos em uma interface de linha de comando.

Nota: Essas instruções não são específicas para a plataforma e exigem conhecimento técnico de certificados de segurança para serem concluídas. O suporte técnico não consegue ajudar na criação dos certificados.

Procedimento

1. Gere um armazenamento de chaves Java e um par de chaves.

```
keytool -genkey -alias mydomain -keyalg RSA -keystore my.keystore
```

2. Gere um CSR para um armazenamento de chaves Java existente.

```
keytool -certreq -alias mydomain -keystore my.keystore -file
 mydomain.csr
```

3. Importe um certificado CA de autoridade de certificação raiz ou intermediária para um armazenamento de chaves Java existente.

```
keytool -import -trustcacerts -alias root -file Thawte.crt -keystore
 my.keystore
```

4. Importe um certificado primário assinado para um armazenamento de chaves Java existente.

```
keytool -import -trustcacerts -alias mydomain -file mydomain.crt
 -keystore my.keystore
```

Como instalar um armazenamento de chaves do provedor de serviços para assinar solicitações SAML

Use as etapas a seguir para remover o armazenamento de chaves de exemplo existente e instalar seu próprio armazenamento de chaves de provedor de serviços que contenha seu par de chaves pública e privada.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Crie um armazenamento de chaves de provedor de serviços.
2. Navegue até **SAML 2 Single Sign-on** > **Certificado** ou **Multiprovedor** > **Administrador** > **Certificado x509**.
3. Clique em **SAML 2.0 Keystore_Key2048_SHA256**.
4. Clique no link **Gerenciar anexos**.
5. Clique em "Excluir" ao lado de *saml2sp_key2048withsha256.jks*.
6. Clique em **Remover**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

7. Clique em **Escolher arquivos** e selecione o armazenamento de chaves que contém seus certificados assinados.
8. Clique em **Anexar**.
9. Feche a pop-up de Anexos.

> **Nota:** É recomendável fornecer um nome diferente para o certificado recém-anexado.

10. Em *Senha do armazenamento de chaves*, insira a senha para acessar o alias do SAML 2.
11. Clique em **Atualizar**.

(Opcional) Propriedades avançadas de SAML

As configurações avançadas a seguir permitem aumentar ainda mais a segurança e depuram a integração.

Configurações avançadas

Navegue até **Todos** > **SAML 2 Single Sign-on** > **Propriedades**.

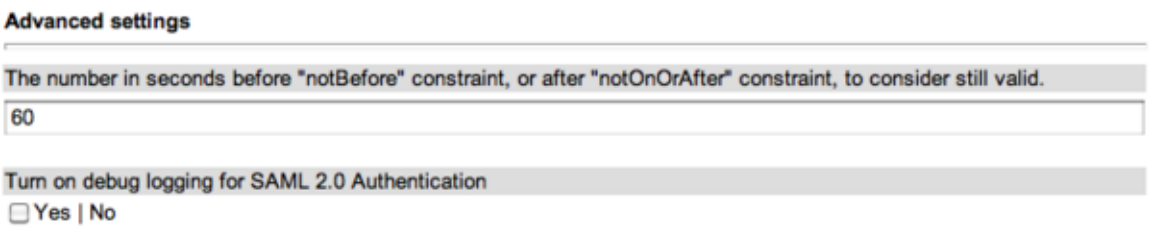


Tabela de propriedades do sistema avançadas

Propriedade	Descrição
O número em segundos da restrição "notBefore", ou depois da restrição "notOnOrAfter", para ainda ser considerado válido.	Insira o número de segundos para adicionar às restrições *NotBefore* e *NotOnOrAfter* para contabilizar as diferenças de tempo entre o relógio do IdP e o relógio do SP. Essas restrições impedem ataques de repetição ao negar solicitações que não sejam feitas dentro do intervalo de tempo especificado. Se o relógio do IdP e o relógio do SP forem significativamente diferentes, a latência da rede poderá fazer com que a solicitação SAML seja não autorizada. Essa propriedade adiciona um período de carência durante o qual as solicitações e respostas SAML ainda são consideradas válidas.
Ativar log de depuração para a Autenticação SAML 2.0	Selecione **Sim** para habilitar informações de registro em log adicionais para eventos SAML 2.0.

Como instalar o certificado de provedor de identidade

Você pode colar um certificado PEM em um formulário de certificado X.509 para que o provedor de identificação possa verificar as comunicações com o provedor de serviços.

Antes de Iniciar

Função necessária: administrador

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

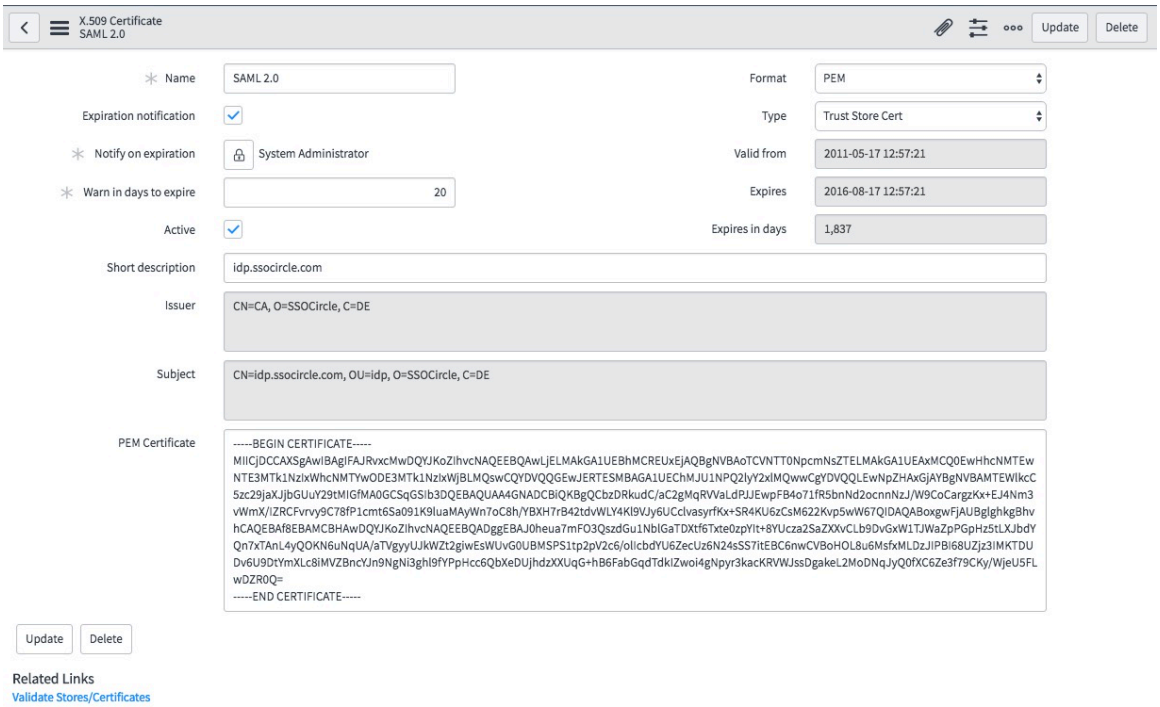
Por Que e Quando Desempenhar Esta Tarefa

O certificado do IdP está localizado nos metadados do IdP. O desenvolvedor IdP determina onde os metadados do certificado residem ao criar o IdP local.

Nota: Os certificados de logon único devem estar sempre no formato PEM para funcionar com certificados SAML.

Procedimento

1. Navegue até **Todos** > **SAML Single Sign-on** > **Certificado**.
2. Preencha os campos de formulário (consultar tabela).
3. Clique em **Salvar**.



Nota: A integração não assina atualmente o certificado nas comunicações entre a instância e o IdP.

Campo	Descrição
Nome	O nome do certificado. Não mude a entrada *Nome*. Para que a integração possa usá-lo, o nome do certificado X.509 deve ser *SAML 2.0*. Esse requisito apenas será verdadeiro se você não estiver usando Single Sign-on (SSO) de vários provedores.
Notificação de expiração	Selecione essa opção para enviar uma notificação aos usuários selecionados no campo **Notificar na expiração**. Por padrão, essa opção está ativada.
Notificar no vencimento	Selecione os usuários para reativar a notificação sobre a expiração do certificado. Se nenhum usuário for selecionado, o usuário conectado será adicionado por padrão, juntamente com os dois últimos usuários conectados com a função de administrador.
Aviso emitido	O número de dias antes da expiração em que a instância envia a notificação. Insira um valor de pelo menos 20. As instâncias atualizadas

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
antes do vencimento (em dias)	para a versão Istanbul e posteriores têm esse valor definido como 20, a menos que um valor maior seja especificado.
Ativo	Uma caixa de seleção indicando que este certificado está ativo.
Formato	O formato do certificado. SAML usa o formato PEM.
Tipo	O contêiner do certificado. A instância reconhece os certificados dos armazenamentos de confiança, armazenamento de chaves Java e armazenamentos de chave PKCS#12.
Válido de	A instância adiciona a data de início da validade do certificado a esse campo automaticamente. Anexe o certificado ao registro do certificado X.509 para preencher este campo.
Expira	A instância adiciona automaticamente a esse campo a data de expiração do certificado. Anexe o certificado ao registro do certificado X.509 para preencher este campo.
Dias até o vencimento	O número calculado de dias até o vencimento.
Descrição resumida	Uma descrição para o certificado.
Problema	A instância adiciona automaticamente a esse campo o emissor do certificado. Anexe o certificado ao registro do certificado X.509 para preencher este campo.
Assunto	A instância adiciona automaticamente a esse campo o assunto do certificado. Anexe o certificado ao registro do certificado X.509 para preencher este campo.
Certificado PEM	Insira o valor do certificado X509.

O que Fazer Depois

Clique em **Validar armazenamentos/certificados** para testar a confiabilidade do armazenamento e do certificado.

Como substituir um certificado ausente para SAML

Se o módulo **Certificado** exibir uma página em branco, o registro do certificado SAML 2.0 foi excluído. Você pode substituir o certificado ausente criando manualmente um registro de certificado.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Navegue até **Todos** > **Definição do sistema** > **Certificados**.
2. Crie um novo registro chamado `SAML 2.0`.

> **Importante:** O uso desse nome é OBRIGATÓRIO. Esse requisito apenas será verdadeiro se você não estiver usando Single Sign-on (SSO) de vários provedores.

3. Clique em **SAML 2 Single Sign-on** > **Certificado**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. No campo *Certificado PEM*, insira o valor do elemento `ds:X509Certificate` dos metadados do seu IdP.
5. Clique em **Salvar**.

Teste a integração do SAML

Teste a integração do SAML depois de concluir todas as outras tarefas de configuração.

Antes de Iniciar
Função necessária: administrador

Procedimento

1. Faça login na instância como um usuário com a função de administrador.
2. Navegue até **SAML 2 Single Sign-on** > **Propriedades**.
3. Na propriedade *Habilitar autenticação externa*, selecione **Sim**.

> **Nota:**
>
> A habilitação da autenticação externa requer que todos os usuários usem o logon único do SAML 2.0. Se alguém tentar acessar a aplicação em um estado não autenticado, a instância enviará automaticamente uma solicitação de autenticação para o IdP e redirecionará o usuário para a página Autenticação do IdP do SAML.

4. Clique em **Salvar**.
5. Faça logout da instância.
6. Navegue até o URL da instância.
   Se a integração estiver funcionando corretamente, o IdP deverá solicitar as credenciais do usuário.

Informações relacionadas

Correções e erros de Multi-SSO (SAML 2.0)

Correções e erros de Multi-SSO (SAML 2.0)

Uma lista de erros comuns e correções associadas para uma instalação e configuração de Multi-SSO (SAML 2.0).

Erros durante a configuração de Multi-SSO (SAML 2.0)

Erro nos logs de instância	Mensagem do Testar conexão	Propriedade SAML	Diagnóstico	Correção
NotAfter: <Thu Jun 05 22:57:44 PDT 2014>.	Certifique-se de que o certificado x509 do IDP esteja presente, válido e ativo.	N/D	O certificado atual ou a declaração SAML expirou.	• Sincronize o relógio do SNC com o relógio do servidor IdP do SAML. • Atualize o registro do certificado SAML 2.0.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Erros durante a configuração de Multi-SSO (SAML 2.0)

Erro nos logs de instância	Mensagem do Testar conexão	Propriedade SAML	Diagnóstico	Correção
• Impossível localizar o certificado SAML 2.0. • Não foi possível encontrar uma assinatura digital armazenada na instância da ServiceNow.	Certifique-se de que o certificado x509 do IDP esteja presente, válido e ativo	A cadeia de caracteres no formato PEM deve ser inserida no campo "Certificado PEM".	O certificado SAML não existe. Ele pode estar inativo.	Certifique-se de que o certificado no formato PEM correto seja carregado para a instância.
Os certificados não coincidem. Esperado: <certStr>, vigente: <inboundCert>.	Certifique-se de que o certificado x509 do IDP esteja presente, válido e ativo.	N/D	O certificado disponível no SNC não corresponde ao certificado na declaração. As causas incluem: • O certificado é atualizado no IdP, mas não na instância da ServiceNow. • O certificado está no formato incorreto.	Confirme se a cadeia de caracteres no formato PEM no registro do certificado SAML 2.0 corresponde ao Certificado X509 no SAMLResponse do IdP do usuário.
Falha ao verificar a validade do certificado.	Certifique-se de que o certificado x509 do IDP esteja presente, válido e ativo	N/D	O certificado atual pode ter expirado.	Atualize o registro do certificado SAML 2.0.
Falha ao validar o perfil de assinatura.	Certifique-se de que o certificado x509 do IDP esteja presente, válido e ativo.	N/D	A declaração pode ter sido assinada com um certificado diferente.	Verifique se o IdP tem o mesmo certificado que a instância do SNC.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Erros durante a configuração de Multi-SSO (SAML 2.0)

Erro nos logs de instância	Mensagem do Testar conexão	Propriedade SAML	Diagnóstico	Correção
Incompatibilidade do atributo "InResponseTo" no "SubjectConfirmationData". Esperado: <inResponseTo>, vigente: <inResponseTo>.	Falha na validação da confirmação do assunto.	N/D	Este erro aparecerá se ocorrer uma das seguintes situações: • O IdP retorna um SAMLResponse para um SAMLRequest diferente • Um usuário marca como favorito o URL com o SAMLRequest em vez de apenas o URL da instância • Se um valor nulo for esperado, a resposta poderá ser enviada para um nó diferente quando a instância tiver vários nós.	O administrador do IdP deve confirmar que o SAMLReponse esperado está sendo retornado. Esta situação pode ser um balanceador de carga ou problema de infraestrutura.
Valor da "SessionIndex" não encontrado: <message>...	"SessionIndex" não é válido.	N/D	O "SessionIndex" é necessário na instância SNC. O IdP o retorna na resposta do SAML para fazer uma autenticação bem-sucedida.	O administrador do IdP deve confirmar se o "SessionIndex" está definido no SAMLResponse.
Não foram encontrados "SubjectConfirmation" válidos.	Falha na validação da confirmação do assunto.	N/D	As condições podem estar ausentes devido a um erro no IdP. O StatusCode na resposta conteria o Respondente em vez do Êxito esperado.	Analise o SAMLResponse para determinar se as condições estão incluídas no SAMLResponse. Os dados de confirmação do assunto válidos podem estar expirados ou não para o público-alvo correto.
Incompatibilidade de público-alvo de declaração.	Certifique-se de que o campo "URI do	O URI do público-alvo que aceita	O URI do público-alvo configurado da instância do SNC	Localizar <saml2:Audience> no SAMLResponse nos logs e verifique se

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Erros durante a configuração de Multi-SSO (SAML 2.0)

Erro nos logs de instância	Mensagem do Testar conexão	Propriedade SAML	Diagnóstico	Correção
Esperado: <propAudience>, vigente: <audienceUri>. ou Falha na validação de AudienceRestriction. Nenhum público-alvo correspondente encontrado.	público-alvo" esteja configurado corretamente.	o token SAML2. (Normalmente, é o URI da sua instância. Por exemplo: `https://demo.service-now.com`.)	deve corresponder ao valor no IdP.	o valor corresponde ao da instância.
O emissor da declaração é inválido. Esperado: <value on instance>, vigente: <value returned by IdP>	O emissor da declaração é inválido.	O URL Provedor de identidade que emite o token de segurança SAML2 com a informação do usuário.	O ID da entidade IdP (emissor) não corresponde ao valor definido na instância do SNC.	• Verifique se o IdP ou o SP está configurado corretamente. • Confirme se a propriedade SAML (O URL Provedor de identidade que emite o token de segurança SAML2 com a informação do usuário) está configurada corretamente.
O assunto é válido no futuro. Agora: <now>, NotBefore: <notBefore> ou Assunto expirado. Agora: <now>, NotOnOrAfter: <notOnOrAfter>	Falha na validação da confirmação do assunto.	O número, em segundos, antes da restrição "notBefore" ou após a restrição "notOnOrAfter", para ainda ser considerado válido.	O relógio do IdP não está sincronizado com o relógio do SP.	Atualize a propriedade SAML "glide.authenticate.sso.saml2.clockske para um valor maior. O padrão é de 180 segundos. Alguns casos exigem uma configuração de 300 ou superior. Também pode ser necessário verificar a hora no servidor IdP.
A estipulação será válida no futuro, agora: <now>, notBefore: <notBefore>	A confirmação é inválida.	O número, em segundos, antes da restrição	O relógio do IdP não está sincronizado com o relógio do SP	Atualize a propriedade SAML para um valor maior. O padrão é de 60 segundos. Alguns

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Erros durante a configuração de Multi-SSO (SAML 2.0)

Erro nos logs de instância	Mensagem do Testar conexão	Propriedade SAML	Diagnóstico	Correção
ou A estipulação perdeu a validade, agora: <now>, notOnOrAfter: <notOnOrAfter>		"notBefore" ou após a restrição "notOnOrAfter", para ainda ser considerado válido.		casos exigem uma configuração de 300 ou superior. Também pode ser necessário verificar a hora no servidor IdP.

Erros comuns de login e IdP

Erro ou sintoma	Diagnóstico	Correção
As solicitações de login geram um loop infinito entre o sistema e o IdP quando a Alta segurança está ativa.	• Normalmente, o endpoint do URL é uma página de erro ou de logout. • O "logout_redirect.do" pode criar esse loop quando você define *glide.security.url.whitelist* sem adicionar o nome do host IdP ao valor da propriedade. **Nota:** Para aprender mais sobre essa propriedade, consulte Lista de permissões de URL para redirecionamentos de logout nas Configurações de proteção de segurança de instância.	Defina (ou crie) a propriedade do sistema "glide.authenticate.failed_redirect" para redirecionar as solicitações de autenticação com falha para esse URL.
O token usado para autenticar o usuário ou a solicitação é assinado com o algoritmo de assinatura "http://www.w3.org/2001/04/xmldsig-more#rsa-sha256", que não é o algoritmo de assinatura esperado "http://www.w3.org/2000/09/xmldsig#rsa-sha1".	Verifique a guia "Contexto" do alerta para obter detalhes do evento.	Navegue até a guia "Avançado" da caixa de diálogo de configuração "Objeto de confiança de terceira parte confiável" e verifique se o algoritmo está definido como SHA-1 e não SHA-256.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Erros comuns de login e IdP

Erro ou sintoma	Diagnóstico	Correção
A mensagem de erro `urn:oasis:names:tc:SAML:2.0:status:Requester` aparece na sua tabela de log do sistema (syslog).	Quando seu IdP (por exemplo, ADFS) responde com um status de `oasis:names:tc:SAML:2.0:status:Requester`, isso significa que o IdP rejeitou o login devido a um problema com a solicitação enviada para ele. Infelizmente, a resposta SAML recebida do IdP não fornece mais detalhes sobre o erro.	Analise a solicitação SAML enviada ao IDP e trabalhe com o administrador do IDP para atualizar as configurações SAML da sua instância para evitar o erro. Pode ser necessário entrar em contato com o provedor de IDP para entender o motivo da falha de login.

Como redirecionar logins de single sign-on (SSO)

Quando o SSO está habilitado, você pode redirecionar usuários para páginas específicas ou direcionar usuários para fazer login localmente.

Por exemplo, se um usuário tentar acessar `https://customerX.service-now.com`, um portal interno da empresa poderá ser exibido em vez da página de login padrão. Ou quando um usuário faz logout de uma aplicação, o navegador pode redirecioná-lo para uma página interna específica. Você pode definir propriedades de redirecionamento dentro da instância para garantir que os usuários vejam uma página de login do SSO em vez da página de login padrão.

Nota: As propriedades a seguir não forçam o SSO. A página "login.do" ainda estará acessível e os usuários poderão fazer login no sistema se tiverem uma senha local definida.

Propriedades de redirecionamento

Quando um usuário faz logout, ou se houver falha na tentativa de login usando o SSO, você pode definir para onde o usuário será levado, como uma página principal do portal ou um artigo da base de conhecimento com informações de login do SSO. Use as seguintes propriedades para especificar os URLs. Se uma dessas propriedades não existir em sua instância, você poderá criá-la.

glide.authenticate.failed_requirement_redirect

URL para redirecionar usuários que tentam acessar uma página que é privada (por exemplo, para exibir um incidente) e não fornecem credenciais de SSO. A propriedade normalmente é definida como o portal de login de um cliente (por exemplo, `http://portal.companya.com/`).

glide.authenticate.failed_redirect

URL para redirecionar usuários após uma falha na tentativa do SSO. Você pode redirecionar para um artigo de conhecimento público que descreve o erro e tem links úteis (por exemplo, `http://portal.companya.com/error`).

glide.authenticate.external.logout_redirect

URL para redirecionar usuários após o logout, normalmente de volta ao portal que habilitou o login de single sign-on (por exemplo, `http://portal.companya.com/logout`).

glide.authentication.external.disable_local_login

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Quando definido como "verdadeiro", requer credenciais de SSO para a página de login principal. O padrão é "falso". Essa propriedade precisa ser usada em conjunto com a propriedade *glide.authenticate.failed_requirement_redirect*.

A tabela a seguir mostra o relacionamento entre os valores de retorno de Saída de instalação, as propriedades e o comportamento esperado.

Forçar login usando somente SSO

Valor de retorno	Propriedade	Comportamento
`failed_missing_requirement`	*glide.authenticate.failed_requirement_redirect*	Quando esse v indica que as c necessárias nã na sessão. Há f sessão é redire especificado p Normalmente, de SSO em que e as credencia
`failed_authentication`	*glide.authenticate.failed_redirect*	Quando esse v ele indica que de SSO forneci autenticação, o usuário está b no login e a ses para o URL esp propriedade. N do provedor de é contestado e coletadas.
<user_id>	N/D	Login autorizad especificado p valor correspon campo definid *glide.authen* ("o nome do c para correspon entrada")

Restrição de login local

Como precaução de segurança, você deve fazer mais do que depender das propriedades de redirecionamento para proibir o registro em log localmente. Se um usuário nunca deve fazer login localmente e sempre será autenticado pelo sistema de single sign-on interno, uma senha aleatória deverá ser atribuída a cada usuário importado para a instância. A senha aleatória é definida com mais facilidade no momento da importação do usuário. Se os dados do usuário forem importados para o sistema por meio de um conjunto para importação, você poderá criar um script de transformação "onBefore" usando o código a seguir.

```
var r  = new Packages. java. util. Random ( ) ;

 var str1  = Packages. java. lang. Long. toString (Packages. java. lang.
 Math. abs (r. nextLong ( ) ) , 36 ) ; var str2  = Packages. java. lang.
```

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

```
Long. toString (Packages. java. lang. Math. abs (r. nextLong ( ) ) , 36
) ;

var newPass  = str1  + str2 ;

target. user_password = newPass ;

//password now set to a random string like this:
//qvm81zdrn7cwwylpvw94eebk
```

Como clonar uma instância com uma integração SAML

Clone uma instância com uma integração SAML. Antes de clonar uma instância que usa SAML 2.0, mantenha as configurações relacionadas ao SSO do SAML na instância de destino; caso contrário, você pode tornar a instância de destino inacessível.

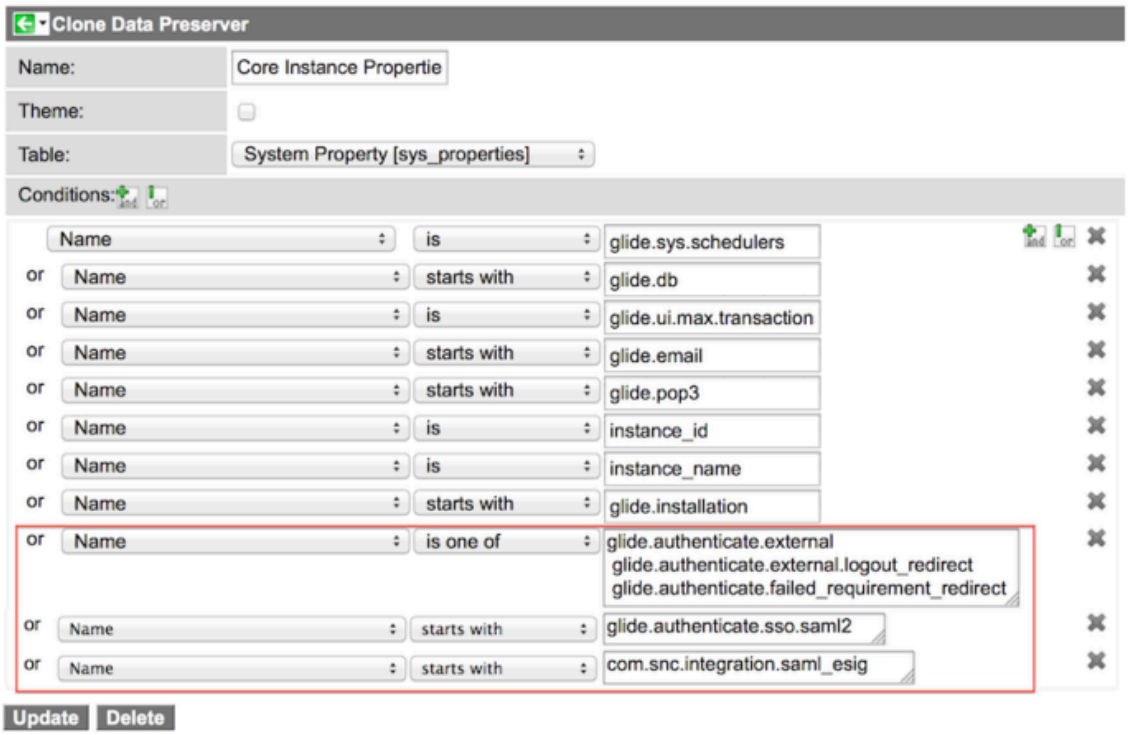
Antes de Iniciar

Função necessária: administrador

Procedimento

1. Na instância de origem, navegue até **Clone do sistema** > **Preservação de dados** > **Propriedades do núcleo da instância**.
2. Certifique-se de que as seguintes propriedades relacionadas ao SSO do SAML sejam preservadas usando as condições.
   - glide.authenticate
   - glide.security
   - glide.entry
   - glide.script
   - glide.session
   - glide.saml2
   - com.glide.communications
   - com.snc.integration.saml_esig

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Nota: Ao criar o clone, inclua anexos para que os certificados sejam transportados para a instância de destino. Além disso, certifique-se de que a caixa de seleção **Tema** esteja desmarcada para que essas propriedades sejam preservadas, independentemente de você preservar o tema da instância.

3. Na instância de origem, navegue até **Clone do sistema** > **Preservar dados** para preservar os certificados SAML em "sys_certificate" e os usuários SAML em "sys_user" relacionados ao SAML/SSO/Multi SSO.

   Se você precisar deles, exporte-os para XML e importe-os manualmente no destino.

   Aviso: Não tente clonar a configuração SAML/SSO/Multi SSO de um sistema para outro. A maioria das transferências de configurações de SAML/SSO ou Multi-SSO NÃO funcionam porque elas devem ser configuradas no provedor de identidade. Se você substituir uma configuração de trabalho, a instância de destino não será autenticada, portanto, sua instância de destino ficará inacessível. Além disso, não altere o "sys_id" do registro do provedor Multi-SSO, pois isso forçará os usuários a limpar os cookies. Para obter mais informações sobre precauções de clonagem, consulte Check-list antes de clonar uma instância.

4. Exclua as tabelas Multi-SSO "sso_properties", "digest_properties" e "saml2_update1_properties".
5. Crie manualmente os registros SAML/SSO/Multi-SSO em cada instância de forma independente e também configure os registros no seu provedor de identidade.
6. Certifique-se de criar manualmente uma conta de administrador LOCAL no registro "sys_user" (não no LDAP ou SAML) na instância de destino e com um "sys_id" que não existe na instância de origem.
7. Clique em **Atualizar**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

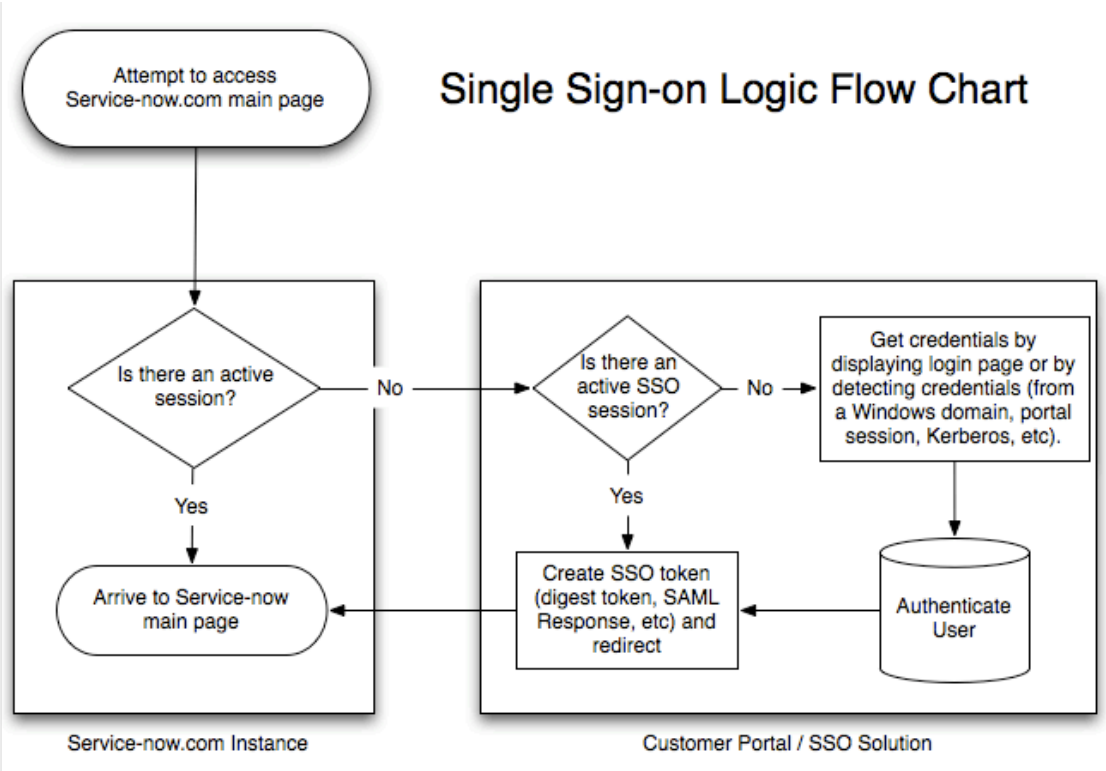
Conceitos do SAML 2.0

Familiarize-se com esses conceitos do SAML.

Fluxo do processo de SAML típico (diagrama)

Um fluxo lógico de SSO típico envolve procurar uma sessão ativa, verificar as credenciais do usuário e criar o token necessário.

SSO padrão



Fluxo do processo de login (AuthnRequest)

O SAML 2.0 especifica um perfil de SSO do navegador da Web que envolve a troca de informações entre um provedor de identidade (IdP), um provedor de serviço (SP) e uma entidade de segurança (usuário) em um navegador da Web.

O provedor de identidade pode ser qualquer serviço SSO que ofereça serviços de autenticação SAML (por exemplo, SSOCircle). O provedor de serviço é sempre uma instância. O fluxo de mensagens começa com uma solicitação de um recurso protegido no provedor de serviço.

Como solicite o recurso de destino no SP

A entidade de segurança solicita um recurso de destino no provedor de serviço:

https://instance.service-now.com/

A instância verifica a solicitação para ver se os parâmetros de URL "SAMLRequest" e "RelayState" estão presentes. Se eles existirem, o usuário já foi validado com o IdP e pode ignorar as etapas 2 a 6.

Como emitir um AuthnRequest para o provedor de identidade

A instância constrói um `AuthnRequest` a ser enviado ao IdP usando o valor `SAMLRequest`. A instância também constrói e envia um valor de parâmetro de URL `RelayState`.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O token `RelayState` é uma referência opaca às informações de estado mantidas no provedor de serviço. O valor do parâmetro `SAMLRequest` é o valor deflacionado e codificado em base64 do elemento `<samlp:AuthnRequest>`:

```
<samlp:AuthnRequest    xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    ID="identifier_1"    Version="2.0"
 IssueInstant="2004-12-05T09:21:59Z"
 AssertionConsumerServiceIndex="0"><saml:Issuer>https://
sp.example.com/SAML2</saml:Issuer><samlp:NameIDPolicy
 AllowCreate="true"
 Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient"/></samlp:Au
thnRequest>
```

A integração codifica por URL o elemento `<samlp:AuthnRequest>` e o envia como o parâmetro de URL `SAMLRequest`

O serviço de SSO processa o elemento `<samlp:AuthnRequest>` por decodificação de URL, decodificação base64 e aumento da solicitação, nessa ordem. Em seguida, ele executa uma verificação de segurança. Se o usuário não tiver um contexto de segurança válido, o IdP identificará o usuário solicitando credenciais de login. Se o usuário já estiver conectado, o IdP simplesmente responderá com os parâmetros de URL `SAMLResponse<tt> e <tt>RelayState` (consulte a etapa 3).

Como responder com um SAMLResponse e RelayState

Depois de coletar as credenciais de login necessárias, o serviço SSO valida a solicitação e responde com um documento que contém um formulário XHTML:

```
<formmethod="post"action="https://
instance.service-now.com/navpage.do" ...><input type="hidden"
 name="SAMLResponse" value="response ..." /><input type="hidden"
 name="RelayState" value="token ..." />
    ...
    <input type="submit" value="Submit" /></form>
```

O valor do parâmetro `RelayState` vem desta etapa. O valor do parâmetro `SAMLResponse` é a codificação em base64 do seguinte elemento `<samlp:Response>`:

```
<samlp:Responsexmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
  ID="s2cdc74f37f923e26fe1aeec42b70a93d24230334f"
  InResponseTo="90AA6073F01567BFB0DF194F596314E2"
 Version="2.0"  IssueInstant="2010-04-29T23:21:51Z"
 Destination="https://dloomac.service-now.com/navpage.do"><saml:Issuer
 xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">http://
idp.ssocircle.com</saml:Issuer><samlp:Status
 xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"><samlp:StatusCode
 xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
 Value="urn:oasis:names:tc:SAML:2.0:status:Success"></samlp:StatusCode
></samlp:Status><saml:Assertion
 xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    ID="s23e536bfc51b8487d4d3299dec162d9c2e338823b"
    IssueInstant="2010-04-29T23:21:51Z"
 Version="2.0"><saml:Issuer>http://
idp.ssocircle.com</saml:Issuer><Signature
 xmlns="http://www.w3.org/2000/09/xmldsig#">

...
```

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

```
      </Signature><saml:Subject><saml:NameID
 Format="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress"
            NameQualifier="http://idp.ssocircle.com"
 SPNameQualifier="https://
dloomac.service-now.com/navpage.do">david.loo@service-now.com</saml:NameI
D><saml:SubjectConfirmation
 Method="urn:oasis:names:tc:SAML:2.0:cm:bearer"><saml:SubjectConfirmation
Data              InResponseTo="90AA6073F01567BFB0DF194F596314E2"
              NotOnOrAfter="2010-04-29T23:31:51Z"
 Recipient="https://dloomac.service-now.com/navpage.do" /
></saml:SubjectConfirmation></saml:Subject><saml:Conditions
 NotBefore="2010-04-29T23:11:51Z"
 NotOnOrAfter="2010-04-29T23:31:51Z"><saml:AudienceRestriction><saml:Audi
ence>https://
dloomac.service-now.com</saml:Audience></saml:AudienceRestriction></saml:
Conditions><saml:AuthnStatement AuthnInstant="2010-04-29T23:21:51Z"

 SessionIndex="s2dbf89ab99001e0e8cdaed67266d9d4b21b968a04"><saml:AuthnCon
text><saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:Pa
sswordProtectedTransport</saml:AuthnContextClassRef></saml:AuthnContext
></saml:AuthnStatement></saml:Assertion></samlp:Response>
```

Como validar o SAMLResponse

O valor `SAMLResponse` é decodificado em base64 e aumentado para revelar o documento XML na etapa 3. O script de login extrai o valor XML do elemento `//Subject/NameID` e o usa para pesquisar um usuário existente na tabela Usuário.

O script de login também extrai o ID da sessão do elemento `//AuthnStatement/@SessionIndex` e o armazena para o `LogoutRequest`.

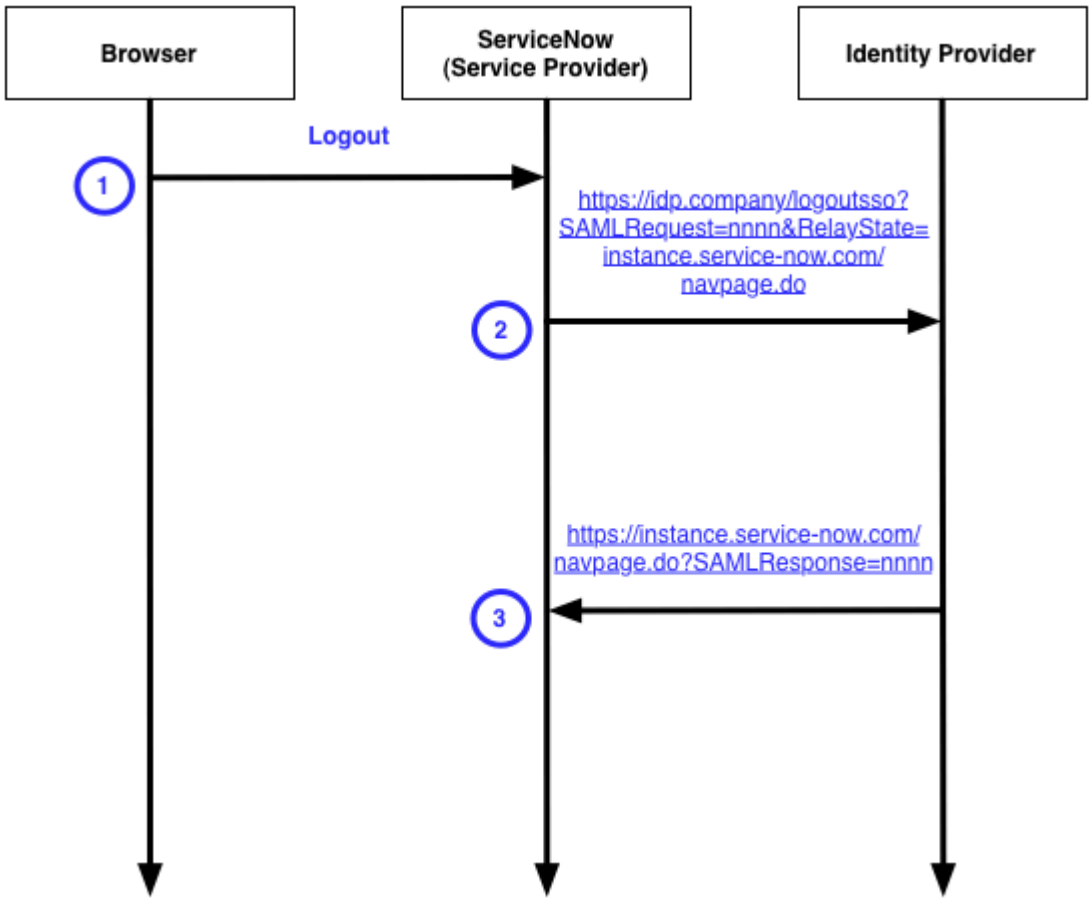
Fluxo do processo de logout (LogoutRequest)

Durante o logout, a instância emite a chamada do serviço *LogoutRequest* do SAML 2.0 para o IdP.

Esse serviço faz o logout do usuário e o redireciona de volta para o URL de logout especificado.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Logout do SAML 2



O usuário clica no botão de logout

O usuário clica no botão **Logout** e a instância executa o script de logout.

LogoutRequest emitido

O script de logout cria um `LogoutRequest` do SAML 2.0 e o publica no serviço "SingleLogoutRequest" pré-configurado do SAML 2.0 no IdP. O IdP esvazia a solicitação e a codifica em base64. Um exemplo de `LogoutRequest` se parece com este:

```
<saml2p:LogoutRequestxmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
 ID="21B78E9C6C8ECF16F01E4A0F15AB2D46"
 IssueInstant="2010-04-28T21:36:11.230Z"  Version="2.0"><saml2:Issuer
 xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">https://
dloomac.service-now.com
 </saml2:Issuer><saml2:NameID
 xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
 Format="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress"
          NameQualifier="http://idp.ssocircle.com"
 SPNameQualifier="https://
dloomac.service-now.com/navpage.do">david.loo@service-now.com</saml2:Name
ID><saml2p:SessionIndex>s211b2f811485b2a1d2cc4db2b271933c286771104
 </saml2p:SessionIndex></saml2p:LogoutRequest>
```

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

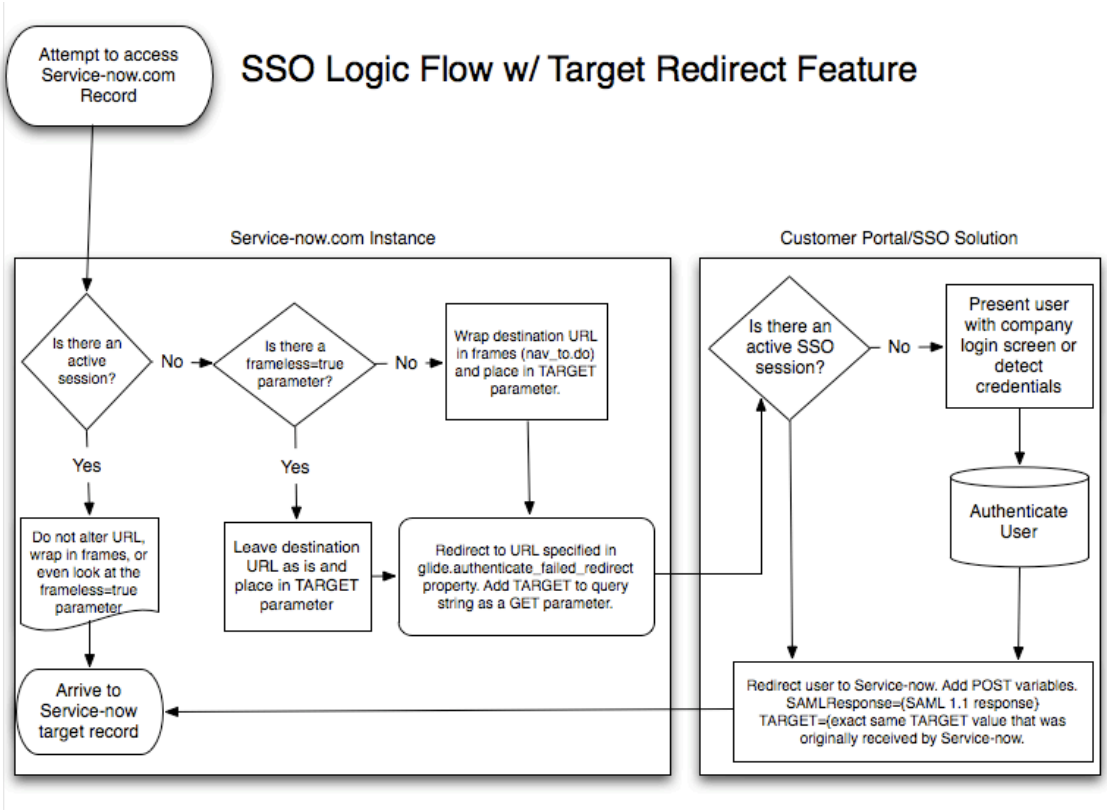
Usuário faz logout

O usuário faz logout do IdP. O IdP redireciona de volta para a instância, que por sua vez redireciona de volta para o IdP, já que o usuário não está conectado.

Informações de URL para um provedor de SSO

Durante uma contestação de login resultante de um link de URL para a instância que requer uma sessão SSO, o URL de referência pode precisar ser fornecido ao provedor de SSO para que, após a autenticação, o URL possa ser passado de volta para a instância e vinculado ao recurso correto.

Redirecionamento de destino do SSO



Os valores de retorno da saída de instalação foram aprimorados para passar um URL em vez de ou além do URL definido pelas propriedades. Normalmente, você retornaria um nome de usuário ou um valor de cadeia de caracteres predefinido para controlar, autorizar ou contestar a sessão do SSO. Os exemplos a seguir mostram o comportamento estendido de passar um URL.

```
return
 "failed_missing_requirement:%26amp;TARGET=https://
instance.service-now.com/nav_to.do?uri=incident.do?sys_id=12345";
```

O exemplo acima passa o URL `https://instance.service-now.com/nav_to.do?uri=incident.do?sys_id=12345` para o provedor SSO na forma de um parâmetro de URL chamado TARGET.

Nota: Presume-se que o provedor SSO usará essas informações no parâmetro TARGET para redirecionar de volta para a instância quando as credenciais do usuário tiverem sido coletadas e a autenticação aprovada.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O sinal de dois pontos (:) demarca os dois valores de retorno e um "&" codificado (%26amp;) concatena o URL definido na propriedade *glide.authenticate.failed_missing_requirement* e o parâmetro TARGET.

Configuração de SAML 2.0 usando SSO de vários provedores

É possível criar ou atualizar uma configuração de SSO do SAML 2.0 no recurso SSO de vários provedores.

Antes de Iniciar

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

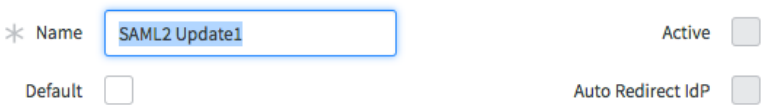
Nota: Novo na versão Jakarta, você deve validar sua configuração usando a funcionalidade Testar conexão antes de ativar sua configuração de IdP. É possível usar a funcionalidade Atualizar para salvar os dados de configuração, mas a configuração não será ativa sem um teste de conexão bem-sucedido.

Procedimento

1. Navegue até **Todos** > **SSO de vários provedores** > **Provedores de identidade**.
2. Especifique uma das seguintes opções.
   - Para atualizar uma configuração, clique em um registro de configuração de SSO.
   - Para criar uma nova configuração, clique em **Novo** > **SAML**.
3. Digite as informações de IdP usando um dos seguintes métodos.

Opção	Descrição
Uso de um URL descritor de metadados	Clique na caixa de seleção URL e insira o URL do IdP que estiver usando.
Uso do arquivo do descritor de metadados XML	Clique na caixa de seleção XML e cole os dados XML gerados a partir do IdP usado.
Inserção manual de metadados	Feche a janela pop-up e insira manualmente os dados nos campos de propriedade.

Todos os campos obrigatórios devem ser preenchidos no formulário Provedor de identidade.



Campos de Single Sign-on de vários provedores

Propriedade	Necessários	Descrição
Nome	Sim	Insira o nome do IdP. Este IdP é a ID do sistema de redirecionamento automático.
Ativo	Sim	Ativo deve ser definido como verdadeiro para o IdP a ser usado para autenticação. **Nota:** A opção para definir esta propriedade é exibida somente após um teste de conexão bem-sucedido.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Propriedade	Necessários	Descrição
Padrão	Não	A configuração Redirecionar IdP automaticamente, anteriormente conhecida como IdP primário, redireciona os usuários automaticamente para que acessem o URL da instância base. Esta propriedade define esta configuração de IdP como padrão.
Redirecionar IdP automaticamente	Não	Define esta configuração de IdP como Redirecionar IdP automaticamente. **Nota:** Se uma nova configuração Redirecionar IdP automaticamente for ativada, o cookie *glide_sso_id* será atualizado com o novo IdP de redirecionamento automático. A propriedade do sistema *glide.authenticate.sso.update.idp.cookie*, habilitada automaticamente, controla este recurso.
URL do provedor de identidade	Sim	Insira o URL do seu IdP. Cada URL de IdP deve ser exclusivo.
AuthnRequest do provedor de identidade	Sim	Insira o URL para a vinculação HTTP-Redirect obtida do elemento SingleSignOnService.
SingleLogoutRequest do provedor de identidade	Não	Insira o URL obtido do elemento SingleLogoutService.
ServiceNow Página inicial	Sim	Insira o URL, incluindo a página de login, da instância para a qual o IdP é autenticado. Por exemplo: https://yourinstance.service-now.com/navpage.do
ID da entidade/ emissor	Sim	Insira o URL base, excluindo a página de login da instância para a qual o IdP faz a autenticação. Por exemplo: https://yourinstance.service-now.com/
URI do público	Sim	Insira o URL base, excluindo a página de login da instância para a qual o IdP faz a autenticação. Por exemplo: https://yourinstance.service-now.com/
Política NameID	Sim	Insira o valor do elemento NameIDFormat usado pela integração.
Redirecionamento de logout externo	Não	Insira o URL para onde a integração redireciona os usuários após o logout.
Redirecionamento de requisito com falha	Não	Insira o URL para redirecionamento de solicitações de autenticação com falha. Por padrão, este é o endpoint do URL de uma página de erro ou página de logout configurada no IdP. É possível preencher este valor no campo glide.authenticate.failed_requirement_redirect.
Tipo de Cliente	Não	Escolha o tipo de cliente com base no tipo do seu cliente. Opções:**Iframe integrado**.

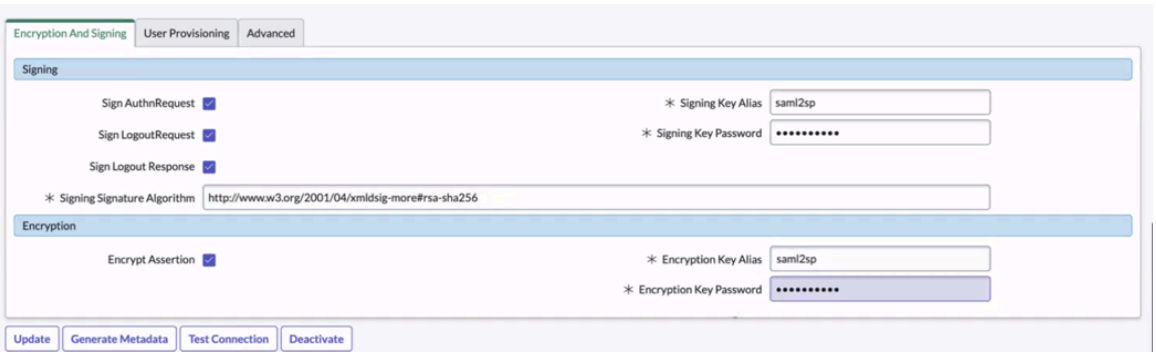
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Propriedade	Necessários	Descrição
		Nota: Se o campo de tipo de cliente for necessário para sua configuração, você poderá editar o formulário e adicionar o campo. Para saber mais, consulte Como configurar o tipo de cliente para registros de OAuth e SSO.

4. Opcional: Guia Criptografia e assinatura

Nota:

- Recomendamos o uso dos seus próprios certificados para criptografia e assinatura.
- O **modo aprovado FIPS** requer certificados diferentes para **Criptografia** e **Assinatura**
- Ao usar os certificados, certifique-se de atualizar as seguintes propriedades do sistema com o sys_id dos certificados (certificados x.509):
  - **Assinatura** (`glide.authenticate.sso.saml2.keystore`)
  - **Criptografia** (`glide.authenticate.sso.saml2.encryption.keystore`)
- Certifique-se de atualizar o alias e a senha da chave dos armazenamentos de chave de **Assinatura** e **Criptografia** no registro do provedor de identidade e gerar os metadados (selecione **Gerar metadados**).
- Carregue os certificados de assinatura e criptografia presentes nos metadados gerados (XML) para o provedor de identidade.



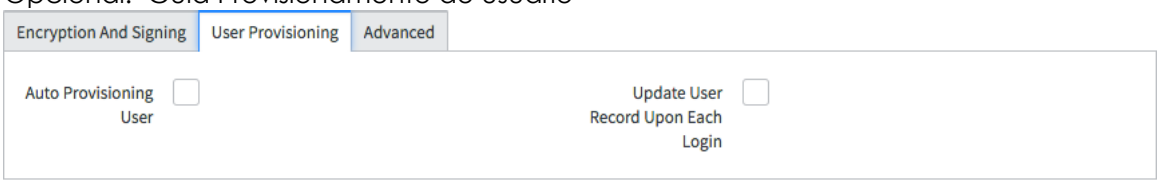
Campos de Criptografia e assinatura

Propriedade	Descrição
Alias das chaves de assinatura	Insira o alias de assinatura da entrada de chave armazenada no armazenamento de chaves SAML 2.0 SP.
Senha da chave de assinatura	Insira a senha de assinatura da entrada de chave armazenada no armazenamento de chaves SAML 2.0 SP.
Alias da chave de criptografia	Insira o alias de criptografia da entrada de chave armazenada no armazenamento de chaves SAML 2.0 SP.
Senha da chave de criptografia	Insira a senha de criptografia da entrada de chave armazenada no armazenamento de chaves SAML 2.0 SP.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Propriedade	Descrição
Estipulação da criptografia	Marque a caixa de seleção para criptografar a estipulação na resposta do SAML. Os metadados gerados para o IDP incorporam o certificado x509, que o IDP usa para criptografar a estipulação na resposta do SAML gerada por ele.
Algoritmo de assinatura para assinar	Insira o URL que aponta para o consumidor de AuthnRequest do provedor de identidade SAML 2.0 para a autenticação de assinaturas eletrônicas.
Assinar AuthnRequest	Marque a caixa de seleção para habilitar o serviço de logon único IdP para receber um AuthnRequest assinado.
Assinar LogoutRequest	Marque a caixa de seleção para habilitar o serviço de logon único IdP para receber um LogoutRequest assinado.
Assinar resposta de logout	Marque a caixa de seleção para habilitar o serviço de logon único IdP para receber uma Resposta de logout assinada.

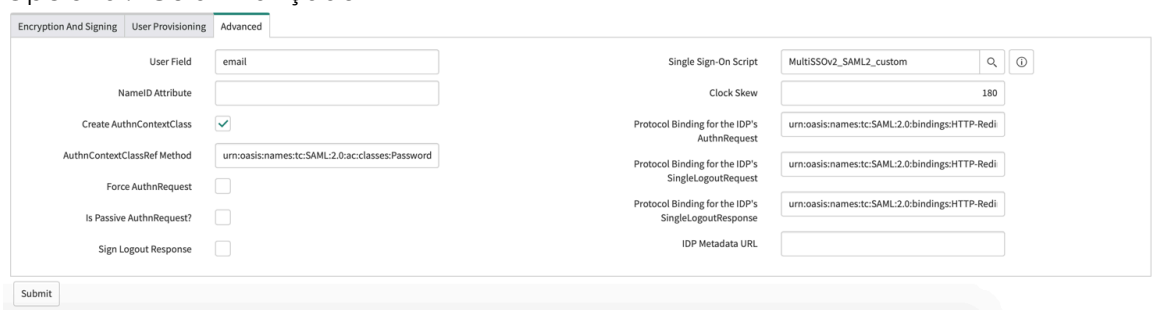
5. Opcional: Guia Provisionamento de usuário



Campos de Provisionamento de usuário

Propriedade	Descrição
Usuário de autoprovisionamento	Habilitar o provisionamento automático de usuários cria os usuários quando o usuário não existir na tabela Usuário da instância com base nas informações fornecidas pelo IdP.
Atualizar registro do usuário a cada logon	Atualiza as informações do usuário na tabela Usuário da instância com as informações no IdP sempre que o usuário faz login usando SAML.

6. Opcional: Guia Avançado



Campos de Avançado

Propriedade	Descrição
Campo de Usuário	Insira o campo na tabela Usuário que contém o valor requerido pelo IdP para identificar o usuário. Esta é uma ID exclusiva como parte da resposta. Por exemplo, nome de usuário, ID de

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Propriedade	Descrição
	funcionário e assim por diante. Na tabela Usuário do sistema, esta ID exclusiva corresponde aos detalhes do usuário.
Atributo NameID	Deixe este campo em branco, a menos que você configure uma nova política NameID. Se você configurar uma nova política, o sistema exigirá a tabela Usuário ser usada para identificar o usuário que faz o login. O sistema corresponde o token NameID ao nome no campo da tabela Usuário aqui.
Criar AuthnContextClass	Marque a caixa de seleção para especificar uma classe de contexto específica, como Transporte protegido por senha. Se a caixa de seleção estiver desmarcada, o IdP selecionará a classe de contexto mais apropriada.
Método AuthnContextClassRef	Insira o URN do mecanismo de login a ser usado pelo IdP para a autenticação de usuários.
Forçar AuthnRequest	Marque a caixa de seleção para forçar a ocorrência de AuthnRequests.
A AuthnRequest é passiva?	Marque a caixa de seleção se a AuthnRequest for passiva.
Script de Single Sign-on	Selecione o script de Single Sign-on O padrão é *MultiSSOV2_SAML2_custom*.
Assinar resposta de logout	Insira os detalhes da resposta de logout neste campo.
Distorção do relógio	Insira o número de segundos entre os dois atributos que compõem o nonce SAMLResponse. O padrão é 60. Um SAMLResponse válido deve estar entre os valores de data e hora *notBefore* e *notOnOrAfter*. Consulte a amostra de resposta SAML 2 com os elementos SubjectConfirmation e SubjectConfirmationData e a amostra de resposta SAML 2 com AudienceRestrictions e Audience Elements para obter uma amostra de mensagem SAMLResponse.
A ligação de protocolo para o SingleLogoutRequest do IDP	Insira um dos valores compatíveis listados no atributo de vinculação do elemento SingleLogoutService.
URL de metadados dos quais as propriedades do IDP são importadas	As propriedades do IdP são importadas deste URL. Se definido, ele habilitará a importação automática do certificado SAML do IdP se o certificado anterior tiver expirado. **Nota:** Se você fizer upgrade da atualização 1 do SAML2 para SSO de vários provedores ou se configurar sua conexão SSO manualmente, o URL de metadados do IdP não será preenchido automaticamente.
Solicitação	Uma ID exclusiva como parte da solicitação. A ID pode ser o nome do usuário, a ID do funcionário e assim por diante.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

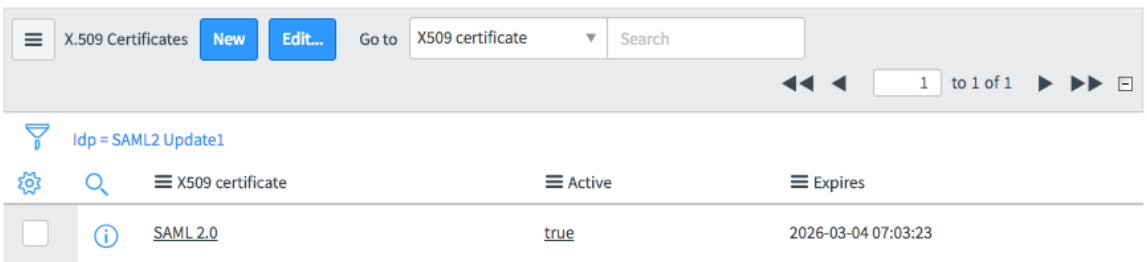
Propriedade	Descrição
	Nota: A vinculação de redirecionamento e publicação é compatível com a solicitação. A opção de definir este campo é exibida somente após um teste de conexão bem-sucedido. Para obter mais informações, consulte Teste de conexões IdP.
Resposta	Uma ID exclusiva como parte da resposta. A ID pode ser o nome do usuário, a ID do funcionário e assim por diante. **Nota:** A vinculação de redirecionamento e publicação é compatível com a resposta. A opção de definir este campo é exibida somente após um teste de conexão bem-sucedido. Para obter mais informações, consulte Teste de conexões IdP.

Certificado X.509 para SAML

Armazene e ative os certificados do IdP necessários para sua configuração SAML.

X.509 são os certificados IdP usados por uma configuração SAML. Depois de instalar um certificado, é possível adicionar quantos certificados forem necessários. Quando vários certificados estão disponíveis, o sistema usa o primeiro certificado ativo encontrado. Se definir o URL do campo **URL de metadados dos quais as propriedades do IdP são importadas**, o sistema pesquisará o IdP automaticamente em busca de um certificado válido quando o seu certificado perder a validade. Ele anexa este certificado à sua instância e o usa para a configuração do SAML ativo.

Nota: A pesquisa ocorrerá se o IdP estiver acessível fora da sua rede.



Tour guiado do SAML

Use o Tour guiado do SAML para configurar o SAML para logon único.

O Tour guiado do SAML ajuda você a praticar e configurar o SSO para sua instância ServiceNow®. Os administradores podem selecionar o tour guiado para saber rapidamente as ações necessárias ao configurar o SSO para as instâncias.

Antes de usar o tour guiado, você deve configurar uma aplicação SAML no seu Provedor de identidade preferencial, como Okta, Microsoft Azure, ADFS e assim por diante. Para saber como configurar uma aplicação SAML, consulte a seguinte documentação:

- Okta: Para o Okta, você deve executar:
  - Adicionar uma aplicação SAML do Okta
  - Configurar SAML 2.0 para ServiceNow®

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Microsoft Azure: Integração de logon único (SSO) com ServiceNow®
- Ping: Configuração de SSO do SAML com ServiceNow®
- ADFS: Integração com SAML 2.0

Para usar o Tour guiado do SAML, ative o plug-in Integration - Multiple Provider Single Sign-On Installer. Para obter mais informações, consulte Ativar plug-in Multi-Provider SSO.

Para usar o Tour guiado do SAML, siga estas etapas:

1. Navegue até **Todos** > **SSO de vários provedores** > **Provedor de identidade**.
2. Clique em **Nova**.
3. Selecione **SAML**.
4. Clique no ícone de **Ajuda**.
5. Clique em **Fazer um tour**.

O Tour guiado do SAML usa uma série de etapas que se estendem por várias páginas para concluir a configuração. Siga as etapas e instruções fornecidas como parte do tour para o concluir. Para saber mais sobre a configuração SAML, consulte Configuração de SAML 2.0 usando SSO de vários provedores.

Como integrar SAML 2.0 com outros recursos

Você pode integrar sua solução SAML 2.0 com outros recursos, como assinatura eletrônica, link profundo e ADFS.

Como adicionar suporte de link profundo para SAML

Os links profundos permitem que as instâncias ofereçam suporte a links de e-mail diretos para um registro específico no sistema.

Com a integração SAML 2.0 habilitada, os URLs de link profundo devem passar por uma verificação de autenticação antes que o IdP redirecione o usuário para o URL solicitado originalmente. Por exemplo, considere um e-mail que contenha este URL: `https://<instance name>.service-now.com/nav_to.do?uri=incident.do?sys_id=46c88ac1a9fe1981014de1c831fbcf6d`

A instância envia uma solicitação de autenticação para o IdP e usa o parâmetro de URL `RelayState` para preservar o recurso solicitado originalmente (neste caso, `uri=incident.do?sys_id=46c88ac1a9fe1981014de1c831fbcf6d`). Depois que o IdP autentica o usuário, a instância lê o valor do parâmetro de URL "RelayState" e redireciona o usuário para o recurso solicitado (se ele existir na instância).

Para adicionar suporte a links profundos, verifique se o provedor de identidade oferece suporte ao parâmetro de URL `RelayState`.

Integração ADFS com SAML 2.0

O plug-in de SSO para Vários Provedores do ServiceNow oferece suporte a uma integração de Single Sign-on (SSO) do SAML 2.0 com o Microsoft ADFS.

Para obter informações sobre como instalar e configurar o ADFS, consulte Visão geral dos Serviços de Federação do Active Directory. O plug-in de SSO para Vários Provedores foi configurado e testado com uma integração SSO do SAML 2.0 com ADFS 2.0 e 3.0. Atributos do Azure AD não são compatíveis com a resposta do SAML em

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Como configurar ADFS para SAML

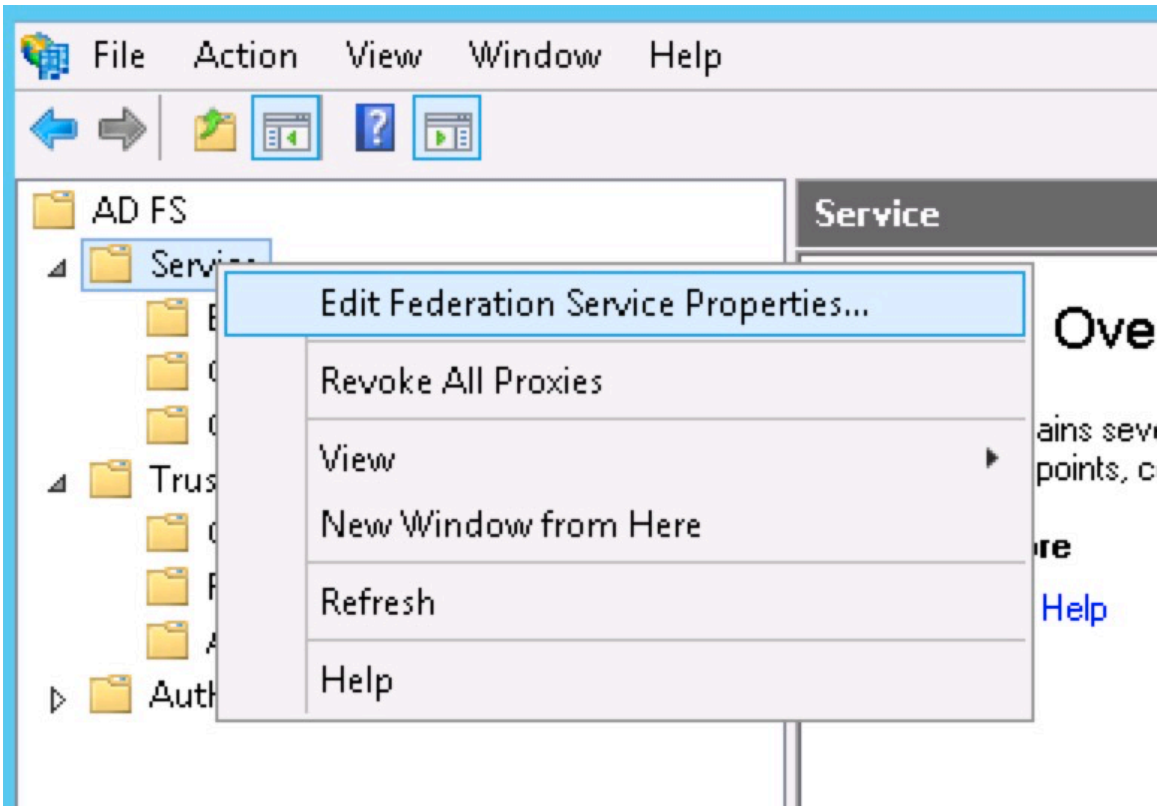
Configure ADFS para SAML. Este procedimento usa ADFS 2.0 e mostra "samportal.example.com" como o site do ADFS. Substitua-o pelo endereço do site do ADFS.

Antes de Iniciar

Função necessária: administrador

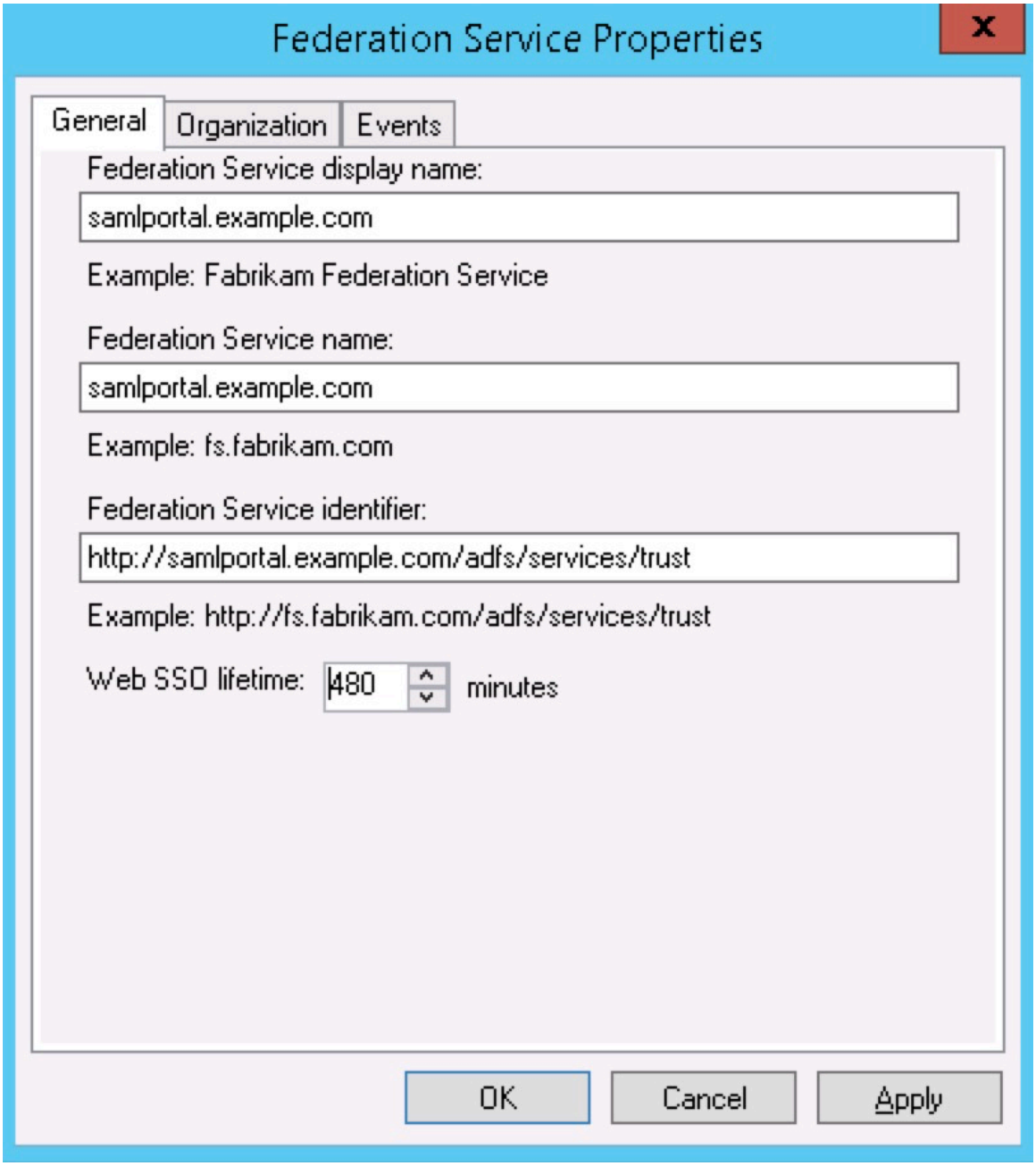
Procedimento

1. Faça login no servidor ADFS 3.0 e abra o console de gerenciamento.
2. Clique com o botão direito do mouse em **Serviço** e selecione **Editar propriedades dos Serviços de Federação**.



3. Confirme se as configurações gerais correspondem às entradas DNS e aos nomes de certificado.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Navegue até os certificados e exporte o certificado de assinatura de token.

a. Clique com o botão direito do mouse no certificado e selecione **Exibir certificado**.

b. Selecione a guia **Detalhes**.

c. Clique em **Copiar para arquivo**.
O Assistente para exportação de certificado é aberto.

d. Selecione **Avançar**.

e. Verifique se a opção **Não exportar a chave privada** está selecionada e clique em **Avançar**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

f. Selecione **X.509 binário com codificação DER (.cer)** e clique em **Avançar**.

g. Selecione onde você deseja salvar o arquivo, atribua um nome a ele e clique em **Avançar**.

h. Selecione **Concluir**.
A instância requer que este certificado esteja no formato PEM. Você pode converter este certificado usando ferramentas de cliente ou ferramentas online, como SSL Shopper.

5. Use o certificado DER/binário que você acabou de criar e exporte-o no formato PEM padrão.

Como configurar a instância para ADFS

Defina sua instância e as configurações SAML 2.0 para funcionar com o ADFS.

Antes de Iniciar

Execute essas etapas somente depois de configurar o ADFS para SAML. Para obter detalhes sobre esse processo, consulte Como configurar ADFS para SAML.

Função necessária: administrador

Procedimento

1. Se ele ainda não estiver ativo, Ativar plug-in Multi-Provider SSO.
2. Configure SAML, mas ao instalar o certificado IdP, anexe o certificado PEM que você criou em Como configurar ADFS para SAML.
3. Clique em **Salvar**.
4. Verifique se os campos **Problema** e **Assunto** estão preenchidos com valores e se não há erros.
Se ocorrer um erro, abra o certificado salvo no formato PEM no bloco de notas e copie e cole o certificado no campo "Certificado PEM".
5. Verifique se a saída de instalação SAML2SingleSignon_update1 está ativa.
6. Continue a configuração do SAML 2.0.

Nota: Quando um certificado é atualizado no servidor ADFS, também será necessário carregar um certificado atualizado para a instância.

Como configurar uma terceira parte confiável do ADFS

Obtenha os metadados da instância e importe-os para o servidor ADFS. No entanto, a configuração manual da terceira parte confiável parece ser mais fácil de implementar.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Navegue até **Todos** > **SSO de vários provedores** > **Provedores de identidade** > **SAML2 Update1** > **Criptografia e assinatura** e verifique se a propriedade SAML "Assinar AuthnRequest" (*glide.authenticate.sso.saml2.require_signed_authnrequest*) não está ativa.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mantenha essa propriedade ativa somente se o administrador do ADFS puder verificar que você precisa de solicitações assinadas.

2. Copie os metadados que você gerou por meio do link de metadados do SAML 2 e salve-os em um arquivo.
3. Faça login no servidor ADFS e abra o console de gerenciamento.
4. Selecione **Objeto de confiança de terceira parte confiável**.
5. Selecione **Adicionar Objeto de confiança de terceira parte confiável** no canto superior direito da janela.

   O assistente de adição é exibido.

6. Clique em **Iniciar** para começar.
7. Use a opção **Importar arquivo** para importar o arquivo de metadados.
8. Atribua a ele um nome de exibição, como `ServiceNow`, e insira as anotações desejadas.
9. Selecione o **Perfil do ADFS 3.0**.
10. Não selecione um certificado de criptografia de token.
    Ele usará o certificado definido no serviço que já foi exportado. Definir um certificado impede a comunicação apropriada com a instância.
11. Não habilite nenhuma configuração em **Configurar URL**.
12. Insira o site da instância ao qual você se conectou como o identificador "Objeto de confiança de terceira parte confiável".
    Nesse caso, use `https://company.service-now.com` e clique em **Adicionar**.
13. Permita que todos os usuários acessem essa terceira parte confiável.
14. Clique em **Avançar** e desmarque a caixa de seleção **Abrir Declarações ao finalizar**.
15. Feche essa página.
    O novo objeto de confiança de terceira parte confiável aparecerá na janela.
16. Clique com o botão direito do mouse em "Objeto de confiança de terceira parte confiável" e selecione **Propriedades**.
17. Navegue até a guia **Avançado** e defina o **algoritmo de hash seguro** como SHA-256 ou SHA-1.
18. Navegue até a guia "Endpoints" e adicione uma **Estipulação do cliente de SAML** com uma vinculação **Post** e um URL de `https://company.service-now.com/navpage.do`.

Configurar regras de declaração de uma terceira parte confiável do ADFS

Edite as regras de declaração para habilitar a comunicação apropriada com a instância.

Antes de Iniciar

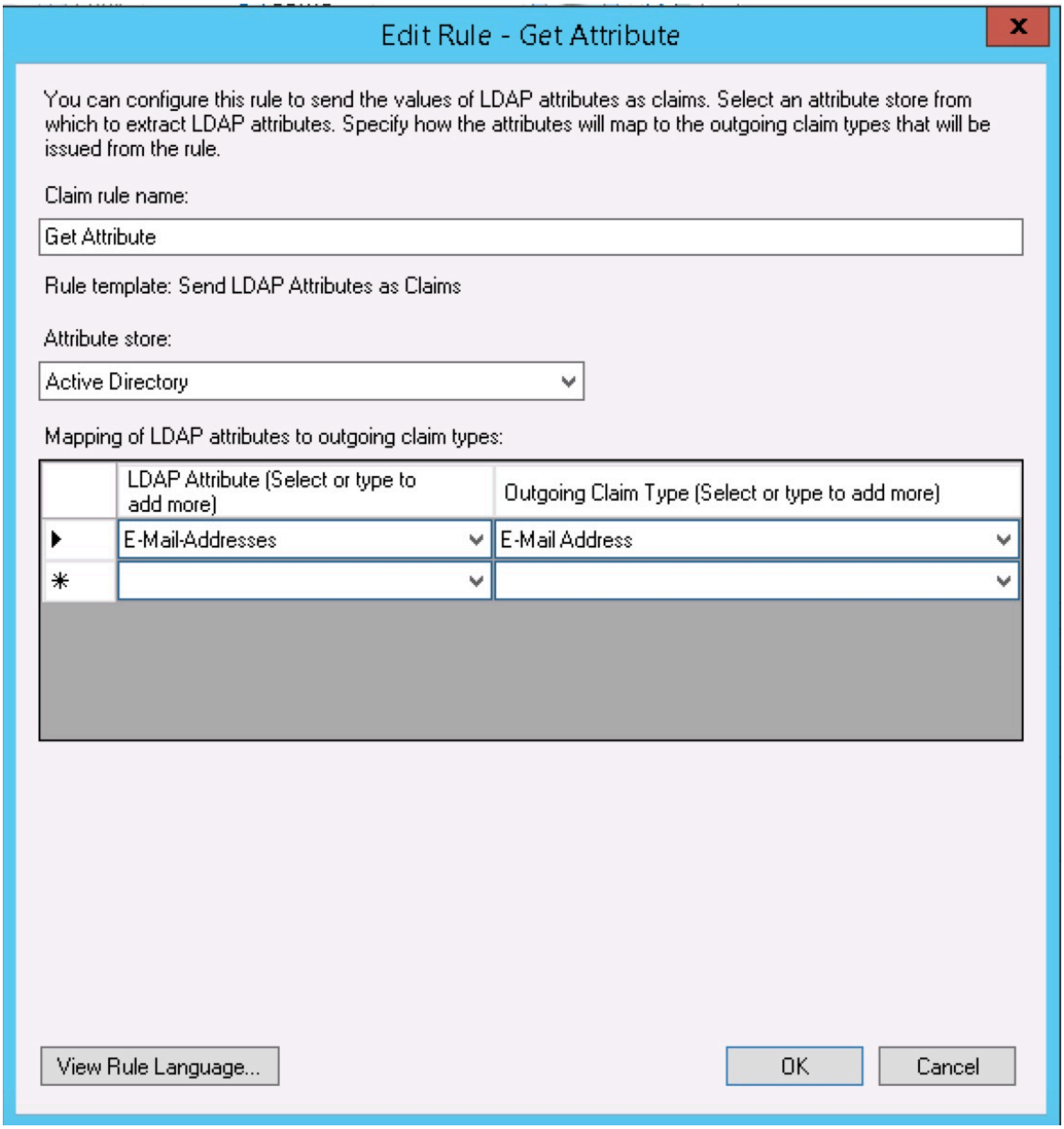
Função necessária: administrador

Procedimento

1. Faça login no servidor ADFS e abra o console de gerenciamento.
2. Clique com o botão direito do mouse em "Objeto de confiança de terceira parte confiável" e selecione **Editar regras de declaração**.
3. Clique na guia **Regras de transformação de emissão**.
4. Selecione **Adicionar regras**.
5. Selecione **Enviar atributo LDAP como declarações** como o modelo de regra de declaração a ser usado.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

6. Atribua à declaração um nome como `Obter atributos LDAP`.
7. Defina o **Armazenamento de atributo** como `Active Directory`, o **Atributo LDAP** como `Endereços de e-mail`e o **Tipo de declaração de saída** como `Endereço de e-mail`.




```
c:[Type ==
 "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccoun
tname", Issuer == "AD AUTHORITY"]
=> issue(store = "Active Directory",
types =
 ("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress
"),
query = ";mail;{0}", param = c.Value);
```

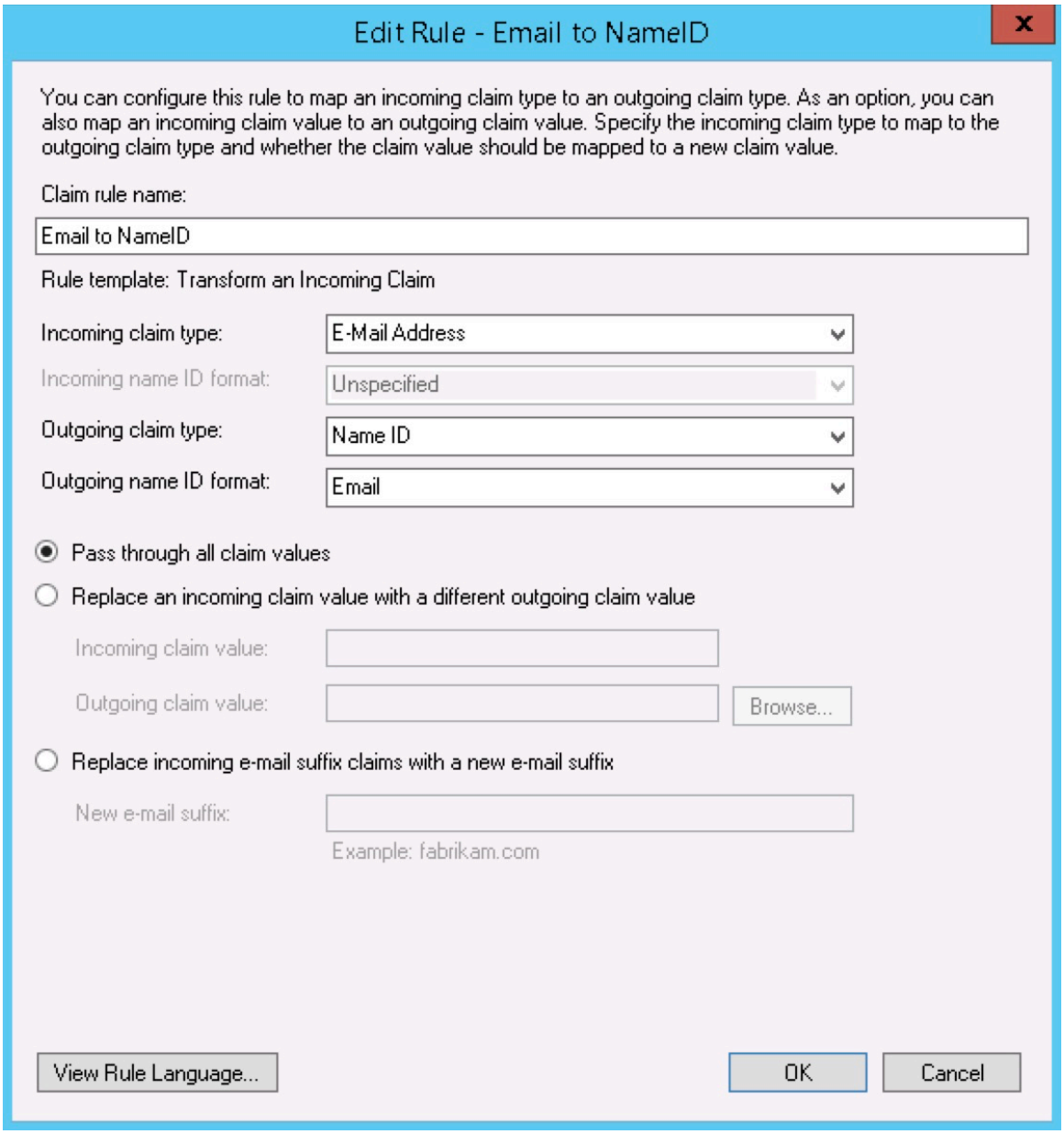
8. Selecione **Concluir**.
9. Selecione **Adicionar regras**.
10. Selecione **Transformar uma declaração de entrada** como o modelo de regra de declaração a ser usado.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

11. Atribua à declaração um nome, como `E-mail para ID do nome`.
12. Defina o **Tipo de declaração de entrada** como o **Tipo de declaração de saída** na regra anterior.
    Por exemplo, `Endereço de e-mail`.
13. Defina o **Tipo de declaração de saída** como `ID do nome` e o **Formato da ID do nome de saída** como `E-mail`.

    Nota: Esses valores devem corresponder à Política de ID de nome que você definiu durante a configuração do SAML 2.0.

14. Selecione **Passar por todos os valores de declaração**.



Essa regra de declaração deve ser semelhante à linguagem de regra a seguir.

```
c:[Type ==
 "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"]
```

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

```
 => issue(Type =
 "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifie
r",
Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value,
 ValueType = c.ValueType,
Properties["http://
schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"]
= "urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress");
```

15. Clique em **Concluir**.

Como criar um endpoint de logout do SAML

Crie um endpoint de logout do SAML para permitir um logout único.

Antes de Iniciar
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa
Consulte este artigo sobre saída do ADFS para obter mais informações.

Procedimento

1. Vá para **Gerente de ADFS** > **Relações de confiança** > **Objeto de confiança de terceira parte confiável** > **Propriedades**.
2. Na guia "Endpoints", clique em **Adicionar SAML**.
3. Defina as configurações:
   - **Tipo de endpoint**: logout do SAML
   - **Vinculação**: POST
   - **URL confiável**: o URL do seu servidor ADFS. Por exemplo,

     ```
     https://myadfsserver.domain.net/adfs/ls/?wa=wsignout1.0
     ```

   - **URL da resposta**: o URL de logout da aplicação. Por exemplo,

     ```
     https://{instancename}.service-now.com/external_logout_complete.do
     ```

Teste a configuração do ADFS

Teste sua configuração do ADFS para verificar se ela está funcionando corretamente como um provedor de identidade.

Antes de Iniciar
Função necessária: administrador

Procedimento

1. Abra o navegador Internet Explorer.
2. Navegue até o seu portal ADFS.

   Por exemplo, `https://samportal.example.com/adfs/ls/idpinitiatedsignon.aspx`. Esta página contém uma lista suspensa de todos os Objetos de confiança de terceira parte confiável configurados.

3. Selecione a terceira parte confiável associada à sua instância.
4. Clique em **Continuar para login**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Se você configurou a autenticação externa SAML 2.0 corretamente, deverá fazer login automaticamente na instância.

5. Para testar um URL de login direto, navegue até `https://samportal.example.com/adfs/ls/idpinitiatedsignon.aspx?logintoRP=https://company.service-now.com`.

(Solução alternativa) Como habilitar uma autenticação iniciada pelo provedor de serviço

Use essa solução alternativa se a autenticação falhar por você não ter o "SAML 2.0 Update 1". Esse problema pode acontecer se os usuários tentarem ignorar a autenticação IdP e navegar diretamente para a instância.

Antes de Iniciar
Função necessária: admin

Por Que e Quando Desempenhar Esta Tarefa
Este erro ocorre quando a instância não informa ao ADFS a definição e a semântica necessárias para o atributo "SPNameQualifier" no SAMLResponse.

Para habilitar a autenticação iniciada pelo provedor de serviço, siga um destes procedimentos:

Procedimento
- Faça upgrade para o "SAML 2.0 Update 1" e desmarque a opção para criar uma solicitação "AuthnContextClass".
- Modifique a inclusão de script do **SAML2** para comentar as definições do atributo `SPNameQualifier` quando o SAML 2.0 estiver ativo (não o SAML 2.0 Update 1).

  Comente as seguintes linhas nas funções "createNameID" e "createNameIDPolicy":

```
//nid.setSPNameQualifier (serviceURL ) ;

 //nameIdPolicy. setSPNameQualifier (serviceURLStr ) ;
```

O que Fazer Depois
Se você não quiser que o aviso de login do servidor ADFS apareça ao acessar a instância, defina como "falsa" a seguinte propriedade do "SAML 2.0 Update 1": **Crie uma solicitação AuthnContextClass na declaração AuthnRequest**(*glide.authenticate.sso.saml2.createrequestedauthncontext*).

(Solução alternativa) Suporte à autenticação Kerberos

Uma solução alternativa está disponível para a integração do SAML 2.0 que muda o contexto de autenticação da autenticação baseada em formulários para a autenticação baseada no Windows.

Antes de Iniciar
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa
Atualmente, a integração do SAML 2 usa um contexto de autenticação "PasswordProtectedTransport" ou "autenticação baseada em formulários". Esse contexto de autenticação requer que o IdP apresente aos usuários um formulário para credenciais de autenticação. Com o Kerberos, uma sessão SAML já está ativa por meio de um login do Windows estabelecido, portanto, o usuário não precisa se autenticar com o IdP.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegue até **Todos** > **SSO de vários provedores** > **Provedores de identidade**.
2. Abra o registro IdP **SAML2 Update1**.
3. Defina **O método AuthnContextClassRef que incluímos em nosso SAML 2.0 AuthnRequest para o Provedor de Identidade** para uma das opções a seguir:

Valores do método "AuthnContextClassRef"
`urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport` (padrão)
`urn:federation:authentication:windows`

4. Clique em **Atualizar**.

Integração do Azure AD com o SAML 2.0

Integre o ServiceNow com o Azure Active Directory (Azure AD).

A integração do ServiceNow com o Azure AD permite que você:

- Controle no Azure AD quem tem acesso a ServiceNow.
- Permita que os usuários entrem automaticamente no ServiceNow usando suas contas do Azure AD.
- Gerencie suas contas no portal do Azure.

Pré-requisitos

Para começar, você precisa fazer o seguinte:

- Uma assinatura do Azure AD. Se você não tiver uma assinatura, poderá obter uma conta gratuita.
- O Single Sign-on (SSO) do ServiceNow habilitado.
- Uma instância do ServiceNow ou um locatário de ServiceNow que ofereça suporte a versões San Diego ou posteriores.
- Um locatário ServiceNow deve ter o plug-in de Single Sign-on de vários provedores habilitado.
- Para configuração automática, habilite o plug-in de vários provedores para ServiceNow.

Conjunto de ações para configuração

A seguir está o conjunto de ações que precisam ser executadas para configurar o Azure AD:

- Adicione ServiceNow da galeria ao Azure AD.
- Configurar o SSO do Azure AD
- Criar um usuário de teste do Azure AD
- Atribuir o usuário de teste do Azure AD
- Configurar o ServiceNow

Adicionar ServiceNow da galeria

Adicione ServiceNow da galeria à sua lista de aplicativos SaaS gerenciados no Azure AD.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: Azure admin

Procedimento

1. Entre no portal do Azure usando uma conta da Microsoft.
2. Selecione o serviço **Azure Active Directory** no painel esquerdo.
3. Navegue até **Aplicações corporativas** > **Todas as aplicações**.
4. Para adicionar uma nova aplicação, selecione **Nova** aplicação.
5. Na seção Adicionar da galeria, insira ServiceNow na caixa de pesquisa.
6. Selecione ServiceNow no painel de resultados e adicione a aplicação.
7. Aguarde alguns segundos enquanto a aplicação é adicionada ao seu locatário.

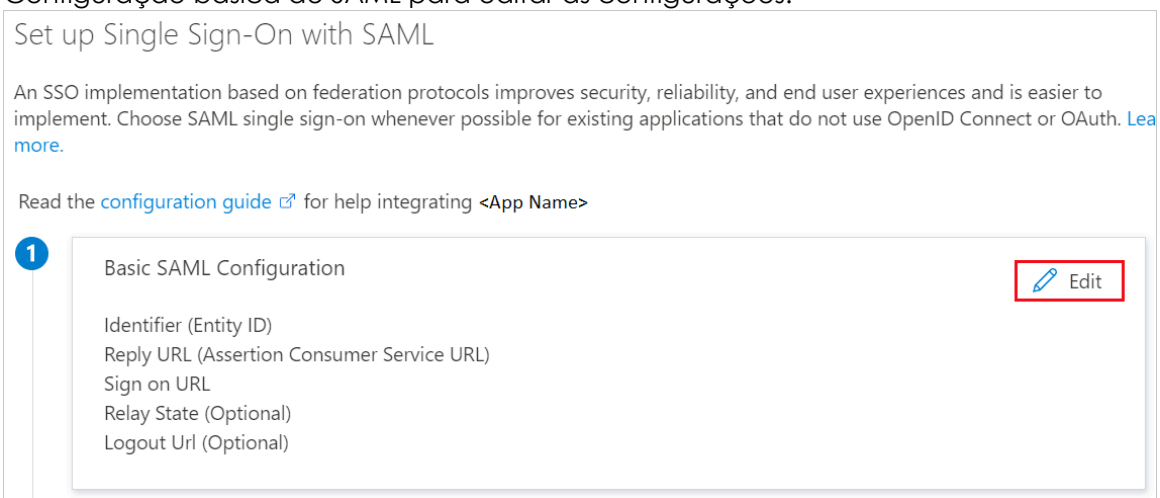
Configuração do SSO do Azure AD

Configure o SSO do Azure AD no portal do Azure.

Antes de Iniciar
Função necessária: Azure admin

Procedimento

1. No portal do Azure, na página de integração de aplicações ServiceNow, localize a seção Gerenciar.
2. Selecione Single Sign-on.
   Na página Selecione um método de Single Sign-on, selecione SAML.
3. Na página Configurar Single Sign-on com SAML, selecione o ícone de caneta para Configuração básica de SAML para editar as configurações.



4. Na seção Configuração básica do SAML, faça o seguinte:

   a. Em **URL de login**, insira um dos seguintes padrões de URL:

```
https://<instancename>.service-now.com/navpage.do
https://<instance-name>.service-now.com/login_with_sso.do?glide_sso_id
=<sys_id of the sso configuration>
```

   Nota: Você precisa fornecer o sys_id deste URL.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

b. No Identificador (ID da entidade), insira um URL com o padrão: `https://<nome-da-instancia>.service-now.com`.

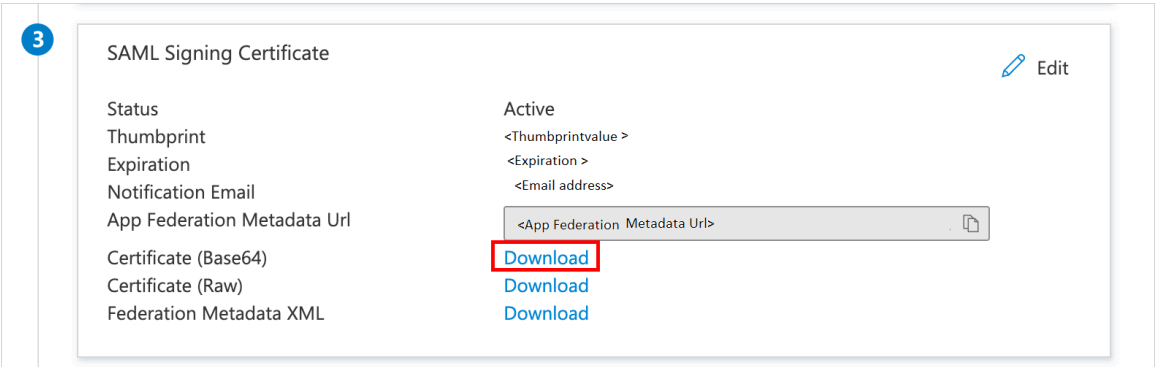
c. Na **URL de resposta**, insira um dos seguintes padrões de URL:

```
https://<instancename>.service-now.com/navpage.do
https://<instancename>.service-now.com/customer.do
```

d. Na URL de logout, insira um URL com o padrão: `https://<nomedainstancia>.service-now.com/navpage.do`

> **Nota:** Você precisa atualizar o URL de logon real, o URL de resposta, o URL de logout e o identificador. Os valores mostrados nesses URLs são para fins de demonstração.

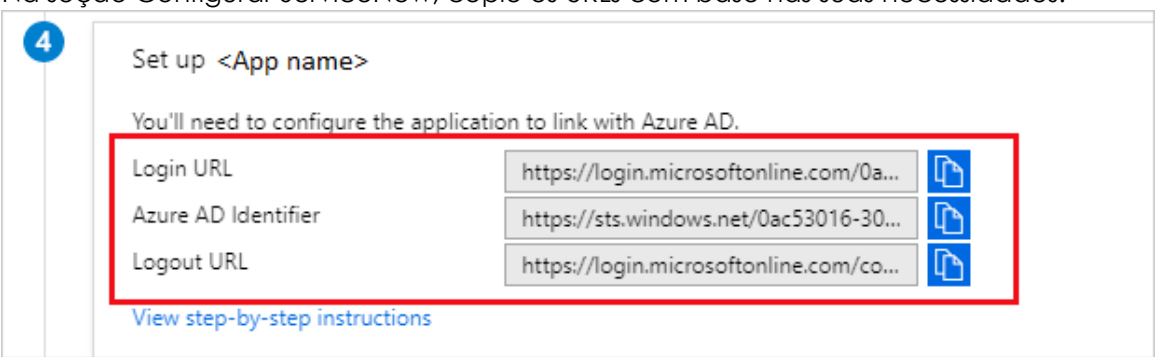
5. Na página Configurar Single Sign-on com SAML, na seção Certificado de assinatura SAML, localize **Certificado (Base64)**.



a. Selecione o botão "Copiar" para copiar o **URL de metadados de federação de app**e cole-o no bloco de notas.
Este URL é necessário para outras configurações.

b. Selecione **"Baixar"** para baixar o Certificado (Base64).

6. Na seção Configurar ServiceNow, copie os URLs com base nas suas necessidades.



Criar um usuário de teste do Azure AD

Crie um usuário de teste no Azure AD.

Antes de Iniciar

Função necessária: Azure admin

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. No portal do Azure, navegue até **Todos** > **Azure Active Directory** > **Usuários** > **Todos os usuários**.
2. Selecione **Novo usuário**.
3. Nas propriedades do usuário, forneça as seguintes informações:
   - Nome
   - Nome de usuário
   - Senha
4. Clique em **Criar**.

Atribuir o usuário de teste do Azure AD

Atribua o usuário de teste do Azure AD criado para usar o Single Sign-on do Azure concedendo acesso a ServiceNow.

Antes de Iniciar
Função necessária: Azure admin

Procedimento

1. No portal do Azure, navegue até **Todos** > **Aplicações corporativas** > **Todas as aplicações**.
2. Na lista de aplicações, selecione ServiceNow.
3. Na página da aplicação, na seção Gerenciar, selecione **Usuários e grupos**.
4. Selecione **Adicionar usuário**.
5. Na janela **Adicionar atribuição**, selecione **Usuários e grupos**.
6. Na janela **Usuários e grupos**, selecione o `usuário de teste` que foi criado a partir da lista de usuários.
7. Escolha a função do usuário atribuído a partir da lista suspensa **Selecionar uma função**, se necessário.
8. Na janela **Adicionar atribuição**, selecione **Atribuir**.

Como configurar o ServiceNow

Configure ServiceNow com os detalhes do Azure AD para usar o SSO.

Antes de Iniciar
Plug-in: `Integração - Instalador do Single Sign-On para vários provedores`

Habilite as propriedades de SSO para vários provedores:

- ◦ Selecione **Habilitar o SSO para vários provedores**.
  - Selecione **Habilitar a Importação Automática de usuários a partir de todos os provedores de identidade para a tabela de usuários**.
  - Selecione **Habilitar registro em log da depuração para integração SSO para vários provedores**.
  - Insira o **e-mail**, o campo da tabela do usuário que…

Função necessária: admin

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegue até **Todos** > **SSO de vários provedores** > **Provedores de identidade**.
2. Na página Provedores de identidade, selecione **Novo**.
3. Na janela Provedores de identidade, selecione **SAML**.
4. Em Importar metadados do provedor de identidade, você pode:
   - **URL**: URL de metadados de federação da aplicação para preenchimento prévio dos detalhes na página de configuração do provedor de identidade.
   - **Importar**: importe o XML para importar os detalhes na página de configuração do Provedor de identidade.
5. Clique com o botão direito do mouse na parte superior da tela, clique em **Copiar sys_id** e use este valor no **URL de login** na seção **Configuração básica do SAML**.
6. No formulário, preencha os campos.

Campos de Single Sign-on de vários provedores

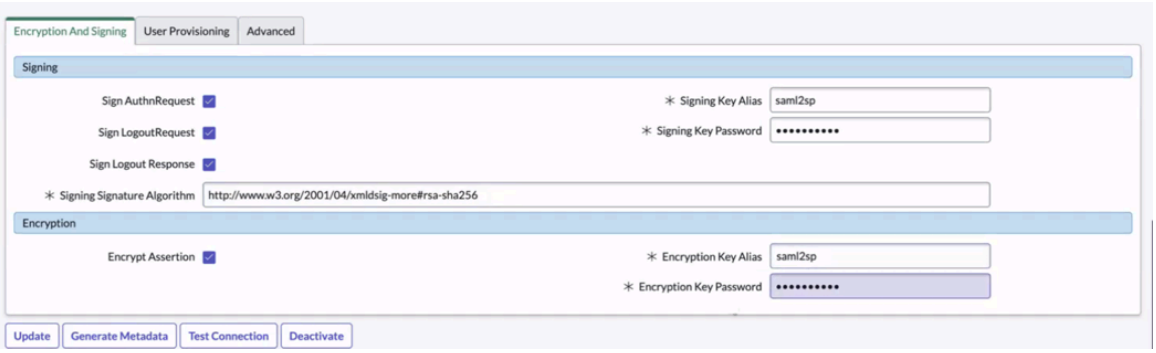
Propriedade	Necessários	Descrição
Nome	Sim	Nome do IdP. Este IdP é a ID do sistema de redirecionamento automático.
Ativo	Sim	Ativo deve ser definido como verdadeiro para o IdP a ser usado para autenticação. **Nota:** A opção para definir esta propriedade é exibida somente após um teste de conexão bem-sucedido.
Padrão	Não	O IdP de redirecionamento automático, anteriormente conhecido como IdP primário, redireciona os usuários automaticamente para que acessem o URL da instância base. Esta propriedade define esta configuração de IdP como padrão.
Redirecionar IdP automaticamente	Não	Configuração de IdP que você pode definir como o IdP de redirecionamento automático. **Nota:** Se você ativar uma nova configuração de IdP de redirecionamento automático, o cookie `glide_sso_id` será atualizado com o novo IdP de redirecionamento automático. A propriedade do sistema `glide.authenticate.sso.update.idp.cookie`, habilitada automaticamente, controla este recurso.
URL do provedor de identidade	Sim	URL para o seu IdP. Cada URL de IdP deve ser exclusivo.
AuthnRequest do provedor de identidade	Sim	URL para a vinculação HTTP-Redirect obtida do elemento SingleSignOnService.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Propriedade	Necessários	Descrição
SingleLogoutRequest do provedor de identidade	Não	URL obtido do elemento SingleLogoutService.
ServiceNow Página inicial	Sim	URL, incluindo a página de login, da instância para a qual o IdP faz a autenticação. Por exemplo: https://yourinstance.service-now.com/navpage.do
ID da entidade/ emissor	Sim	URL base, excluindo a página de login da instância para a qual o IdP faz a autenticação. Por exemplo: https://yourinstance.service-now.com/
URI do público	Sim	URL base, excluindo a página de login da instância para a qual o IdP faz a autenticação. Por exemplo: https://yourinstance.service-now.com/
Política NameID	Sim	Valor do elemento NameIDFormat usado pela integração.
Redirecionamento de logout externo	Não	URL para onde a integração redireciona os usuários após o logout.
Redirecionamento de requisito com falha	Não	URL para redirecionamento de solicitações de autenticação com falha. Por padrão, este é o endpoint do URL de uma página de erro ou página de logout configurada no IdP. É possível preencher este valor no campo glide.authenticate.failed_requirement_redirect.

7. Opcional: Guia Criptografia e assinatura

Nota: Use seus próprios certificados para criptografia e assinatura.



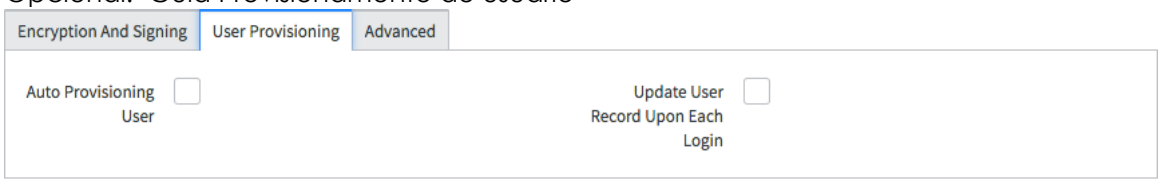
Campos de Criptografia e assinatura

Propriedade	Descrição
Alias das chaves de assinatura/ criptografia	Alias da entrada de chave armazenada no armazenamento de chaves SAML 2.0 SP.
Senha da chave de assinatura	Senha da entrada de chave armazenada no armazenamento de chaves SAML 2.0 SP.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Propriedade	Descrição
Estipulação da criptografia	Caixa de seleção para criptografar a estipulação na resposta do SAML. Os metadados gerados para o IDP incorporam o certificado x509, que o IDP usa para criptografar a estipulação na resposta do SAML gerada por ele.
Algoritmo de assinatura para assinar	URL que aponta para o consumidor de AuthnRequest do provedor de identidade SAML 2.0 para a autenticação de assinaturas eletrônicas.
Assinar AuthnRequest	Caixa de seleção para habilitar o serviço de single sign-on do IdP para receber um AuthnRequest assinado.
Assinar LogoutRequest	Caixa de seleção para habilitar o serviço de single sign-on do IdP para receber um LogoutRequest assinado.

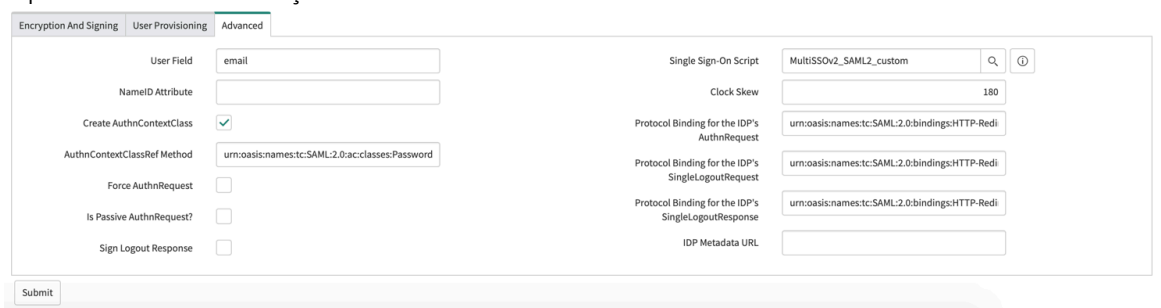
8. Opcional: Guia Provisionamento de usuário



Campos de Provisionamento de usuário

Propriedade	Descrição
Usuário de autoprovisionamento	Provisionamento automático de usuários cria os usuários quando o usuário não existir na tabela Usuário da instância com base nas informações fornecidas pelo IdP.
Atualizar registro do usuário a cada logon	Atualiza as informações do usuário na tabela Usuário da instância com as informações no IdP sempre que o usuário faz login usando SAML.

9. Opcional: Guia Avançado



Campos de Avançado

Propriedade	Descrição
Campo de usuário	Campo na tabela Usuário que contém o valor requerido pelo IdP para identificar o usuário. Esta ID exclusiva faz parte da resposta. Por exemplo, nome de usuário, ID de funcionário e assim por diante. Na tabela Usuário do sistema, esta ID exclusiva corresponde aos detalhes do usuário.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Propriedade	Descrição
Atributo NameID	Campo em branco, a menos que você configure uma nova política NameID. Se você configurar uma nova política, o sistema exigirá a tabela Usuário ser usada para identificar o usuário que faz o login. O sistema corresponde o token NameID ao nome no campo da tabela Usuário.
Criar AuthnContextClass	Caixa de seleção para especificar uma classe de contexto específica, como Transporte protegido por senha. Se a caixa de seleção estiver desmarcada, o IdP selecionará a classe de contexto mais apropriada.
Método AuthnContextClassRef	URN do mecanismo de login a ser usado pelo IdP para a autenticação de usuários.
Forçar AuthnRequest	Caixa de seleção para forçar a ocorrência de AuthnRequests.
A AuthnRequest é passiva?	Marque a caixa de seleção se a AuthnRequest for passiva.
Script de Single Sign-on	Script de Single Sign-on. O padrão é *MultiSSOV2_SAML2_custom*.
Assinar resposta de logout	Detalhes da resposta de logout neste campo.
Distorção do relógio	Número de segundos entre os dois atributos que compõem o nonce SAMLResponse. O padrão é 60. Um SAMLResponse válido deve estar entre os valores de data e hora *notBefore* e *notOnOrAfter*. Consulte a amostra de resposta SAML 2 com os elementos SubjectConfirmation e SubjectConfirmationData e a amostra de resposta SAML 2 com AudienceRestrictions e Audience Elements para obter uma amostra de mensagem SAMLResponse.
A ligação de protocolo para o SingleLogoutRequest do IDP	Um dos valores compatíveis listados no atributo de vinculação do elemento SingleLogoutService.
URL de metadados dos quais as propriedades do IDP são importadas	As propriedades do IdP são importadas deste URL. Se definido, ele habilitará a importação automática do certificado SAML do IdP se o certificado anterior tiver expirado. **Nota:** Se você fizer upgrade da atualização 1 do SAML2 para SSO de vários provedores ou se configurar sua conexão SSO manualmente, o URL de metadados do IdP não será preenchido automaticamente.
Solicitação	ID exclusivo como parte da solicitação. O ID pode ser um nome de usuário, ID de funcionário e assim por diante. **Nota:** A vinculação de redirecionamento e publicação é compatível com a solicitação. A opção de definir este campo é exibida somente após um teste de conexão bem-sucedido. Para obter mais informações, consulte Teste de conexões IdP.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Propriedade	Descrição
Resposta	ID exclusivo como parte da resposta. O ID pode ser um nome de usuário, ID de funcionário e assim por diante. **Nota:** A vinculação de redirecionamento e publicação é compatível com a resposta. A opção de definir este campo é exibida somente após um teste de conexão bem-sucedido. Para obter mais informações, consulte Teste de conexões IdP.

10. Selecione **Testar conexão** no canto superior direito da página.
11. Insira suas credenciais.
    Os resultados de testes de logout do SSO são exibidos.
12. Selecione **Ativar** para ativar a configuração.

Links de e-mail com autenticação externa

Você pode usar links de e-mail ao usar a autenticação externa de token Digest. No entanto, você deve estabelecer como lidar com links em notificações por e-mail.

Os links padrão contêm um URL que direciona você para um local específico na instância, como um incidente ou solicitação de mudança, sem incorporar credenciais de SSO. Você pode ver a seguir exemplos para direcionar o usuário para o local na instância sem fazer login na página de login da instância.

- Técnica HTTP não criptografada para se conectar à instância /demo (ela não navega até o registro específico):

```
https://<instance
 name>.service-now.com/?SM_USER=user_name&DE_USER=lQjIVp7aRJtyPx5+2O/vg
U24tbE=
```

- Link (em uma notificação por e-mail) para um registro específico, assim o usuário acessará primeiro o portal de login da própria empresa:

```
https://login.company_portal_page.com/nav_to.do?uri=incident.do?sys_id=
009f8eda0a0a0b2b01ab4eb094223466%26sysparm_stack=incident_list.do%3Fsys
parm_query=active=true
```

  Você deve definir a propriedade *glide.email.override.url* em sua instância para conter o URL da página do portal da empresa. Se essa propriedade não existir, você poderá criá-la.

- O portal da empresa deve obter esse URL e criar o URL de redirecionamento para a instância, preservando o segmento necessário para acessar o registro específico e adicionando as credenciais de SSO ao final do URL:

```
https://<instance
 name>.service-now.com/nav_to.do?uri=incident.do?sys_id=009f8eda0a0a0b2
b01ab4eb094223466%26sysparm_stack=incident_list.do%3Fsysparm_query=acti
ve=true&SM_USER=user_name&DE_USER=lQjIVp7aRJtyPx5+2O/vgU24tbE=
```

Como adicionar suporte de assinatura eletrônica para SAML

Configure as seguintes propriedades para assinatura eletrônica com a Linguagem de marcação de segurança (SAML) 2.0, atualização 1.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Quando a assinatura eletrônica está ativa com o Multi-SSO, as propriedades do SAML não são usadas. O sistema adiciona propriedades de assinatura eletrônica à tabela "SAML2 Update1 Properties" [saml2_update1_properties]:

Propriedade	Descrição	Padrão
Índice de estipulação do cliente, para autenticação da assinatura eletrônica	Um número de índice que identifica o endpoint.	1
URL de estipulação do cliente, para autenticação da assinatura eletrônica	O URL que identifica o cliente.	`https://yourinstance.service-now.com/consumer.do`
URL do AuthnRequest para autenticação com assinatura eletrônica	O URL para autenticação	nenhum

Se você estiver usando a assinatura eletrônica com o SAML 1.0 ou SAML 2.0 (não incluindo a atualização 1), consulte as instruções de configuração especiais: Assinatura eletrônica com SSO para vários provedores.

Nota: Se você for um Cliente de ciências biológicas que usa assinatura eletrônica, desative a regra de negócio de prevenção contra o autobloqueio de usuário.

Como migrar uma integração SAML 1.1 existente para SAML 2.0

Para migrar de uma integração SAML 1.1 para uma integração SAML 2.0, entre em contato com o suporte ao cliente.

Atualizar sua integração de SAML 2.0 existente

Atualize sua integração de SAML 2.0 existente.

Antes de Iniciar

Função necessária: admin

Por Que e Quando Desempenhar Esta Tarefa

Solicite o plug-in "SAML 2.0 Update 1". Entre em contato com Suporte e atendimento ao cliente para solicitar o plug-in *SAML 2.0 Single Sign-On - Update 1: melhorias de segurança*. O plug-in aplica versões atualizadas da saída de instalação do *SAML2SingleSignon* (script de login), saída de instalação do *SAML2Logout* (script de logout) e inclusão de script do *SAML2* (objeto de script).

Mescle personalizações de scripts de saída de instalação existentes em novos scripts. A atualização salva uma cópia inativa dos scripts de saída de instalação original da integração. Você pode usar essas cópias para mesclar quaisquer personalizações feitas nos scripts de login e logout com as novas versões dessas saídas de instalação.

Mesclar personalizações de scripts de saída de instalação existentes em novos scripts

Nome do script de saída de instalação original	Status do script original	Nome do novo script de saída de instalação	Status do novo script
SAML2SingleSignon	Inativo	SAML2SingleSignon_update1	Ativo
SAML2	Inativo	SAML2_update1	Ativo
SAML2Logout	Inativo	SAML2Logout_update1	Ativo

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você pode navegar até os scripts de saída de instalação de login e logout do SAML 2.0 usando os seguintes caminhos:

- **SAML 2 Single Sign-on** > **Script de login**.
- **SAML 2 Single Sign-on** > **Script de logout**.
- **Definição do sistema** > **Saídas de instalação**.

Você pode navegar até a inclusão de script do "SAML 2.0 Update 1" usando os seguintes caminhos:

- **SAML 2 Single Sign-on** > **Objeto de script**.
- **Definição do sistema** > **Inclusões de script**.

Teste a atualização.

Procedimento

1. Adicione uma propriedade do sistema chamada *glide.authenticate.sso.saml2.debug* com o valor *verdadeiro*.
2. Tente fazer login no SAML 2.0.
3. Revise o log do sistema.
   Os erros de validação do SAML2 começam com o texto *SAML2ValidationError*.
4. Identifique e corrija erros de login típicos.
   Para obter mais informações, consulte Correções e erros de Multi-SSO (SAML 2.0).

Amostra de resposta SAML 2 após a atualização

As seções a seguir ilustram os novos elementos e atributos necessários que o IdP deve fornecer na Resposta SAML.

Amostra de resposta SAML 2 com elemento "Issuer"

A resposta do SAML 2 a seguir usa o elemento *Issuer*.

```
<samlp:Responsexmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
  Destination="https://demoi2.service-now.com/navpage.do"
  ID="s28da6774c88ae1eab292bf25fe625db81919d8e1e"
 InResponseTo="SNC841720c227c81948cfd68cadcad235c6"
 IssueInstant="2012-01-30T20:07:10Z"  Version="2.0"><saml:Issuer
 xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">http://
idp.ssocircle.com</saml:Issuer>
   ...
   <saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
     ID="s2f347f973c063836cf70ea38302d94976f9c5b851"
     IssueInstant="2012-01-30T20:07:10Z"
 Version="2.0"><saml:Issuer>http://idp.ssocircle.com</saml:Issuer>
      ...
   </saml:Assertion></samlp:Response>
```

Amostra de resposta SAML 2 com os elementos "SubjectConfirmation" e "SubjectConfirmationData"

A resposta do SAML 2 a seguir usa os elementos *SubjectConfirmation* e *SubjectConfirmationData* com os atributos *NotOnOrAfter* e *Recipient*.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

```
<saml:SubjectConfirmationMethod="urn:oasis:names:tc:SAML:2.0:cm:bearer"><
saml:SubjectConfirmationData
 InResponseTo="SNC841720c227c81948cfd68cadcad235c6"
     NotOnOrAfter="2012-01-30T20:17:10Z"
 Recipient="https://
demoi2.service-now.com/navpage.do"/></saml:SubjectConfirmation>
```

Amostra de resposta SAML 2 com os elementos "AudienceRestrictions" e "Audience"

A resposta do SAML 2 a seguir usa os elementos *AudienceRestrictions* e *Audience* com os atributos *NotBefore* e *NotOnOrAfter*.

```
<saml:ConditionsNotBefore="2012-01-30T19:57:10Z"
 NotOnOrAfter="2012-01-30T20:17:10Z"><saml:AudienceRestriction><saml:Audi
ence>https://
demoi2.service-now.com</saml:Audience></saml:AudienceRestriction></saml:C
onditions>
```

Provisionamento de usuário do SAML

Se houver usuários em seu IdP, mas não em sua instância, o provisionamento de usuário do SAML poderá criar automaticamente os usuários na tabela "Usuário" [sys_user] da sua instância.

O provisionamento de usuário do SAML é compatível com o SAML 2.0 Update 1 quando o Multi-SSO estiver habilitado.

Como funciona o provisionamento de usuário do SAML

Quando o provisionamento de usuário do SAML está habilitado e o sistema encontra um novo usuário que não está na instância, esta cria automaticamente um registro em uma tabela temporária com o nome `u_imp_saml_user_<suffix>`, sendo que `<suffix>` é um identificador de texto gerado automaticamente. O sistema também cria um mapa de transformação que especifica os relacionamentos de dados entre a tabela de importação e a tabela Usuário. Cada IdP identificado no sistema tem o próprio mapa de transformação, que é criado uma vez para cada IdP. Os administradores podem atualizá-lo conforme necessário.

Quando o usuário faz login, ele acessa um IdP para fazer login.

- O sistema apresenta uma lista de todos os IdPs que podem usar o provisionamento de usuário do SAML. Se houver apenas um IdP que possa usar o provisionamento de usuário do SAML, este será usado automaticamente.
- Se nenhuma das condições acima for verdadeira, o sistema usará o Redirecionamento automático de IdP.

Como administrar o provisionamento de usuário do SAML

Atualize a tabela “Usuário” com os usuários em seu IdP, primeiramente configurando o mapeamento de campo e, em seguida, habilitando o provisionamento de usuário por meio das configurações de IdP Multi-SSO.

Antes de Iniciar

Configure o mapeamento de IdP para identificar quais campos no IdP estão mapeados para os campos corretos na tabela “Usuário”.

Função necessária: admin

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegue até **Todos** > **SSO de vários provedores** > **Propriedades**.
2. Selecione **Habilitar a Importação automática de usuários de todos os provedores de identidade para a tabela Usuário** (*glide.authenticate.multisso.user.autoprovision*) para ativar esse recurso.
3. Clique em **Salvar**.
4. Navegue até **SSO de vários provedores** > **Provedores de identidade**.
5. Abra o registro do provedor de identidade que você quer usar.
6. Para criar um registro na tabela "Usuário" quando o usuário ainda não existir, selecione **Provisionar usuários automaticamente**.
   Se você fez upgrade para esta versão, será necessário configurar o formulário e adicionar este campo.
7. Para permitir que os registros do usuário sejam atualizados quando os usuários fizerem login no IdP e as informações no IdP estiverem desatualizadas com as informações na tabela "Usuário", selecione **Atualizar registro do usuário em cada login**.
   Se você fez upgrade para esta versão, será necessário configurar o formulário e adicionar este campo.
8. Clique em **Mapa de transformação de provisionamento de usuário** para ver o mapa que o sistema criou automaticamente.
9. Faça mudanças no mapa conforme necessário.

Resultados

Quando os primeiros usuários desconhecidos tentarem fazer login, o sistema criará os campos na tabela de conjunto para importação do arquivo metadata.xml.

Nota: Você não poderá mapear os campos da tabela IdP até que este primeiro usuário faça login.

Solução de problemas do SAML 2.0

Antes de entrar em contato com o suporte, tente as soluções de problemas disponíveis na base de conhecimento do Hi.

Nota: A instância não oferece suporte a soluções fornecidas por sites externos.

Consulte o seguinte artigo da base de conhecimento: KB0540617 "'SAML Error Matrix"'.

Outros problemas comuns

Erro ou sintoma	Solução
Mensagem de erro: "não é uma função". Este problema pode ocorrer em um ambiente de vários nós. Se o plug-in não for ativado em todos os nós, será exibido um erro como o seguinte: "org.mozilla.javascript.EcmaError: *[JavaPackage org.opensaml.saml2.core.impl.AuthnRequestBuilder]* não é uma função".	Este erro ocorre porque o plug-in não estava ativo e não carregou o arquivo .jar. Portanto, o código parece estar ausente. Entre em contato com o suporte técnico para reiniciar os nós que não tenham o plug-in.
O SAML não autentica usuários que acessam páginas do CMS.	Por padrão, as páginas do CMS são públicas e, portanto, não exigem

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Outros problemas comuns

Erro ou sintoma	Solução
	autenticação. Se você quiser que o SAML autentique as páginas do CMS, altere a página pública *view_content.do* de *active=true* para *active=false*.
Não é possível redirecionar um usuário de volta para uma página do CMS após a autenticação SAML.	Por padrão, a integração SSO usa um parâmetro de URL chamado *URI* para controlar para onde o usuário é direcionado após a autenticação no IdP. O SSO ignora URLs relativos. Por exemplo, o SSO não pode redirecionar os usuários para um URL relativo */ess*. Em vez disso, o usuário precisa navegar até um URL como */nav_to.do?uri=/ess*, que usa sintaxe de link profundo. No entanto, isso coloca o portal ESS dentro do conteúdo de navegação principal do IFrame. Em outras palavras, o site não ocupa a página inteira, mas sim carrega como uma página em sua instância. Para obter mais informações, consulte CMS Sites e Single Sign-On. Se você alterar a página de entrada do CMS para torná-la privada, definindo *view_content.do* como *active=false*, o comportamento do link profundo exigirá uma personalização do script de login de Saída de instalação. Crie um script que procure a parte do *URI* do URL e crie um parâmetro de URL *RelayState* que contenha o caminho do URL relativo para redirecionar os usuários após a autenticação no IdP.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Outros problemas comuns

Erro ou sintoma	Solução
O SAML não redireciona os usuários para a página apropriada após a autenticação.	Determine se o estado de retransmissão é passado para o IdP e, em seguida, passado de volta durante a autenticação. Você pode fazer isso com um navegador capaz de salvar cabeçalhos de solicitação HTTP e informações de POST, como o Chrome com suas ferramentas de desenvolvedor internas ou o Firefox com o complemento chamado "HTTPfox". Para o Internet Explorer, use um aplicativo de terceiros, como o Fiddler. O objetivo é observar as solicitações passarem do cliente (navegador) para a instância e do cliente para o IdP.

Como monitorar a fila de eventos para atividades de login

Cada integração de single sign-on cria eventos para atividades de login.

Você pode usar esses eventos para monitorar falhas de login e determinar se há problemas de segurança a serem resolvidos.

Monitoramento da fila de eventos para falhas de login

Nome do evento	Descrição	Registro	Parâmetro 1	Parâmetro 2
external.authentication.succeeded	A autenticação externa foi bem-sucedida e o usuário acessou o URL da instância.	ID da sessão	ID do usuário que fez login com sucesso	O URL que o usuário acessou (que pode ser um link profundo)
external.authentication.failed	Os requisitos de single sign-on não estão presentes ou estão faltando.		ID da sessão	Os requisitos de autenticação ausentes
external.authentication.failed	O usuário não existe na tabela Usuário `[sys_user]`		ID do usuário	A cadeia de caracteres "O usuário não existe"

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Monitoramento da fila de eventos para falhas de login

Nome do evento	Descrição	Registro	Parâmetro 1	Parâmetro 2
external.authentication.failed	O usuário está bloqueado.		ID do usuário	A cadeia de caracteres "Usuário bloqueado".

Eventos de login da fila de eventos

A integração SAML 2.0 cria eventos para atividades de login.

Você pode usar esses eventos para monitorar falhas de login e determinar se há problemas de segurança a serem resolvidos.

Eventos de atividades de login

Nome do evento	Descrição	ID usado com o evento	Cadeia de caracteres do evento
saml2.logout.validation.failed	A resposta de logout da validação do IdP falhou em relação à sua solicitação de logout. O evento valida o elemento <inResponseTo> em relação ao ID da sessão (atributo de ID do elemento <saml2p:LogoutRequest>). Por exemplo, consulte o fluxo de trabalho da solicitação de logout emitida.	ID da sessão	A cadeia de caracteres "Falha na validação LogoutResponse do SAML2".
external.authentication.succeeded	Autenticação externa bem-sucedida.		A cadeia de caracteres "Autenticação bem-sucedida"
external.authentication.succeeded	A autenticação externa foi bem-sucedida e o usuário acessou o URL da instância.	ID da sessão e ID do usuário que fez login bem-sucedido	O URL que o usuário acessou (que pode ser um link profundo)
external.authentication.failed	Os requisitos de single sign-on não estão presentes ou estão faltando.	ID da sessão	Os requisitos de autenticação ausentes
external.authentication.failed	O usuário não existe na tabela Usuário [sys_user].	ID do usuário	A cadeia de caracteres "O

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Eventos de atividades de login

Nome do evento	Descrição	ID usado com o evento	Cadeia de caracteres do evento
			usuário não existe"
external.authentication.failed	O usuário está bloqueado.	ID do usuário	A cadeia de caracteres "Usuário bloqueado"

Autenticação de entrada e saída do OAuth

A autenticação baseada em OAuth valida a identidade do cliente que tenta estabelecer uma relação de confiança no sistema usando um protocolo de autenticação.

OAuth 2.0 - Open Authorization é o protocolo padrão do setor para autorização, que se concentra na simplicidade do desenvolvedor do cliente enquanto fornece fluxos de autorização específicos para aplicações da Web, aplicações de desktop e dispositivos móveis.

É um padrão projetado para permitir que um site ou aplicação acesse recursos hospedados por outras aplicações da web em nome de um usuário.

Em vez de usar as credenciais do usuário do recurso para acessar recursos protegidos, o cliente obtém um token de acesso. Os tokens de acesso são emitidos para clientes de terceiros com a aprovação do usuário. Em seguida, o cliente usa o token de acesso para acessar os recursos protegidos.

Entrada

Crie um endpoint para clientes externos que desejam acessar sua instância. Isso cria um registro de aplicação cliente OAuth e gera um ID e segredo do cliente de que o cliente precisa para acessar os recursos restritos na instância. Para obter mais informações, consulte Entrada de OAuth.

Saída

Use um provedor OAuth de terceiros que forneça a autorização de acesso à sua instância. Especifique um perfil OAuth e um escopo OAuth ao se conectar a outro provedor OAuth. Para obter mais informações, consulte Saída de OAuth.

OAuth 2.0

O OAuth 2.0 permite que os usuários acessem recursos da instância por meio de clientes externos, obtendo um token em vez de inserir credenciais de login com cada solicitação de recurso.

Você deve ter a função security_admin para gerenciar a integração do OAuth. Configure o OAuth 2.0 para os seguintes cenários:

- **Cenário de cliente OAuth externo** (entrada): sua instância fornece um endpoint para que os clientes de terceiros extraiam dados da instância.
- **Cenário do provedor OAuth** (saída): sua instância extrai dados de um provedor de terceiros.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Você deve autenticar o usuário pela primeira vez para obter a publicação do token. Não é necessário autenticá-lo usando uma conta de usuário antes da expiração do token.

Tanto as estruturas de segurança simples quanto as estruturas de alta segurança oferecem suporte ao OAuth 2.0. A alta segurança é recomendada. Consulte para obter informações sobre quais versões já têm alta segurança ativa e como ativar a alta segurança.

Principais conceitos da implementação do OAuth 2.0

Conceito	Descrição
Responsável pelo recurso	Uma entidade capaz de conceder acesso a um recurso protegido. Um responsável pelo recurso que seja uma pessoa é chamado de usuário final. O responsável pelo recurso é sempre uma conta de usuário.
Cliente	Uma aplicação que, com a autorização do responsável pelo recurso, faça solicitações de recursos protegidos em nome do responsável pelo recurso.
Servidor de recursos	O servidor que hospeda os recursos protegidos, capaz de aceitar e responder a solicitações de recursos protegidos.
Servidor de autorização	O servidor que emite tokens de acesso para o cliente após a autenticação bem-sucedida do responsável pelo recurso e a obtenção de autorização.
Solicitação de autorização	A permissão exigida por um cliente para acessar um recurso protegido. A solicitação de autorização é sempre uma mensagem HTTP POST que contém o ID de cliente que está agindo em nome do responsável pelo recurso e as credenciais que autorizam a solicitação.
Concessão de autorização	Uma credencial que representa a autorização do responsável pelo recurso para acessar um recurso. A concessão de autorização são credenciais de login do usuário ou um token de atualização.
Token de acesso	Uma cadeia de caracteres segura que um cliente usa para acessar recursos protegidos. Uma instância emite tokens de acesso para clientes que tenham uma concessão de autorização válida. Cada token de acesso tem um escopo, tempo de validade e outros atributos específicos. Por padrão, uma instância emite tokens de acesso com uma vida útil de 30 minutos no cenário em que a instância é o provedor OAuth. Para tokens de terceiros, 30 dias.
Token de atualização	Uma credencial que um cliente usa para obter novos tokens de acesso sem exigir autorização adicional do usuário. Uma instância emite um token de atualização para um cliente quando ele é autorizado a ter um token de acesso. Por padrão, uma instância emite tokens de atualização com uma vida útil de 100 dias no cenário em que a instância é o provedor OAuth. Para tokens de terceiros, 365 dias.
Certificados autoassinados	A Now Platform não oferece suporte a certificados autoassinados. O cliente OAuth não utiliza o armazenamento confiável do certificado nem permite a conexão com endpoints OAuth que incorporam um certificado autoassinado.
Agente do usuário	O usuário que delega direitos de acesso a uma aplicação cliente, que geralmente é um site. Os direitos de acesso permitem que a aplicação

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Conceito	Descrição
	cliente ou o site acesse os dados na instância à qual o usuário tem direitos de acesso. O agente do usuário é usado no cenário.

Tipos de concessão de OAuth

Um tipo de concessão é a maneira como o cliente obtém o token de acesso. Os seguintes tipos de concessão são compatíveis:

- **Código de autorização**: o consumidor primeiro obtém um código de autorização e, em seguida, o usa para obter um token de acesso. Você pode especificar um perfil OAuth e especificar este tipo de concessão. O processo que usa o código de autorização também é conhecido como fluxo de código de autenticação ou fluxo de código de autorização.
- **Credenciais de senha do responsável pelo recurso**: o consumidor do recurso já tem as credenciais do usuário para obter o token de acesso. Este processo também é conhecido como fluxo de senha.
- **Credenciais do cliente**: o consumidor do recurso usa o ID e o segredo do cliente que já estão configurados no registro do aplicativo.

Armazenamento de credenciais de autenticação básica

O segredo do cliente OAuth é armazenado como um campo do tipo *password2*, que é criptografado com KMF. As senhas do usuário, que são usadas para verificar as solicitações de endpoint de entrada, são armazenadas como um valor de hash na tabela Usuário em um campo do tipo *password* (SHA 256). Para obter detalhes sobre essa criptografia, consulte Criptografia de Password2 com KMF.

Configurar OAuth

Configure e ative o OAuth, habilite a propriedade do sistema OAuth, crie um endpoint da aplicação OAuth para que aplicações cliente externos acessem a instância e defina os parâmetros do OAuth.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Verifique se o plug-in OAuth está ativo e se a propriedade de ativação OAuth está definida como verdadeira.
2. Crie um registro de aplicação OAuth usando um dos seguintes métodos:
   - Crie um endpoint para clientes externos que desejam acessar sua instância. Isso cria um registro de **aplicação cliente OAuth** e gera um ID e segredo do cliente de que o cliente precisa para acessar os recursos restritos na instância.
   - Use um provedor OAuth de terceiros que forneça a autorização de acesso à sua instância.

     Especifique um perfil OAuth e Especifique um escopo OAuth ao se conectar a outro provedor OAuth.
3. Configure suas aplicações cliente para criar um HTTP POST que solicite um token OAuth. A aplicação também deve ser capaz de analisar a resposta JSON para usar o token de acesso retornado e o token de atualização.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Ativar OAuth

Por padrão, o plug-in **OAuth 2.0 (com.snc.platform.security.oauth)** está ativo em instâncias novas e com upgrade. Se o plug-in não estiver ativo em sua instância, você poderá ativá-lo.

Antes de Iniciar
Função necessária: administrador

Procedimento

1. Navegue até **Todos** > **Aplicações do sistema** > **Todas as aplicações disponíveis** > **Todas**.
2. Encontre o plug-in usando os critérios de filtro e a barra de pesquisa.

   Pesquise o plug-in pelo nome ou ID. Se não conseguir encontrar um plug-in, talvez seja necessário solicitá-lo ao pessoal ServiceNow.

3. Selecione **Instalar** para iniciar o processo de instalação.

   Nota: Quando a separação de domínio e o administrador delegado estão habilitados em uma instância, o usuário administrativo deve estar no domínio **global**. Caso contrário, será exibido o seguinte erro: `A instalação da aplicação não está disponível porque há outra operação em execução: ativação de plug-in para <plugin name>.`

   Você verá uma mensagem após a conclusão da instalação.

Definir a propriedade OAuth

Para gerar tokens OAuth 2.0 para aplicações registradas, a propriedade `com.snc.platform.security.oauth.is.active` deve estar ativa para a instância.

Antes de Iniciar
Função necessária: administrador

Procedimento

1. Para usar o OAuth 2.0, insira **sys_properties.list** no navegador de filtros do Workspace e, em seguida, clique em **Novo**.
2. Preencha o formulário com as seguintes configurações:

   - **Nome**: com.snc.platform.security.oauth.is.active
   - **Tipo**: verdadeiro | falso
   - **Valor**: verdadeiro

Alterar o parâmetro de senha OAuth

Use esta propriedade para garantir que somente os parâmetros do corpo POST sejam aceitos como entrada para todos os tipos de concessão compatíveis.

O envio de informações confidenciais por meio de parâmetros de consulta de URI pode levar à divulgação de informações confidenciais por parte dos clientes, do servidor ou de qualquer host entre as solicitações. A partir da versão Madrid, essa nova propriedade garante que apenas os parâmetros do corpo POST sejam aceitos como entrada para todos os tipos de concessão compatíveis. Os tipos de concessão compatíveis incluem:

- código de autorização
- senha

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- credencial do cliente
- token de atualização

Propriedade do parâmetro de senha OAuth

Propriedade	Descrição
`glide.oauth.allow.parameters.in.post.body.only`	Esta propriedade é definida como verdadeira somente para zBoots, como parte do plug-in OAuth 2.0. Se você precisar desta configuração para sua instância, crie e defina a propriedade como verdadeira.

Entrada de OAuth

Entrada de OAuth fornece um endpoint para que os clientes de terceiros extraiam dados da instância.

Você deve ter a função `security_admin` para gerenciar a integração do OAuth.

Você pode configurar o **cenário de cliente OAuth externo** (entrada), quando desejar que sua instância forneça um endpoint para que os clientes de terceiros extraiam dados da instância.

Nota: Você deve autenticar o usuário pela primeira vez para obter a publicação do token. Não é necessário autenticá-lo usando uma conta de usuário antes da expiração do token.

Você pode executar a configuração de entrada do OAuth, dependendo dos seguintes tipos de concessão:

- **Fluxo de concessão do código de autorização**: para um fluxo de concessão iniciado pelo usuário, em que o usuário pode configurar uma URL autorizada para autenticação sem precisar digitar o nome de usuário ou a senha, mas sim o token de acesso. Para obter mais informações, consulte Fluxo de concessão de código de autorização OAuth.
- **Fluxo de concessão de senha**: para um fluxo de concessão iniciado pelo usuário, em que a autenticação requer a interação do usuário. Para mais informações, consulte a configuração Fluxo de concessão de senha.

  Nota: Para o fluxo de código de autorização, o usuário precisa concluir a autenticação por login local, SSO ou MFA e fornecer consentimento.

- **Fluxo de concessão de transmissor JWT**: para uma integração entre sistemas em que não é necessária a intervenção do usuário. Para mais informações, consulte a configuração Fluxo de concessão do portador JWT.
- **Fluxo do token de ID**: para usar um token de ID emitido por provedores OIDC terceirizados, como Okta e Azure. Para mais informações, consulte Fluxo do token de ID para autenticação.
- **Concessões implícitas do OAuth**: para permitir que o token de acesso seja fornecido diretamente à aplicação cliente por meio do agente do usuário, que normalmente

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

é o navegador da web ou o dispositivo móvel. Para obter mais informações, consulte Concessões implícitas do OAuth.

- **Credenciais do cliente**: para usar o tipo de concessão de credenciais do cliente do OAuth para integrações de entrada de um cliente de OAuth de terceiro para a plataforma ServiceNow®. Para obter mais informações, consulte Credenciais do cliente.

Escopos do OAuth

É possível pode definir o escopo do suporte de autenticação OAuth à REST API. O escopo do OAuth fornece acesso somente às REST APIs específicas. Para obter mais informações, consulte Escopo de autenticação da REST API.

Fluxo de concessão de código de autorização OAuth

O fluxo de concessão de código de autorização permite que um usuário acesse um recurso autenticando diretamente com um servidor OAuth que confie no recurso, em contraste com a autenticação com credenciais de nome de usuário/senha.

Esta implementação do fluxo de código de autorização OAuth permite o acesso a um recurso via REST. A estrutura do código de autorização obtém o token de acesso por meio do URL autorizado que o usuário configura em vez de exigir que o usuário insira um nome de usuário/senha. O nome de usuário/senha nunca são expostos ao cliente que está solicitando acesso ao recurso.

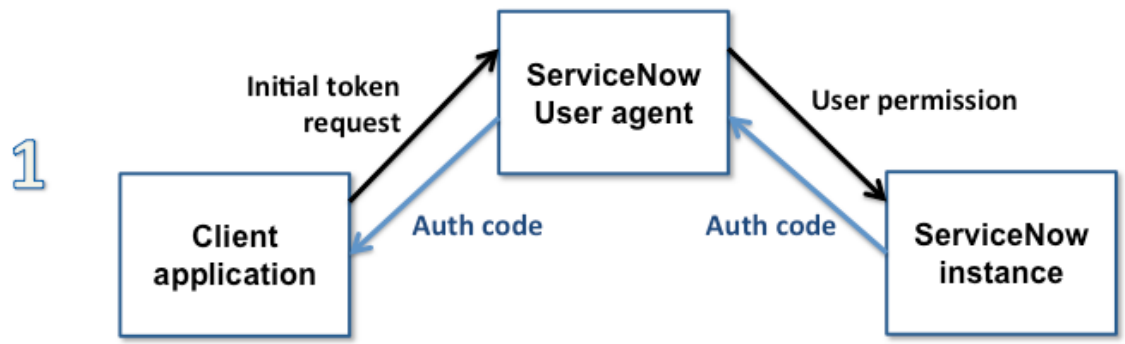
Uma instância da ServiceNow como o servidor de autorização

O servidor OAuth normalmente é um servidor de autorização de terceiros. Você também pode especificar uma instância da ServiceNow como o servidor de autorização que emite os tokens para o fluxo de código de autorização.

O usuário responsável pelo recurso restrito deve autorizar o acesso. O usuário também pode revogar o token de acesso emitido a qualquer momento para encerrar o acesso.

Processo de fluxo de concessão de código de autorização

O processo de fluxo de concessão do código de autorização consiste nestas três etapas:



Na etapa um, a aplicação cliente ou site inicia uma chamada de REST API na forma de uma solicitação GET para a instância por meio do agente do usuário. Normalmente, a chamada REST é iniciada quando o usuário final clica em um botão ou link na aplicação cliente ou site para solicitar um token de acesso. Na aplicação cliente, o usuário final também precisa especificar o URL de autorização, o URL do token, o ID de cliente e o segredo do cliente. Para obter uma explicação desses itens, consulte as descrições dos campos neste tópico: Usar um provedor OAuth de terceiros. Se o cliente solicitar um tipo de concessão, o usuário final deverá selecionar o **Código de autorização**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exemplo de solicitação GET da aplicação cliente para a instância:

```
https://myinstance.service-now.com/oauth_auth.do?response_type=code&redir
ect_uri={the_redirect_url}&client_id={the_client_identifier}
```

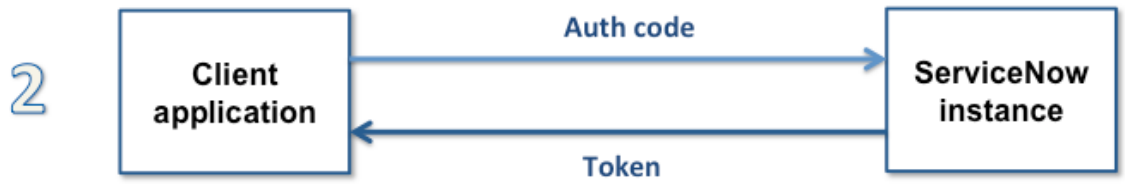
Nota: O **response_type** deve ser um **código** para usar o fluxo de concessão de código OAuth padrão.

O usuário final deve permitir o acesso manualmente ao recurso restrito na instância. Na implementação da ServiceNow, o usuário final deve estar conectado à instância. A instância exibe ao usuário final uma página de IU que tem botões **Permitir** e **Negar**.

O item ao qual a aplicação cliente está realmente solicitando o token é o registro da aplicação do provedor OAuth que você criou, também conhecido como endpoint de autorização (consulte Usar um provedor OAuth de terceiros). O código de autenticação é enviado do endpoint de autorização para o cliente. Ele não vai para o cliente diretamente, mas para o **URL de redirecionamento** que você especifica no formulário de endpoint de autorização. Este URL também é conhecido como URL de retorno de chamada. Você pode obter este URL na aplicação cliente ou no site.

Exemplo de resposta da instância para a aplicação cliente, fornecendo um código de autorização:

```
https/http://{callbackURL}?code={the actual auth code}
```



Agora que a aplicação cliente tem o código de autorização, o cliente usa o código para solicitar o token de acesso. O código de autorização prova que houve consentimento do usuário na etapa 1.

Exemplo de solicitação POST da aplicação cliente para a instância da ServiceNow que fornece o código de autenticação e solicita o token de acesso:

```
https://myinstance.service-now.com/oauth_token.do?grant_type=authorizatio
n_code&code={the auth
 code}&redirect_uri={the_same_redirect_url}&client_id={the_same_client_id
entifier}&client_secret={client_secret_value}
```

O endpoint na instância retorna um token de acesso e um token de atualização. O token de atualização pode ser usado para solicitar tokens de acesso adicionais.

Você pode gerenciar os tokens, incluindo a revogação do token, na instância. Consulte Gerenciar tokens OAuth.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A aplicação cliente usa o token de acesso para autenticar a REST API. Depois de autenticar a aplicação cliente, a REST API retorna os dados solicitados em uma carga JSON.

Exemplo de solicitação GET para a carga JSON de dados para a tabela Incidente [incidente]:

```
https://myinstance.service-now.com/api/now/table/incident?access_token={the_token}
```

Nota: O sistema também é compatível com Concessões implícitas do OAuth, também conhecidas como fluxo de código de concessão implícito.

Suporte à integração

O fluxo do código de autorização é compatível com as seguintes integrações na instância:

- Multi-SSO
- SAML 2.0 Atualização 1
- Autenticação multifator

A interface para celular também é compatível.

Autorizar o acesso a um endpoint OAuth usando o fluxo de código de autenticação

Os usuários finais que possuem um recurso protegido na instância da ServiceNow devem autorizar o acesso ao recurso antes que a instância possa fornecer o token de acesso.

Antes de Iniciar

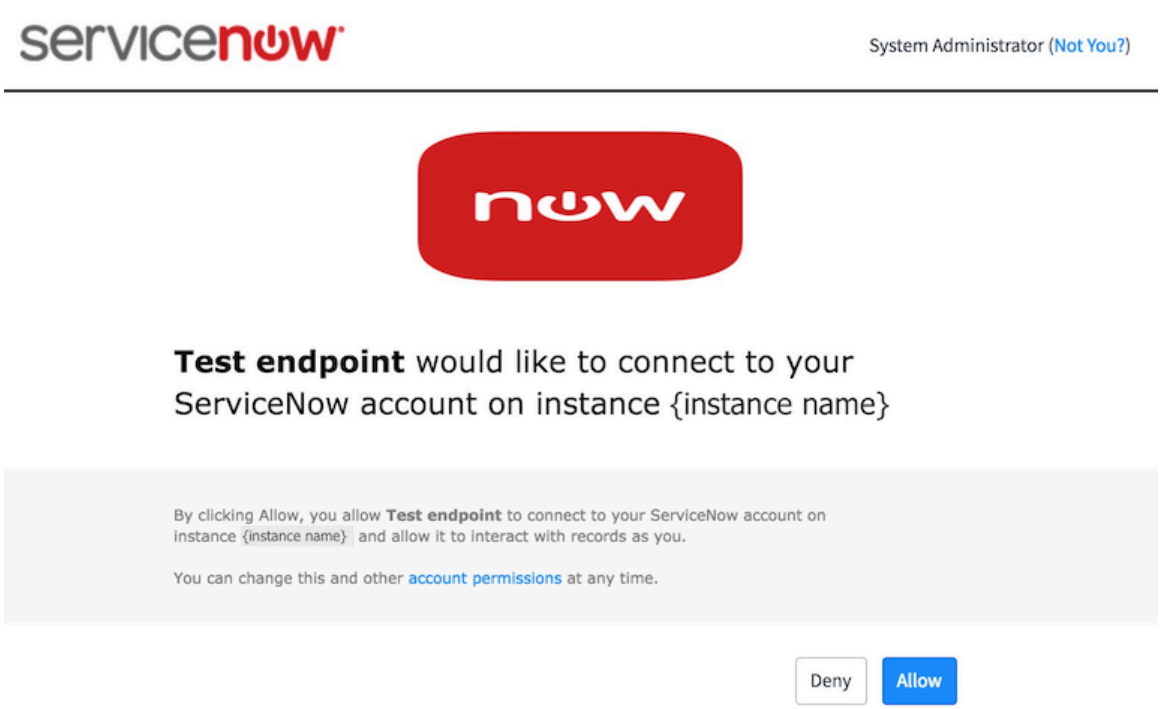
Função necessária: nenhuma Você já deve estar conectado à instância que contém o recurso protegido. Como alternativa, você pode fazer login usando o método de autenticação (como autenticação multifator ou SAML) que o seu administrador da ServiceNow já configurou.

Procedimento

1. Clique no link ou botão no aplicativo cliente em que você está solicitando acesso ao recurso protegido na instância.
   Isso inicia a solicitação de token. Se você estiver fazendo uma chamada REST de uma instância para outra, este link será **Obter token OAuth** no formulário de mensagem REST.
2. Se você não estiver conectado, faça login agora.
   Se você não for o mesmo usuário especificado no canto superior direito, clique em **Não é você?** e faça login.
3. Clique em permissões de conta para abrir a lista de tokens de acesso que você já emitiu. Esta é igual à lista de tokens **Autoatendimento** > **Minhas apps conectadas**.
4. Clique em **Permitir** para permitir o acesso e fazer com que a instância emita o código de autorização (se estiver usando o fluxo de código de autenticação) ou o token de acesso (se estiver usando o tipo de concessão implícita).

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Se você clicar em **Negar**, a autorização não será permitida, mas você não será desconectado da instância.



Uma mensagem que confirma o acesso deve ser exibida. Se você estiver solicitando acesso no formulário de Mensagem REST em uma instância, a seguinte mensagem será exibida na parte superior do formulário: O token de atualização do OAuth está disponível e expirará em {date}.

Requisito de parâmetro de estado de fluxo de código de autorização

A propriedade do sistema glide.oauth.state.paramater.required permite que o parâmetro de estado seja obrigatório em uma solicitação OAuth para o fluxo de código de autorização.

Parâmetro de estado

Função necessária: nenhuma

Começando na versão Madrid, a propriedade do sistema *glide.oauth.state.parameter.required* adiciona um parâmetro de estado para uma solicitação OAuth. Para instâncias zbootadas, a propriedade é verdadeira. Para instâncias atualizadas, a propriedade não está presente, portanto, o parâmetro de estado não está habilitado. O parâmetro de estado é um valor de cadeia de caracteres e não deve conter caracteres especiais. O parâmetro de estado não pode ficar em branco ou “ ”.

Validação do parâmetro de estado

Crie um endpoint para os clientes acessarem a instância. Inicie um fluxo de código de autorização para um oauth_auth.do. Por exemplo:

```
http://myinstance.service-now.com/oauth_auth.do?grant_type=authorization_
code&client_id=e9dba45b380d1300e676ccc91cef468f&response_type=code
```

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Se você não especificar o parâmetro de estado na solicitação, receberá um erro e o código de autorização não será retornado.`Parâmetro de estado ausente na solicitação.`

Adicionar o parâmetro de estado à solicitação:

```
http://myinstance.service-now.com/oauth_auth.do?grant_type=authorization_code&client_id=e9dba45b380d1300e676ccc91cef468f&response_type=code&state=123
```

Adicionar o parâmetro de estado redireciona você para a tela de login e o fluxo do código de autorização regular retorna o código de autorização.

Nota: O URL de resposta contém o parâmetro de estado passado na solicitação. No exemplo, o parâmetro adicionado é `state=123`.

Se o fluxo de código de autorização iniciar em oauth_initiator.do:

```
http://myinstance.service-now.com/oauth_initiator.do?oauth_requestor_context=sys_rest_message&oauth_requestor=eab8341fec0d1300964f214a2c2fcf67&oauth_provider_profile=dfa8f01fec0d1300964f214a2c2fcf51&response_type=code
```

O parâmetro de estado é adicionado automaticamente quando redirecionado por oauth_auth.do.

```
http://myinstance.service-now.com/oauth_auth.do?response_type=code&state=-790938844&redirect_uri=http://10.11.95.5:16001/oauth_redirect.do&client_id=e9dba45b380d1300e676ccc91cef468f
```

Exemplo de fluxo de código de autorização: instância da ServiceNow como servidor de autorização

Você pode usar uma instância como um servidor de autorização para emitir tokens para um cliente usando o fluxo de código de autorização.

Antes de Iniciar

Função necessária: nenhuma

Este exemplo usa duas instâncias: uma como o servidor de autorização e a outra como o cliente. Uma instância usa uma chamada REST para solicitar tokens de outra instância.

Você deve Ativar OAuth em ambas as instâncias.

Procedimento

1. Na instância do servidor de autorização (executando a versão Istanbul ou posterior), navegue até **Sistema OAuth** > **Registro de aplicação** e, em seguida, clique em **Novo**.
2. Clique em **Criar um endpoint da API do OAuth para clientes externos**.
3. Preencha os campos de formulário para o registro da aplicação OAuth conforme descrito em Criar um endpoint para os clientes acessarem a instância.
   A conclusão dessas etapas configura um servidor de autorização. Siga as próximas etapas para configurar o servidor do cliente.
4. Na instância do cliente, navegue até **Sistema OAuth** > **Registro de aplicações** e, em seguida, clique em **Novo**.
5. Clique em **Conectar-se a um provedor OAuth de terceiros**
6. Preencha os campos de formulário para o registro da aplicação OAuth conforme descrito em .
   Observe os seguintes valores de campos:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- **Nome**: Um nome exclusivo que identifica a aplicação para a qual você solicitou acesso ao OAuth.
- **ID de cliente**: ID de cliente do registro de registro do aplicativo que você criou para o servidor de autorização.
- **Segredo do cliente**: [Somente leitura] O ID exclusivo da aplicação, gerado automaticamente. A instância usa o ID de cliente ao solicitar um token de acesso.
- **Tipo de concessão padrão**: selecione **código de autorização**.
- **URL de autorização**: o URL da instância que é o servidor de autorização. Lembre-se de anexar `oauth_auth.do` no final do URL.
- **URL do logotipo**: O URL que contém uma imagem a ser usada como logotipo da aplicação. O logotipo aparece na página de aprovação quando o usuário recebe uma solicitação para conceder acesso a uma aplicação cliente a um recurso restrito na instância.
- **URL do token**: o URL da instância que é o servidor de autorização. Lembre-se de acrescentar `oauth_token.do` no final do URL.
- **URL de redirecionamento**: URL da instância: a instância do servidor cliente. Lembre-se de acrescentar `oauth_redirect.do` no final do URL.

7. Crie um perfil para o registro com o tipo de concessão **Código de autorização**
   O servidor do cliente está configurado. Agora você pode criar uma mensagem de saída do REST e obter um token OAuth.

Criar um endpoint para os clientes acessarem a instância

Crie um endpoint de aplicação OAuth para aplicações cliente externos acessarem a instância da ServiceNow.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Navegue até **Todos** > **Sistema OAuth** > **Registro de Aplicação** e, em seguida, clique em **Novo**.
2. Na página do interceptador, clique em **Criar um endpoint de API do OAuth para clientes externos** e preencha o formulário.

Campo	Descrição
Nome	Um nome exclusivo que identifica a aplicação para o qual você solicitou acesso ao OAuth.
ID de cliente	[Somente leitura] O ID exclusivo da aplicação, gerado automaticamente. A instância usa o ID de cliente ao solicitar um token de acesso.
Segredo do Cliente	[Obrigatório] A cadeia de caracteres do segredo compartilhado que a instância e a aplicação cliente ou site usam para autorizar as comunicações entre si. A instância usa o segredo do cliente ao solicitar um token de acesso. Deixe este campo em branco para que a instância gere automaticamente um segredo do cliente. Para exibir segredos de cliente existentes, clique no ícone do cadeado.
URL de redirecionamento	O URL de retorno de chamada para o qual o servidor de autorização é redirecionado. Insira os URLs completos dos clientes que solicitam

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	acesso ao recurso, anexados por `/oauth_redirect.do`. Por exemplo, `http://token_consumer:port/oauth_redirect.do`. Insira quantos URLs forem necessários para todos os consumidores de token possíveis. A instância corresponde ao URL da solicitação de entrada para um dos URLs de redirecionamento. Se nenhuma correspondência for feita, a instância usará o primeiro URL de redirecionamento.
URL do logotipo	O URL que contém uma imagem a ser usada como logotipo da aplicação. O logotipo aparece na página de aprovação quando o usuário recebe uma solicitação para conceder acesso a uma aplicação cliente a um recurso restrito na instância.
Ativo	Marque a caixa de seleção para ativar o registro da aplicação.
Tempo de vida do token de atualização	O número de segundos que um token de atualização é válido. A instância usa o valor de tempo de vida ao solicitar um token de atualização. Por padrão, os tokens de atualização expiram em 100 dias (8.640.000 segundos).
Impor restrições de token	Selecione para permitir que somente tokens sejam usados com APIs definidas para permitir o perfil de autenticação. Você pode definir a concessão de acesso usando uma política de acesso à API. Para obter mais informações, consulte Criar política de acesso à REST API. Padrão: não selecionado.
Cliente móvel	Representa a entidade para aplicativo para celular ou Web. Essas informações são usadas para analisar as informações de login com celular ou pela web.
Tempo de vida do token de acesso	O número de segundos que um token de acesso é válido. A instância usa o valor de tempo de vida ao solicitar um token de acesso. Por padrão, os tokens de acesso expiram em 30 minutos (1800 segundos).
Comentários	Informações adicionais a serem associadas à aplicação.
Tipo de Cliente	Escolha o tipo de cliente com base no tipo do seu cliente. Opções: ◦ **Iframe integrado** ◦ **Integração como um usuário** ◦ **Integração como um serviço** Para saber mais, consulte Como configurar o tipo de cliente para registros de OAuth e SSO.

3. Clique em **Enviar**.

Resultados

O sistema cria um registro na tabela de registros da aplicação [oauth_entity] com o tipo de cliente OAuth. Quando a instância realmente emite tokens e códigos de autorização, eles são armazenados na tabela. Para obter mais informações, consulte Gerenciar tokens OAuth.

Parâmetros de resposta da API do OAuth

A API do OAuth 2.0 produz uma resposta JSON contendo os seguintes parâmetros como nome: pares de valor.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Parâmetros de resposta do token de acesso

Parâmetro de resposta	Descrição
escopo	Quantidade de acessos concedido pelo token de acesso. O escopo é sempre **useraccount**, o que significa que o token de acesso tem os mesmos direitos que a conta do usuário que autorizou o token. Por exemplo, se Abel Tuter autorizar uma aplicação fornecendo credenciais de login, o token de acesso resultante concederá ao portador do token os mesmos privilégios de acesso que Abel Tuter.
token_type	Tipo de token emitido pela solicitação, conforme definido no OAuth RFC. O tipo de token é sempre **Portador**, o que significa que qualquer pessoa que tenha o token de acesso pode acessar um recurso protegido sem fornecer uma chave criptográfica. Consulte RFC6750 para obter mais informações sobre como o OAuth 2.0 usa tokens de portador.
expires_in	Tempo de vida do token de acesso em segundos.
refresh_token	Valor da cadeia de caracteres do token de atualização.
access_token	Valor da cadeia de caracteres do token de acesso. As solicitações de acesso feitas dentro do tempo de expiração do token de acesso sempre retornam o token de acesso atual.
formato	[Opcional] Formato de saída da resposta. Este valor é sempre JSON.

Nota: Se algum provedor OAuth enviar o corpo da resposta como "tipo de conteúdo" em vez de "Tipo de Conteúdo", o cliente HTTP OAuth poderá não analisar a resposta corretamente. Para corrigir esse problema, crie uma propriedade do sistema usando esses parâmetros.

Campo	Valor
Nome	glide.oauth.inhouse.httpclient.enabled
Tipo	verdadeiro | falso
Valor	falso

Para obter detalhes sobre como criar propriedades do sistema, consulte Adicionar uma propriedade do sistema.

O exemplo a seguir ilustra a cadeia de caracteres JSON retornada por uma solicitação de token de acesso. (Espaços foram adicionados para melhorar a leitura.)

```
{"scope":"useraccount","token_type":"Bearer","expires_in":1800,
"refresh_token":"w599voG89897rGVDmdp12WA681r9E5948c1CJTPi8g4HGc4NWaz62k6k
1K0FMxHW40H8yOO3Hoe",
"access_token":"F0jh9korTyzd9kaZqZ0SzjKZuS3ut0i4P46Lc52m2JYHiLIcqzFAumpyx
shU9mMQ13gJHtxD2fy"}
```

Parâmetros de solicitação da API do OAuth

Saiba mais sobre os parâmetros de solicitação da API do OAuth que acessam as solicitações de token.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: O tipo de conteúdo da API do OAuth deve ser *aplicação/x-www-form-urlencoded*. Um tipo de conteúdo de *aplicação/json* resulta em um erro não especificado.

Parâmetros de solicitação de token de acesso

Parâmetro da solicitação	Descrição
grant_type	[Obrigatório] O tipo de credenciais que autorizam a solicitação de um token de acesso. Este parâmetro deve ter um dos seguintes valores: • **password**: um conjunto de credenciais do usuário para autorizar a solicitação de token de acesso. Especifique as credenciais do usuário nos parâmetros de nome de usuário e senha. • **refresh_token**: um token de atualização existente autoriza a solicitação de token de acesso. Especifique o token de atualização no parâmetro refresh_token.
client_id	[Obrigatório] ID exclusivo gerado automaticamente da aplicação cliente que solicita o token de acesso.
client_secret	[Obrigatório] A cadeia de caracteres do segredo compartilhado que a instância e a aplicação OAuth usam para autorizar as comunicações entre si.
username	Nome da conta do usuário que autoriza a solicitação de token de acesso. Este parâmetro é obrigatório para solicitações de token de acesso com um **grant_type** de **password**.
password	Senha para a conta de usuário que autoriza a solicitação de token de acesso. Este parâmetro é obrigatório para solicitações de token de acesso com um **grant_type** de **password**.
refresh_token	Token de atualização existente que autoriza a solicitação de token de acesso. Este parâmetro é obrigatório para solicitações de token de acesso com um **grant_type** de **refresh_token**.

Solicitações usando credenciais de usuário

A instância exige que os clientes forneçam credenciais de login do usuário ao autorizar o cliente pela primeira vez ou ao autorizar a criação de um novo token de atualização. Este tipo de solicitação sempre retorna dois tokens:

- Um token de acesso
- Um token de atualização

A instância verifica se o usuário está ativo, não está bloqueado no momento e tem uma sessão interativa. Se alguma dessas condições for falsa, a instância não produzirá um token de acesso. As solicitações de acesso feitas dentro do tempo de expiração do token de acesso sempre retornam o token de acesso atual.

Nota: Este tipo de concessão de autorização depende da criptografia TLS para proteger as credenciais do usuário durante a transmissão.

O exemplo a seguir ilustra a solicitação de um token de acesso com um conjunto de credenciais do usuário (espaços foram adicionados para melhorar a leitura).

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

```
$ curl -d"grant_type=password&client_id=be3aeb583ace210011c15b24a43e25d8
&client_secret=client_password
&username=admin&password=admin"
https://instancename.service-now.com/oauth_token.do
```

Solicitações usando um token de atualização

A instância pode usar um token de atualização existente para criar um novo token de acesso. Este tipo de solicitação retorna apenas um token de acesso. A instância confirma que o token de atualização não expirou antes de gerar um novo token de acesso. As solicitações de acesso feitas dentro do tempo de expiração do token de atualização sempre retornam o token de atualização atual. Transmitir tokens de atualização geralmente é mais seguro do que transmitir credenciais de usuário. O exemplo a seguir ilustra a solicitação de um token de acesso com um token de atualização existente (espaços foram adicionados para melhorar a leitura).

```
$ curl
 -d"grant_type=refresh_token&client_id=be3aeb583ace210011c15b24a43e25d8
&client_secret=client_password
&refresh_token=w599voG89897rGVDmdp12WA681r9E5948c1CJTPi8g4HGc4NWaz62k6k1K
0FMxHW40H8yOO3Hoe"
https://instancename.service-now.com/oauth_token.do
```

Como criar um endpoint de API JWT do OAuth para clientes externos (integração entre máquinas)

O token transmissor JWT do OAuth permite que as aplicações da Web de clientes se autentiquem perfeitamente na sua instância usando o tipo de concessão JWT de entrada, em vez de exigir que o usuário final faça login manualmente ou compartilhe a senha.

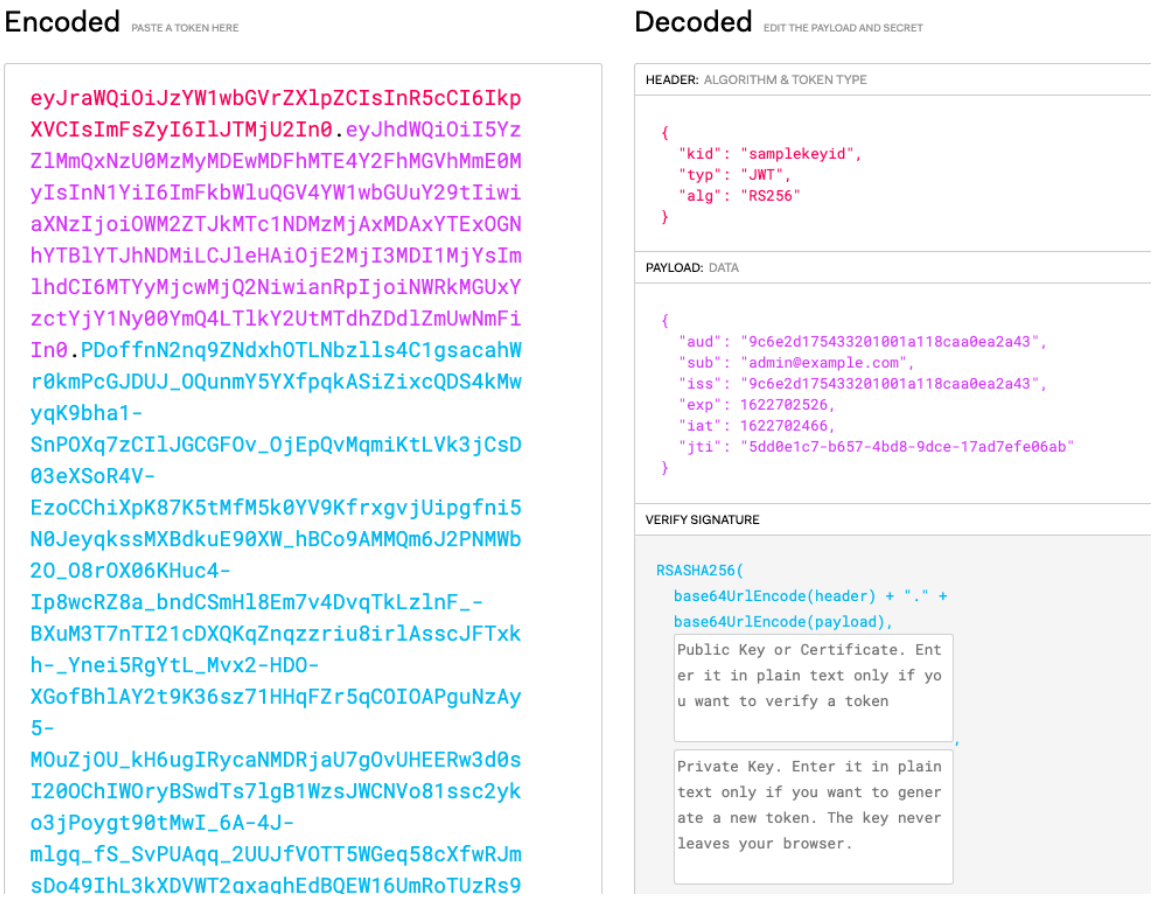
Antes de começar

Gere um JWT (JSON Web Token) com as seguintes declarações no lado do cliente:

- `aud`: deve corresponder ao valor do ID de cliente.
- `sub`: deve ser um identificador de usuário, como o e-mail do usuário ao qual você deseja associar o token.
- `iss`: recomenda-se que corresponda ao valor do ID do cliente. Se `aud` e `iss` não corresponderem, adicione o valor `iss` à validação da declaração.
- `exp`: qualquer expiração desejada.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exemplo de token Web JSON decodificado



Configuração na ServiceNow

Por Que e Quando Desempenhar Esta Tarefa

Já que o uso do tipo de concessão JWT não inclui a senha na solicitação, ele proporciona maior segurança entre os serviços da Web. Por exemplo, é possível desenvolver uma aplicação externa e usar tokens para autenticar solicitações de entrada para sua instância da ServiceNow.

Função necessária: administrador

Para obter mais informações sobre tokens Web JSON, consulte https://jwt.io/.

Procedimento

1. Adicione a chave pública do app cliente à tabela **sys_certificate**.
2. Defina a configuração em sua instância da ServiceNow para verificar o JWT de entrada.

   a. Navegue até **Sistema OAuth** > **Registro de aplicação**.

   b. Selecione **Criar um endpoint da API da OAuth JWT para clientes externos**

   c. Preencha o formulário com informações sobre seu token.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela OAuth JWT

Campo	Descrição
Nome	Um nome exclusivo que identifica a aplicação para o qual você solicitou acesso ao JWT OAuth.
ID de cliente	O ID exclusivo da aplicação, gerado automaticamente. O sistema usa o valor deste campo para recuperar a chave pública ou compartilhada e validar o JWT. O valor deste campo deve corresponder ao valor das declarações do emissor e do público no JWT.
Segredo do Cliente	A cadeia de caracteres do segredo compartilhado que a instância e a aplicação cliente ou site usam para autorizar as comunicações entre si. Deixe este campo em branco para que a instância gere um segredo do cliente automaticamente. Para exibir segredos existentes do cliente, clique no ícone de cadeado. **Nota:** Se for selecionado **Cliente público**, você poderá omitir o **segredo do cliente**.
Campo de usuário	Campo na tabela Usuário (sys_user) que o sistema usa para corresponder ao valor da declaração do assunto no JWT. Por exemplo, se você adicionar um token que tenha um valor de declaração de assunto de nome.usuário@exemplo.com, defina o **campo Usuário** como **E-mail**. Este campo informa ao sistema para pesquisar o campo de e-mail para o valor nome.usuário@exemplo.com e usar o registro de usuário correspondente na solicitação de entrada.
Habilitar a verificação de JTI	Selecione para exigir um novo token a cada troca de token. Padrão: selecionado.
Aplicação	Escopo da aplicação de somente leitura. Este campo é preenchido automaticamente.
Acessível de	Política de acesso entre escopos. Para obter mais informações, consulte Configurações de acesso à aplicação.
Tempo de vida do token de acesso	Quantidade de tempo em que o token é válido. Unidade: segundos
Distorção do relógio	Diferença de tempo permitida entre os relógios do servidor e do cliente ao validar as declarações `exp` e `nbf` no JWT. Unidade: segundos Padrão: 300.
Impor restrições de token	Selecione para permitir somente o uso de tokens com as APIs definidas a fim de ativar o perfil de autenticação. Você pode definir a concessão de acesso usando uma política de acesso à API. Para obter mais informações, consulte Criar política de acesso à REST API.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Padrão: não selecionado.
Comentários	Informações adicionais a serem associadas à aplicação.
Cliente público	Adicione este campo ao formulário se o cliente JWT for público. Ao selecioná-lo, não é necessário incluir um **segredo do cliente**. Padrão: não selecionado.
Tipo de Cliente	Escolha o tipo de cliente com base no tipo do seu cliente. Opções: ▪ **Integrado em iframe** ▪ **Integração como um usuário** ▪ **Integração como um serviço** Para saber mais, consulte Como configurar o tipo de cliente para registros de OAuth e SSO.

d. Salve o formulário.

e. Adicione registros à lista relacionada "Mapas do verificador JWT" para verificar a assinatura do JWT.

Tabela "Mapas do verificador JWT"

Campo	Descrição
Nome	Nome do registro de mapeamento do JWT.
Criança	ID da chave do JWT.
Chave Compartilhada	A chave compartilhada para o ID da chave especificado.
Aplicação	Escopo da aplicação de somente leitura.
Certificado de sistema	Registro de certificado na tabela Certificados X.509 (sys_certificate). O certificado que foi carregado na etapa 1.

f. Adicione quaisquer declarações personalizadas associadas ao seu JWT à lista relacionada de Validações da declaração de JWT do OAuth.

Não é necessário adicionar registros para as seguintes declarações obrigatórias:

- iss
- aud
- sub
- exp

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

- Se `aud` e `iss` não corresponderem, adicione o valor `iss` à validação da declaração.
- Para certificados, é possível adicionar vários mapas de verificador associados a várias chaves.

Tabela Validações de declaração OAuth JWT

Campo	Descrição
Meu cliente externo	Preenchido automaticamente com o registro OAuth JWT.
Tipo de Valor de Declaração	Tipo de dados do valor da declaração.
Nome da declaração	Nome da declaração que você deseja adicionar.
Valor da declaração	Valor da declaração
Aplicação	Escopo da aplicação de somente leitura.

3. Envie uma solicitação cURL contendo o token JWT para obter um token de acesso da sua instância.

Example

A seguir está um exemplo de comando cURL solicitando um token de acesso:

```
$ curl -d"grant_type= urn:ietf:params:oauth:grant-type:jwt-bearer
&client_id=be3aeb583ace210011c15b24a43e25d8
&client_secret=client_password
&assertion=
 eyJraWQiOiJzYW1wbGVrZXlpZCIsInR5cCI6IkpXVCIsImFsZyI6IlJTMjU2In0.eyJhdW
QiOiI5YzZlMmQxNzU0MzMyMDEwMDFhMTE4Y2FhMGVhMmE0MyIsInN1YiI6ImFkbWluQGV4Y
W1wbGUuY29tIiwiaXNzIjoiOWM2ZTJkMTc1NDMzMjAxMDAxYTExOGNhYTBlYTJhNDMiLCJl
eHAiOjE2MjI3MDI1MjYsImlhdCI6MTYyMjcwMjQ2NiwianRpIjoiNWRkMGUxYzctYjY1Ny0
0YmQ4LTlkY2UtMTdhZDdlZmUwNmFiIn0.PDoffnN2nq9ZNdxhOTLNbzlls4C1gsacahWr0k
mPcGJDUJ_OQunmY5YXfpqkASiZixcQDS4kMwyqK9bha1-SnPOXq7zCIlJGCGFOv_OjEpQvM
qmiKtLVk3jCsD03eXSoR4V-EzoCChiXpK87K5tMfM5k0YV9KfrxgvjUipgfni5N0Jeyqkss
MXBdkuE90XW_hBCo9AMMQm6J2PNMWb2O_O8rOX06KHuc4-Ip8wcRZ8a_bndCSmHl8Em7v4D
vqTkLzlnF_-BXuM3T7nTI21cDXQKqZnqzzriu8irlAsscJFTxkh-_Ynei5RgYtL_Mvx2-H
DO-XGofBhlAY2t9K36sz71HHqFZr5qCOIOAPguNzAy5-MOuZjOU_kH6ugIRycaNMDRjaU7g
OvUHEERw3d0sI20OChIWOryBSwdTs7lgB1WzsJWCNVo81ssc2yko3jPoygt90tMwI_6A-
4J-mlgq_fS_SvPUAqq_2UUJfVOTT5WGeq58cXfwRJmsDo49IhL3kXDVWT2gxaqhEdBQEW16
UmRoTUzRs9A9sOm18y3skmOVtnEOm-MlJMFQZ754UMzbiH0ZsMmk1ivCGIjex5J0_lDjKEl
WF5RHGz3YShCoa4JKDZsqYMvIk1SvzyQXjuFqPdS2vzg2m1eKGUwr3m6uNs_HflcDystwVd
MZ7nLlBG4"
https://instancename.service-now.com/oauth_token.do
```

Se o cliente JWT for um cliente público, como o Mobile SDK, você poderá omitir os parâmetros client_id e client_secret da solicitação. A seguir está um exemplo de comando cURL solicitando um token de acesso que omite o client_id e o client_secret:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

```
$ curl -d"grant_type= urn:ietf:params:oauth:grant-type:jwt-bearer
&assertion=
 eyJraWQiOiJzYW1wbGVrZXlpZCIsInR5cCI6IkpXVCIsImFsZyI6IlJTMjU2In0.eyJhdW
QiOiI5YzZlMmQxNzU0MzMyMDEwMDFhMTE4Y2FhMGVhMmE0MyIsInN1YiI6ImFkbWluQGV4Y
W1wbGUuY29tIiwiaXNzIjoiOWM2ZTJkMTc1NDMzMjAxMDAxYTExOGNhYTBlYTJhNDMiLCJl
eHAiOjE2MjI3MDI1MjYsImlhdCI6MTYyMjcwMjQ2NiwianRpIjoiNWRkMGUxYzctYjY1Ny0
0YmQ4LTlkY2UtMTdhZDdlZmUwNmFiIn0.PDoffnN2nq9ZNdxhOTLNbzlls4C1gsacahWr0k
mPcGJDUJ_OQunmY5YXfpqkASiZixcQDS4kMwyqK9bha1-SnPOXq7zCIlJGCGFOv_OjEpQvM
qmiKtLVk3jCsD03eXSoR4V-EzoCChiXpK87K5tMfM5k0YV9KfrxgvjUipgfni5N0Jeyqkss
MXBdkuE90XW_hBCo9AMMQm6J2PNMWb2O_O8rOX06KHuc4-Ip8wcRZ8a_bndCSmHl8Em7v4D
vqTkLzlnF_-BXuM3T7nTI21cDXQKqZnqzzriu8irlAsscJFTxkh-_Ynei5RgYtL_Mvx2-H
DO-XGofBhlAY2t9K36sz71HHqFZr5qCOIOAPguNzAy5-MOuZjOU_kH6ugIRycaNMDRjaU7g
OvUHEERw3d0sI20OChIWOryBSwdTs7lgB1WzsJWCNVo81ssc2yko3jPoygt90tMwI_6A-
4J-mlgq_fS_SvPUAqq_2UUJfVOTT5WGeq58cXfwRJmsDo49IhL3kXDVWT2gxaqhEdBQEW16
UmRoTUzRs9A9sOm18y3skmOVtnEOm-MlJMFQZ754UMzbiH0ZsMmk1ivCGIjex5J0_lDjKEl
WF5RHGz3YShCoa4JKDZsqYMvIk1SvzyQXjuFqPdS2vzg2m1eKGUwr3m6uNs_HflcDystwVd
MZ7nLlBG4"
https://instancename.service-now.com/oauth_token.do
```

A instância retorna o token de acesso em sua resposta:

```
{
    "access_token":
 "KynMY2H0uwWkRc8g8YLXjnQxWbH5_wbnSiLsnaOoKw61GZkkV0ytZP74uF7hJyjfsWfaa
FijqQzq2kcABNJxNA",
    "scope": "useraccount",
    "token_type": "Bearer",
    "expires_in": 1799
}
```

Nota: O tipo de concessão JWT de entrada não inclui tokens de atualização.

4. Faça uma chamada de REST API para acessar um recurso usando o token de acesso.

Example

A seguir está um comando cURL para acessar a tabela de incidentes usando o token.

```
$ curl -H "Authorization: Bearer
 KynMY2H0uwWkRc8g8YLXjnQxWbH5_wbnSiLsnaOoKw61GZkkV0ytZP74uF7hJyjfsWfaaF
ijqQzq2kcABNJxN"
https://instancename.service-now.com/api/now/v1/table/incident
```

Resultados
O sistema recupera o token de acesso na chamada REST e permite o acesso ao recurso solicitado.

Como configurar um provedor de OAuth e OIDC para aceitar token de terceiros

É possível configurar um provedor de OAuth e OIDC para aceitar tokens de identidade gerados por um provedor de OIDC terceirizado usando chamadas de API de entrada com a opção de Single Sign-On (SSO de vários provedores).

Antes de Iniciar
Função necessária: administrador

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

A Now Platform é compatível com o OIDC por meio de nossa implementação de Single Sign-On (SSO) externa, além de chamadas de API de entrada. Para obter um exemplo de configuração de provedor OIDC, consulte Configuração do Azure AD. Para obter um exemplo específico de SSO de uma configuração de provedor OIDC, consulte Criar uma configuração OpenID Connect (OIDC) para Single Sign-On (SSO).

Procedimento

1. Navegue até **Todos** > **OAuth de sistema** > **Registro de aplicações**.
   - Selecione **Novo**, selecione **Configurar um provedor de OIDC para verificar tokens de ID** e preencha o formulário.
   - Selecione um modelo existente para um provedor OIDC (ADFS, Auth0, Azure AD, Google, Okta) e preencha o formulário.

     Nota: Os modelos de provedor OIDC estão disponíveis após o carregamento de dados de demonstração com o plug-in OAuth 2.0.

Campo	Descrição
Nome	Um nome exclusivo que identifica a entidade OAuth OIDC.
ID de cliente	O ID de cliente da aplicação registrado no servidor OAuth OIDC de terceiros. Esse valor deve ser igual ao valor da declaração `aud` no token JWT.
Script do API da OAuth	Um script que você pode usar para personalizar solicitações e respostas para um provedor OAuth externo.
Configuração do provedor OAuth OIDC	É possível usar os provedores de OIDC (ADFS, Auth0, Azure AD, Google, Okta) para validar o token JWT. Selecione o registro da configuração do provedor de OIDC para validar se a **Declaração do usuário** e o **Campo de usuário** estão definidos corretamente. Além disso, certifique-se de preencher os seguintes campos: ◦ **Ativar a verificação de declaração JTI**: quando ativada, a validação de token JWT da ServiceNow também valida o JTI enviado pelo provedor. ◦ **URL de metadados OIDC**: detalhes da configuração conhecida do provedor de OIDC. **Nota:** Se a validação não for verificada, não será possível validar o `jti`, independentemente de estar presente no token JWT. O nome da declaração no token deve ser `jti`.
Distorção do relógio	O número, em segundos, para a restrição ser considerada válida. O padrão é 300.
Impor restrições de token	Selecione para permitir somente o uso de tokens com as APIs definidas a fim de ativar o perfil de autenticação. Você pode definir a concessão de acesso usando uma política de acesso à API. Para obter mais informações, consulte Criar política de acesso à REST API. Padrão: não selecionado.
Ativo	Marque a caixa de seleção para ativar a aplicação OAuth.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Tipo de Cliente	Escolha o tipo de cliente com base no tipo do seu cliente. Opções: ◦ **Iframe integrado** ◦ **Integração como um usuário** ◦ **Integração como um serviço** Para saber mais, consulte Como configurar o tipo de cliente para registros de OAuth e SSO.

2. Selecione **Enviar**.
   O registro é salvo na tabela Registros da aplicação [oauth_entity].
   Quando sua instância emite tokens e códigos de autorização, ela cria um registro na tabela Registros da aplicação [oauth_entity] com o tipo **Provedor OIDC externo**. Para obter mais informações, consulte .
3. Opcional: Vá para a lista relacionada nos perfis de entidade OAuth do registro para validar um perfil padrão gerado pelo sistema para o novo provedor OAuth sem qualquer escopo.
   Você pode mudar ou adicionar um perfil de provedor OAuth, incluindo o nome, o tipo de concessão e o escopo do OAuth.
4. Opcional: Vá para a lista relacionada no registro de Escopos de entidade OAuth para definir todos os escopos OAuth disponíveis para este provedor OAuth.
   Os escopos definidos podem ser selecionados ao criar ou atualizar um perfil. Cada escopo OAuth definido contém um nome e um escopo que você deve obter da especificação do provedor, como um escopo de leitura ou um escopo de gravação. Cada escopo deve ser definido separadamente.
5. Opcional: Vá para a lista relacionada no registro de Provisionamento de usuário para habilitar o provisionamento automático de usuário.

Opção	Descrição
Provisionar usuários automaticamente	Opção para habilitar autenticação forçada para usuários.
Provisionar fonte de dados	A fonte de dados a ser usada para transformar um token OIDC em um usuário da ServiceNow. Use a **Lista de pesquisa** para selecionar o modelo predefinido de fonte de dados e abra o registro para configurar o mapeamento da tabela de transformações. Configurando o mapeamento de transformação, os campos de origem são de *JWT token* e os campos de destino são da tabela *sys_user*.
Funções de usuário aplicadas aos usuários provisionados	Lista de funções de usuário aplicadas aos usuários da ServiceNow recém-provisionados.

Example: Abaixo, há um exemplo de uma solicitação cURL para acionar uma chamada de REST API

Acione uma chamada de REST API.

Execute as seguintes ações:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Registre o app no provedor de OpenID Connect.
- Configure a entidade OIDC do OAuth.
- Configure o provedor de OIDC:

Provedor de OIDC

Provedor de OIDC	Nome do provedor de OIDC.
URL de Metadados OIDC	Especifique a URL de metadados OIDC (URL de configuração conhecida). Essas informações são usadas para obter as chaves públicas para validar o token por meio do endpoint `jwks`.
Declaração do usuário	A declaração que é validada em relação à tabela do usuário.
Campo de usuário	Declaração do usuário que identifica o registro do usuário.
Ativar a verificação de declaração JTI	Quando ativada, a validação do token JWT da ServiceNow também validará o JTI enviado pelo provedor. **Nota:** Se a validação não for verificada, não será possível validar o `jti`, independentemente de estar presente no token JWT. O nome da declaração no token deve ser `jti`. Essas informações são usadas para impedir ataques de repetição.

- Obtenha um token JWT.
- Acione uma chamada de REST API.
  - O token de ID no cabeçalho de autorização para acessar a API da tabela ou os Serviços web com script.

```
curl -X GET --header "Accept:application/json"
 https://<instance_name>.service-now.com/api/now/table/incident/897b04
f2dbd4a300a135364e9d961952 -k
--header "Authorization: Bearer
 eyJraWQiOiJjNTZtZTlXU0xPVnY3UFMwcTg4Qzl1b0lzNjFQYTdmUG4yZFVFOW9RNUg4I
iwiYWxnIjoiUlMyNTYifQ.eyJzdWIiOiIwMHVnZDg1OD
VkczI1WXpUSjBoNyIsIm5hbWUiOiJpbXJhbiBhbGkiLCJsb2NhbGUiOiJlbi1VUyIsImVt
YWlsIjoiaW1yb241NDNAZ21haWwuY29tIiwidmVyIjoxLCJpc3MiOiJodHRwczovL2Rldi
05MzQ
xMjEub2t0YXByZXZpZXcuY29tIiwiYXVkIjoiMG9hZ2Q4bzk3a2lCT3dwd0IwaDciLCJpY
XQiOjE1Mzc5MzMzMjYsImV4cCI6MTUzNzkzNjkyNiwianRpIjoiSUQueThVdXpWNUg2bm1
6SzRs
OTI1RFVrQnJoR1o1MmJzVVpGVHRVTEphQjg3ayIsImFtciI6WyJwd2QiXSwiaWRwIjoiMD
BvZ2Q4NTgycEFqZDZTemcwaDciLCJub25jZSI6InNub3ciLCJwcmVmZXJyZWRfdXNlcm5h
bWUiO
iJpbXJvbjU0M0BnbWFpbC5jb20iLCJnaXZlbl9uYW1lIjoiaW1yYW4iLCJmYW1pbHlfbmF
tZSI6ImFsaSIsInpvbmVpbmZvIjoiQW1lcmljYS9Mb3NfQW5nZWxlcyIsInVwZGF0ZWRfY
XQiOj
```

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

```
E1Mzc5MzAxOTcsImVtYWlsX3Z1cmlmaWVkIjp0cnVlLCJhdXRoX3RpbWUiOjE1Mzc5Mjk2
NjF9.OG87SYxWFgHGlhBYby2H79diRm9rlYZTeEkIINRUatwg-p4739htB8xEY-5_t6yU_
6k5w1
0pdgtt5M5QFZRPXVbQZNoGtY-Bxn0BjaimcFgoWfhY_0ldnGTkzN2RYyIHvrf9-yhxg347
zvczmLrgMMa_VwG4rxrtE6rUXaIpIeIK5b-Deq8ADz8UTUTKpF_5RWk4X-oh5xK6BLniFH
k4ShO
Zq2v_mjproXwKk5euJKrVrar2lQ4adZCOSTRuTf3ThMO5WDh0sel-82LngXtLzRJJ51Iqx
AsXns0kJHLLqLtH1hXNRKfwT1ScQoE_OfWm4t0KryI2j4wSMEanFtLXIw"
```

◦ Se o usuário for autenticado, uma resposta de aplicação/json válida será exibida. Caso contrário, será exibida uma mensagem de erro de usuário não autenticado.

```
User Not Authenticated
{"error":{"message":"User Not Authenticated","detail":"Required to
 provide Auth information"},"status":"failure"}
```

Como configurar o tipo de cliente para registros de OAuth e SSO

Configure o campo **Tipo de cliente** para configurações relacionadas a registros de OAuth e SSO.

Ao estabelecer sessões para vários tipos de login, como IU web (login interativo), integrado em Iframe, incorporado ou integração, você pode configurar o tipo de cliente para os registros OIDC (entidade OAuth), SAML e Digest que são usados para vários logins.

Estas são as opções de tipo de cliente:

- **Integrado em Iframe**: pode ser usado para a instância interativa da ServiceNow que reside em um Iframe em sites de terceiros. Por exemplo, se houver uma tabela confidencial (tabela sys_user - número de telefone do usuário), como administrador, você poderá configurar a ACL com o atributo sec (integrado em Iframe) definido como falso. Isso evitará que o usuário acesse os dados (informações da tabela) na sessão "Integrado em Iframe" do terceiro.
- **Integração como usuário**: pode ser usado para o bot de bate-papo do Virtual Agent que está instalado em apps para desktop, como Slack, Teams, etc.
- **Integração como serviço**: pode ser usado para integração entre máquinas (comunicação entre serviços).

Nota:

- Para OIDC (entidade OAuth): todas as opções estão disponíveis.
- Para SAML e Digest: somente integrado em Iframe. Você deve editar o formulário, adicionar o campo **Tipo de cliente** ao registro e selecionar o tipo de cliente **Integrado em Iframe**.
- Se não selecionar um **Tipo de cliente**, não haverá classificação da sessão.

É recomendável usar o campo "Tipo de cliente" em todos os registros criados para OIDC (entidade OAuth), SAML e Digest. Isso permite que você tenha um controle melhor sobre cada método de login que tem as mesmas configurações, mas que é diferenciado pelo tipo de cliente.

Depois de configurar o campo, sempre que um usuário fizer login a partir da configuração correspondente (OAuth ou SSO), quando a autenticação for bem-sucedida, a sessão será considerada baseada no tipo de cliente configurado e, consequentemente, o tempo limite da sessão será utilizado.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para a sessão atual, incluem-se ou utilizam-se os atributos de segurança correspondentes para impedir que os usuários acessem informações específicas da tabela do tipo de cliente selecionado. Para obter mais informações, consulte Atributos de segurança OOB (prontos para uso).

Tempo limite da sessão para os tipos de cliente

Estas são as propriedades do sistema relacionadas ao tempo limite da sessão para os vários tipos de cliente:

- `glide.session_timeout.iframe_embedded`
- `glide.session_timeout.integration_as_a_user`
- `glide.session_timeout.integration_as_a_service`

Concessões implícitas do OAuth

As instâncias da ServiceNow são compatíveis com a concessão implícita de um token de acesso.

O tipo de concessão implícita, também conhecido como *`implicit grant code flow`*, permite que o token de acesso seja fornecido diretamente à aplicação cliente por meio do agente do usuário, que normalmente é o navegador da Web ou o dispositivo móvel. Nenhum token de atualização é concedido. O usuário final ainda deve conceder acesso ao recurso protegido na instância, assim como acontece com o padrão.

Processo de fluxo de concessão implícita OAuth

Assim como com o processo de fluxo de código de autorização padrão, a aplicação cliente faz uma solicitação para usar o recurso restrito na instância e o usuário final o aprova. A solicitação está na forma de um URL enviado para a instância. O URL deve incluir os seguintes parâmetros:

- `client_id=<the necessary client ID>`. Isso é obrigatório para identificar qual recurso protegido a aplicação cliente deseja acessar.
- `response_type = token`. Isso é obrigatório para solicitar o token de acesso diretamente (em vez de solicitar um código de autorização). O valor deve ser `token` para concessões implícitas. No exemplo de fluxo de código de autorização padrão, o tipo de resposta é `código`.
- `redirect_uri =<a URL>`: o local para onde o token é enviado.

O servidor de autorização envia o token de acesso, em vez de um código de autorização, para a aplicação cliente por meio do agente do usuário.

Aqui está um exemplo de solicitação GET para receber a carga JSON de dados para a tabela Incidente [incidente]:

```
https://myinstance.servicenow.com/oauth_auth.do?response_type=token&redir
ect_uri={the_redirect_url}&client_id={the_client_identifier}
```

Se o usuário conceder acesso, o token será incluído no URL de redirecionamento (retorno de chamada):

```
https/http://{callbackURL}?access_token={the_token}
```

Gerenciar tokens OAuth

Abra os tokens OAuth para fornecer acesso a recursos restritos.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: qualquer usuário ou administrador

Por Que e Quando Desempenhar Esta Tarefa
Os tokens OAuth emitidos pela instância e pelo provedor OAuth de terceiros são armazenados na tabela oauth_credential.

Algumas das colunas importantes nesta tabela:

- Token: valor do token emitido pela instância da ServiceNow.
- Tipo: determina se o token é um token de acesso ou um token de atualização.
- Expira: dados/hora em que o token de acesso ou de atualização expira.
- Token recebido: valor do token emitido por um provedor OAuth de terceiros. Este valor está em formato criptografado.

A expiração e a validade do token são as seguintes:

- Token de acesso: por padrão, uma instância emite tokens de acesso com vida útil de 30 minutos no cenário em que a instância é o provedor OAuth.
- Token de atualização: por padrão, uma instância emite tokens de atualização com uma vida útil de 100 dias no cenário em que a instância é o provedor OAuth.

Procedimento
1. Navegue até uma das seguintes opções de menu:
   - **Autoatendimento** > **Meus aplicativos conectados** para ver os tokens que a instância criou quando você concedeu acesso a um recurso na instância.
   - **Sistema OAuth** > **Gerenciar tokens** para ver todos os tokens. Somente administradores podem acessar este módulo.
2. Clique no **Nome** para abrir o token.
3. Clique em **Revogar acesso** para impedir o acesso ao recurso restrito.

   Você também pode visualizar outras informações sobre o token, incluindo o escopo ao qual ele permite acesso e a data de expiração.

   É possível selecionar o registro **Limpar credenciais expiradas do OAuth** na página "Programação" (`sys.trigger.list`) e configurar o seguinte:

   - **com.snc.platform.security.oauth.is.active**: por padrão, o valor é definido como 0 (verdadeiro).
   - **com.snc.platform.security.oauth.hours.expired.credential.is.kept**: defina o valor com base em seu requisito para determinar o número de horas durante o qual você deseja manter a credencial `oauth` expirada no sistema.
   - **com.snc.platform.security.oauth.day.old.credential.is.kept**: defina o valor com base em seu requisito para determinar o número de dias durante o qual você deseja manter a credencial `oauth` expirada no sistema.

Revogar um token OAuth

Você pode revogar um token de acesso ou atualização do OAuth por motivos de segurança.

Antes de Iniciar
Função necessária: administrador

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

A revogação do token refere-se à situação em que sua instância atua como o servidor de recursos OAuth. Você pode revogar o token por meio de um URL ou por .

Procedimento

Acesse sua instância usando `oauth_revoke_token.do` e acrescente o token de acesso ou de atualização.

Por exemplo: `https://[Sua_Instância_ServiceNow]:[porta]/oauth_revoke_token.do?token=[token de acesso ou atualização]` sem os colchetes `[ ]`.

Resultados

Este acesso de endpoint não exige autenticação. O token nesta solicitação está marcado como expirado.

Credenciais do cliente

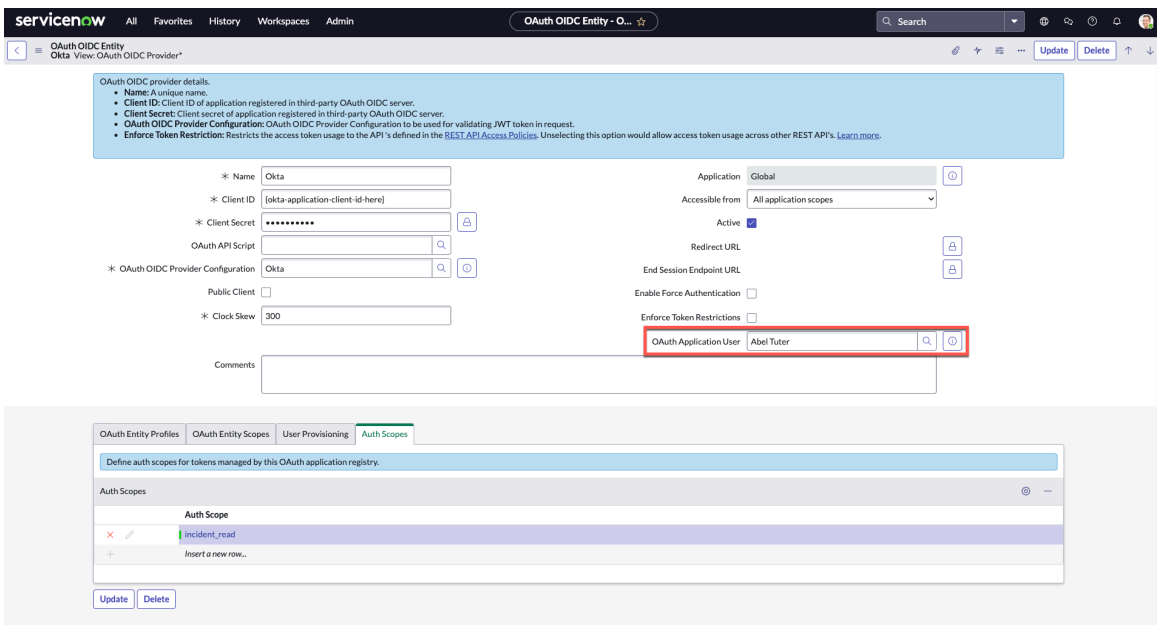
Use o tipo de concessão de credenciais do cliente do OAuth para integrações de entrada de um cliente de OAuth de terceiros para a plataforma ServiceNow®.

Os administradores podem usar o tipo de concessão de credenciais do cliente (CC) para habilitar a integração de um cliente OAuth de terceiros para a plataforma ServiceNow.

O tipo de concessão de credenciais do cliente de entrada é um recurso que pode ser controlado por uma propriedade do sistema. Por padrão, a propriedade do sistema está definida como falsa.

Para usar o tipo de concessão de credenciais do cliente, execute as seguintes etapas:

- Crie a propriedade de sistema `glide.oauth.inbound.client.credential.grant_type.enabled`.
- Adicione o campo **Usuário da aplicação OAuth** ao formulário da Entidade OAuth.



© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Criar propriedade do sistema Credenciais do cliente

Crie a propriedade de sistema `glide.oauth.inbound.client.credential.grant_type.enabled` para usar o tipo de concessão de Credenciais do cliente para integrações de entrada de OAuth.

Antes de Iniciar

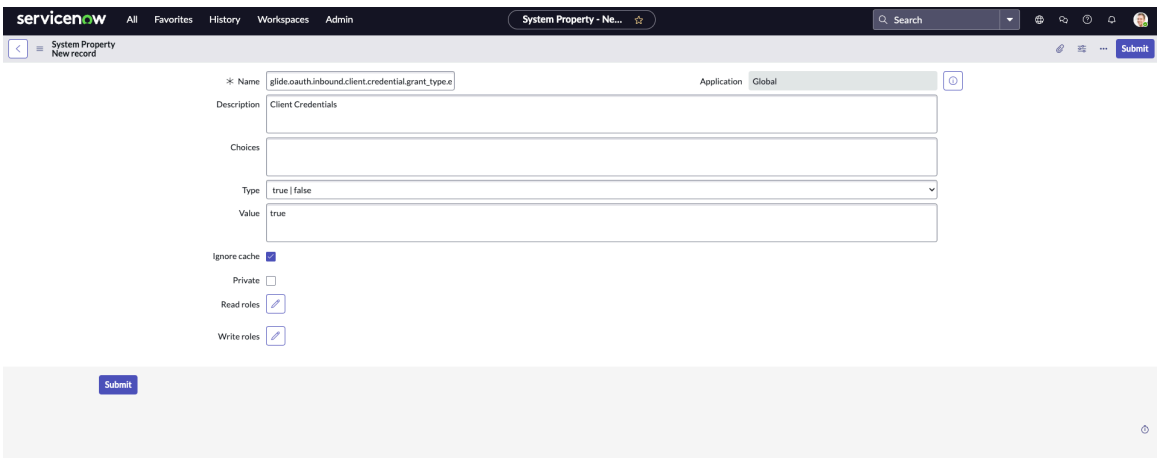
Função necessária: administrador

Plug-in necessário: OAuth 2.0.

Procedimento

1. No filtro de navegação, insira `sys_properties.list`.
   A lista inteira de propriedades na tabela Propriedades do sistema [sys_properties] é exibida.
2. Selecione **Novo**.
3. Preencha os campos a seguir no formulário.

Campo	Descrição
Nome	Nome da propriedade que você está criando. Nesse caso, `glide.oauth.inbound.client.credential.grant_type`
Descrição	Insira um resumo, uma frase que descreva a função da propriedade.
Tipo	Selecione o tipo de dado apropriado na lista. Nesse caso, `verdadeiro | falso`.
Valor	Defina o valor desejado para a propriedade. Nesse caso, `verdadeiro` para habilitar o tipo de concessão de credenciais do cliente para integrações de entrada do OAuth.



Nota: Você pode configurar outros campos no formulário, como Opções, Ignorar cache, Privado, Funções de leitura e Funções de gravação, de acordo com seus requisitos.

4. Selecione **Enviar**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Se a caixa de seleção **Ignorar cache** estiver marcada, o sistema limpará o cache do servidor quando o parâmetro for alterado.

Em seguida, você deve criar um cliente OAuth (endpoint de API do OAuth para cliente externo) e adicionar o campo Usuário da aplicação OAuth ao registro do cliente OAuth.

Adicionar usuário da aplicação OAuth

Adicione o campo Usuário da aplicação OAuth ao formulário de Entidade OAuth para usar o tipo de concessão de Credenciais do cliente para integrações de entrada de OAuth.

Antes de Iniciar

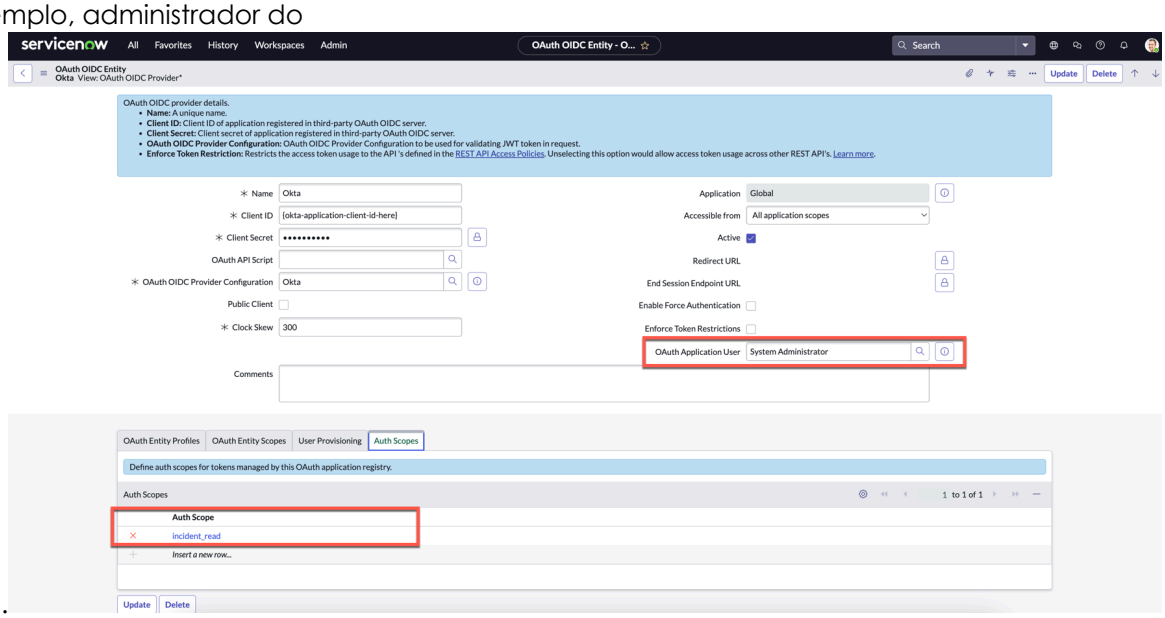
Função necessária: administrador

Plug-in necessário: OAuth 2.0.

Você deve criar um cliente OAuth. Para obter mais informações, consulte Criar um endpoint para os clientes acessarem a instância.

Procedimento

1. Abra o registro de cliente OAuth que foi criado.
2. Selecione o ícone de mais opções no cabeçalho da página.
3. Selecione **Configurar** > **Design de formulário**.
4. Na página Design de formulário, adicione **Usuário da aplicação OAuth** na lista de campos.
5. Salve ou atualize o formulário.
6. Selecione o usuário para o **Usuário da aplicação OAuth**.
   Por exemplo, administrador do sistema.



Nota: Você deve usar o Escopo de autenticação da REST API com o tipo de concessão de credenciais do cliente para controlar o acesso fornecido ao cliente de terceiros.

7. Salve ou atualize o formulário.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Qualquer solicitação de autorização com o **Tipo de concessão** como **Credenciais do cliente**, **ID de cliente** e **Segredo** será aprovada para o Usuário da aplicação OAuth associado na ServiceNow®.

Nota: Se o Usuário da aplicação OAuth não estiver selecionado no registro do cliente OAuth ou a propriedade Credenciais do cliente estiver definida como `falso`, a solicitação de autorização não será aprovada.

Saída de OAuth

A saída de OAuth permite que você extraia dados de um provedor de terceiros para sua instância.

Você deve ter a função security_admin para gerenciar a integração do OAuth.

Você pode configurar o OAuth 2.0 de saída para os seguintes tipos de concessão:

- **Conectar a um provedor de terceiros**: use o ID e o segredo do cliente para enviá-los ao provedor OAuth. Para obter mais informações, consulte Conectar-se a um provedor OAuth de terceiros.
- **JWT Bearer**: um servidor de autorização valida um token JWT, que habilita informações de identidade e segurança a serem compartilhadas entre domínios de segurança. Para obter mais informações, consulte Configurar provedor OAuth com tipo de concessão de Transmissor JWT.
- **SAML2 Bearer**: gera a estipulação SAML2 e, em seguida, troca com o provedor a estipulação para os tokens de acesso.

  Nota: Para solicitações de saída para SuccessFactors, use o **SAML2 Bearer** como tipo padrão de concessão. Para saber mais sobre como configurar o **Portador do SAML2**, consulte o exemplo em Configurar v4.xx.

- **Código de autorização**: o código fornecido ao cliente para obter um token de acesso, que é então usado para ter acesso ao recurso. Se você selecionar essa opção, precisará de um URL de autorização (o URL do servidor de autorização).
- **Credenciais de senha do responsável pelo recurso**: nome de usuário e senha do usuário tentando obter acesso ao recurso.
- **Credenciais do cliente**: ID do cliente e segredo do cliente, ambos usados para obter o token de acesso. Esse método não fornece atualização de tokens.

Você pode configurar o **cenário do provedor OAuth** (saída): sua instância extrai dados de um provedor de terceiros.

Nota: Você deve autenticar o usuário pela primeira vez para obter a publicação do token. Não é necessário autenticá-lo usando uma conta de usuário antes da expiração do token.

Conectar-se a um provedor OAuth de terceiros

Configure como o ID e o segredo do cliente são enviados para o provedor OAuth.

Antes de Iniciar
Função necessária: administrador

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegue até **Todos** > **Sistema OAuth** > **Registro de Aplicação** e, em seguida, clique em **Novo**.
2. Na página do interceptador, clique em **Conectar-se a um provedor OAuth de terceiros** e preencha o formulário.

Campo	Descrição
Nome	Nome exclusivo da conexão OAuth de terceiros.
ID de cliente	O ID de cliente da aplicação registrado no servidor OAuth de terceiros.
Segredo do cliente	O segredo do cliente da aplicação registrado no servidor OAuth de terceiros.
Script do API da OAuth	O script usado para personalizar a solicitação e a resposta ao provedor OAuth externo.
URL de logotipo	O URL de logotipo da aplicação OAuth.
Tipo de concessão padrão	O tipo de concessão padrão usado para estabelecer o token. As opções incluem: ◦ **Código de autorização**: o código fornecido ao cliente para obter um token de acesso, que é então usado para ter acesso ao recurso. Se você selecionar essa opção, precisará de um URL de autorização (o URL do servidor de autorização). ◦ **Credenciais de senha do responsável pelo recurso**: nome de usuário e senha do usuário tentando obter acesso ao recurso. ◦ **Credenciais do cliente**: ID do cliente e segredo do cliente, ambos usados para obter o token de acesso. Esse método não fornece atualização de tokens. ◦ **JWT Bearer**: um servidor de autorização valida um token JWT, que habilita informações de identidade e segurança a serem compartilhadas entre domínios de segurança. ◦ **SAML2 Bearer**: gera a estipulação SAML2 e, em seguida, troca com o provedor a estipulação para os tokens de acesso. **Nota:** Para solicitações de saída para SuccessFactors, use o **SAML2 Bearer** como tipo padrão de concessão.
Tempo de vida do token de atualização	Tempo, em segundos, em que o token de atualização é válido. O tempo padrão é 8.640.0000 segundos.
Cliente público	Permite que clientes públicos exijam o PKCE para uma autorização. **Nota:** Você pode usar somente o código de autorização como *Default Grant type* quando o PKCE estiver habilitado.
Método de desafio do código	Método de desafio do código usado no fluxo de trabalho PKCE do OAuth As opções incluem:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	◦ S256 [Padrão] ◦ Simples ◦ Nenhum
Comentários	Adicione comentários sobre o aplicativo OAuth.
Aplicação	Aplicação e escopo que contenham este registro.
Acessível de	Torne este aplicativo acessível a partir de todos os escopos de aplicativo ou somente a partir deste escopo.
Ativo	Marque a caixa de seleção para ativar o aplicativo.
URL de Autorização	O endpoint do código de autorização OAuth.
URL do token	O endpoint do token do servidor OAuth.
URL de revogação do token	O endpoint de revogação de token do servidor OAuth.
URL de redirecionamento	O endpoint de retorno de chamada do OAuth Se estiver em branco, a instância gerará uma entrada automaticamente.
Usar autenticação mútua	Marque a caixa para usar autenticação mútua para solicitação e revogação de token. Este recurso exige que um perfil de autenticação mútua seja especificado.
Enviar credenciais	O cliente OAuth preenche as credenciais do cliente na solicitação: ◦ No corpo das solicitação (formulário codificado em URL) ◦ Cabeçalho de autorização básica ◦ Como chave privada JWT
Tipo de Cliente	Escolha o tipo de cliente com base no tipo do seu cliente. Opções: ◦ **Iframe integrado** ◦ **Integração como um usuário** ◦ **Integração como um serviço** Para saber mais, consulte Como configurar o tipo de cliente para registros de OAuth e SSO.

O sistema cria um registro na tabela Registros da aplicação [oauth_entity] com o tipo Provedor OAuth.

3. Opcional: Vá para a lista relacionada nos perfis de entidade OAuth do registro para validar um perfil padrão gerado pelo sistema para o novo provedor OAuth sem qualquer escopo.
   Você pode mudar ou adicionar um perfil de provedor OAuth, incluindo o nome, o tipo de concessão e o escopo do OAuth.
4. Opcional: Vá para a lista relacionada no registro de Escopos de entidade OAuth para definir todos os escopos OAuth disponíveis para este provedor OAuth.
   Você pode selecionar os escopos ao criar ou atualizar um perfil. Cada escopo OAuth contém um nome e um escopo que você deve obter da especificação do provedor, como um escopo de leitura ou um escopo de gravação. Cada escopo deve ser definido separadamente.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Transmissor JWT

Os JSON Web Tokens (JWTs) habilitam o recurso de configurar interações de API de servidor para servidor entre ServiceNow e provedores de API externos sem exigir qualquer intervenção do usuário.

A concessão do portador do JSON Web Token (JWT) é uma cadeia de caracteres JSON que contém valores de declaração que são avaliados e validados pelos manipuladores de concessão JWT no final do servidor de autorização, antes de emitir um token de acesso.

Usando o tipo de concessão de portador JWT, você pode configurar o fluxo de concessão de portador OAuth 2.0 JWT para mensagem de REST de saída.

Configurar provedor OAuth com tipo de concessão de Transmissor JWT

Os JSON Web Tokens (JWTs) habilitam o recurso de configurar interações de API de servidor para servidor entre ServiceNow e provedores de API externos sem exigir qualquer intervenção do usuário. Este suporte habilita o Integration Hub ou outras tarefas automatizadas usando JWTs para configurar integrações de API e serviço com diferentes provedores.

Antes de Iniciar
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa
As tarefas a seguir mostram como a ServiceNow pode ser configurada para usar JWTs para autenticação de cliente OAuth 2.0 e concessões de autorização. A ServiceNow é o cliente OAuth e você pode configurar um provedor OAuth, como o Box ou o Docusign.

Procedimento

1. Carregar certificado Java KeyStore
   Anexe um certificado JKS à sua instância para usar para habilitar a autenticação do cliente JWT.
2. Configurar uma chave de assinatura JWT
   Crie uma chave de assinatura JWT para atribuir ao seu certificado Java KeyStore (JKS).
3. Criar um provedor JWT com uma chave de assinatura JWT
   Adicione um provedor JWT à sua instância da ServiceNow.
4. Conectar-se a um provedor OAuth de terceiros
   Crie um provedor OAuth de terceiros com um Transmissor JWT como o tipo de concessão padrão no Registro de aplicação da ServiceNow.
5. Especificar um perfil OAuth
   Abra o perfil de entidade OAuth do provedor OAuth e atribua um provedor JWT.

Carregar certificado Java KeyStore

Você pode anexar um certificado Java KeyStore (JKS) à sua instância para usar para habilitar a autenticação do cliente JWT.

Antes de Iniciar
Função necessária: administrador

Procedimento

1. Navegue até **Todos** > **SSO de vários provedores** > **Certificado x509**.
2. Preencha o formulário conforme necessário.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
Nome	Um nome exclusivo para o seu certificado.
Notificar no vencimento	Designe quem notificar quando o certificado expirar.
Aviso emitido antes do vencimento (em dias)	Envie uma notificação por e-mail ao seu gerenciador de certificados antes que seu certificado expire.
Ativo	Habilita o certificado a ser usado para solicitações de token.
Tipo	O tipo de certificado que você está carregando.
Dias até o vencimento	A quantidade de dias até que o certificado expire.
Senha do armazenamento de chaves	A senha associada ao certificado.
Descrição resumida	

3. Clique em **Enviar**.

Configurar uma chave de assinatura JWT

Crie uma chave de assinatura JSON Web Token (JWT) para atribuir ao seu certificado Java KeyStore (JKS).

Antes de Iniciar

Função necessária: administrador

Nota: Se você quiser adicionar o **Impressão digital SHA-1 do certificado X.509 (x5t)** ao cabeçalho como parte da chave JWT, deverá configurar o formulário e adicionar o campo **Impressão digital SHA-1 do certificado X.509 (x5t)**.

Procedimento

1. Navegue até **Todos** > **OAuth do Sistema** > **Chaves de JWT**.
2. Preencha o formulário conforme necessário.

Opção	Descrição
Nome	Um nome exclusivo para configuração da sua assinatura de chave JWT.
Armazenamento de chaves de assinatura	O armazenamento de chaves designado ao assinar o JWT.
ID da chave	O ID da chave (secundária) ajuda a identificar qual chave é usada quando várias chaves são usadas para assinar tokens.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	Nota: Se você configurar este campo, a declaração do ID da chave será incluída no JWT. Se você não configurar este campo, seu JWT não terá uma declaração de ID da chave.
Algoritmo de assinatura	O algoritmo a ser usado para assinar com a chave JWT. RSA 256 é o único algoritmo disponível.
Senha da chave de assinatura	A senha associada à chave de assinatura.
Ativo	Designe que o alias da chave JWT seja referenciado ativamente de um provedor JWT.

3. Clique em **Enviar**.

Criar um provedor JWT com uma chave de assinatura JWT

Adicione um provedor JSON Web Token (JWT) à sua instância da ServiceNow.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Navegue até **Todos** > **Sistema OAuth** > **Provedor JWT**.
2. Preencha o formulário e clique em **Enviar**.

Opção	Descrição
Nome	Um nome exclusivo para configuração do seu provedor JWT.
Intervalo de vencimento (s)	A vida útil dos tokens, em segundos, gerados pelo provedor JWT.
Configuração de Assinatura	Configuração de assinatura JWT da ServiceNow a ser aplicada.

Gerar um Token Web JSON (JWT)

Crie um Token Web JSON (JWT) para representar declarações com segurança entre duas partes na Now Platform.

A API GlideJWT é uma API passível de script com escopo que gera um JWT. Há três argumentos necessários antes de gerar o JWT:

- Sys_id do ProvedorJWT
- Cabeçalho JSON serializado
- Carga JSON serializada

Há dois scripts da API do JWT, JWTTokenInternal e JWTTokenRestricted, que você pode usar ao configurar um Provedor JWT. O script JWTTokenRestricted permite que os administradores

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

configurem quem pode gerar um JWT. O script JWTTokenInternal é somente leitura e permite que somente usuários conectados gerem um JWT.

Para gerar um JWT:

- Crie uma chave JWT com uma chave compartilhada (HMAC) ou um armazenamento de chaves de assinatura (RSA)
- Associe um provedor JWT à configuração de assinatura que faz referência a uma chave JWT

Você pode usar a API para criar seu token.

Você pode usar declarações padrão e personalizadas ao configurar um provedor JWT. Você pode passar cabeçalho dinâmico e declarações de carga como parte da assinatura da API generateJWT.

Script de exemplo para testar a API:

```
var jwtAPI = new sn_auth.GlideJWTAPI();
var headerJSON = {  "kid": "a1234"  };
var header = JSON.stringify(headerJSON);

var payloadJSON = { "jti": "testjti", "iss": "testiss", "sub":
 "testsub" };
var payload = JSON.stringify(payloadJSON);

var jwtProviderSysId = "7a40dde2d5303300964fb7c8f3c14ab5";
var jwt = jwtAPI.generateJWT(jwtProviderSysId, header, payload);

gs.info("JWT:" + jwt);
```

APIs do cliente OAuth

A API do cliente OAuth fornece métodos para solicitar e revogar tokens OAuth.

O cliente OAuth fornece estas classes:

- GlideOAuthClient : métodos para solicitar e revogar os tokens de atualização e acesso.
- GlideOAuthClientRequest : métodos para lidar com solicitações do cliente.
- GlideOAuthClientResponse : métodos para lidar com repostas do cliente.
- GlideOAuthToken : métodos para recuperar o token de acesso e informações sobre o token de acesso.

Você também pode personalizar a inclusão de script OAuthUtil para interceptar os parâmetros de solicitação e também analisar as respostas de provedores OAuth externos.

Ao usar classes OAuth em um script com escopo, use o identificador de namespace `sn_auth`.

Parâmetros OAuth para suporte de perfil padrão

O recurso de perfil padrão exige um conjunto de parâmetros que você pode usar com a API *`setParameter()`* para especificar o solicitante do OAuth, um contexto para a solicitação e o perfil do provedor.

No cenário do provedor OAuth, você deve definir três parâmetros que informam ao provedor OAuth qual perfil OAuth usar por padrão. Quando esses três parâmetros são definidos, o token de acesso é salvo no banco de dados da instância. Use os parâmetros com *`GlideOAuthClientRequest`*.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Parâmetros OAuth para suporte de perfil padrão

Parâmetro	Descrição
`oauth_requestor`	O sys_id do objeto, que pode ser um registro de usuário ou uma conta de e-mail.
`oauth_requestor_context`	Descritor que fornece contexto para o solicitante do OAuth. Como prática recomendada, use o nome da tabela em que o objeto `oauth_requestor` foi salvo.
`oauth_provider_profile`	O sys_id do registro de perfil OAuth que é o padrão (consulte Especificar um perfil OAuth).

Você não precisa usar parâmetros para definir o tipo de concessão e o escopo porque os valores são configurados no registro de perfil do OAuth. Se você não usar os parâmetros, poderá usar os métodos da API *`GlideOAuthClientRequest setScope`* e *`setGrantType`*. Para obter informações adicionais, consulte setScope e setGrantType.

Suporte para JWT de chave privada para autenticação de cliente OAuth 2.0

Suporte ao JWT para autenticação de cliente OAuth 2.0.

A autenticação de cliente JWT de chave privada é um método de autenticação que pode ser usado por clientes para se autenticarem no servidor de autorização ao usar o endpoint de token.

Neste mecanismo de autenticação, somente os clientes que registraram uma chave pública e assinaram um JWT usando essa chave podem ser autenticados.

O JWT deve conter valores de declaração NECESSÁRIOS e pode conter valores de declaração OPCIONAIS. Para saber mais sobre os valores de declaração necessários para o JWT para autenticação `private_key_jwt`, consulte a seção Autenticação de cliente na documentação principal da Conexão OpenID.

Nota: O token de autenticação deve ser enviado como o valor do parâmetro client_assertion. O valor do parâmetro **client_assertion_type** deve ser `urn:ietf:params:oauth:client-assertion-type:jwt-Bearer`.

Plug-ins necessários para a Autenticação de cliente OAuth 2.0 usando o token JWT:

- **OAuth 2.0 (com.snc.platform.security.oauth)**: este plug-in está ativo em instâncias novas e atualizadas. Se o plug-in não estiver ativo em sua instância, você poderá ativá-lo.
- **Integração - Instalador de Single Sign-On de vários provedores (com.snc.integration.sso.multi.installer)**: para caso de uso de Single Sign-On baseado em OIDC.

Você pode usar a Autenticação de cliente OAuth 2.0 usando o JWT de chave privada para os seguintes casos:

- Single Sign-on baseado em OIDC
- Integrações de saída de OAuth

Configurar JWT de chave privada para SSO baseado em OIDC

Configure o JWT de chave privada para integrações SSO baseadas em OIDC.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Função necessária: administrador

Você precisa executar as seguintes tarefas antes de escolher o JWT de chave privada para o SSO baseado em OIDC.

- Carregar certificado Java KeyStore: anexe um certificado JKS à sua instância para usar para habilitar a autenticação do cliente JWT.
- Configurar uma chave de assinatura JWT: crie uma chave de assinatura JWT para atribuir ao seu certificado Java KeyStore (JKS).

  Nota: Se você quiser adicionar o **Impressão digital SHA-1 do certificado X.509 (x5t)** ao cabeçalho como parte da chave JWT, deverá configurar o formulário e adicionar o campo **Impressão digital SHA-1 do certificado X.509 (x5t)**.

- Criar um provedor JWT com uma chave de assinatura JWT: adicione um provedor JWT à sua instância da ServiceNow.

Para incluir uma chave JWT para o Provedor de identidade baseado em OIDC:

- Instale o plug-in **Integração - Instalador de Single Sign-On** (`com.snc.integration.sso.multi.installer`).
- Habilite as **Propriedades de SSO de vários provedores**. Para obter mais informações, consulte Propriedades, tabelas e scripts de SSO de vários provedores.
- Crie um Provedor de identidade de OIDC. Para obter mais informações, consulte Criação de uma configuração OpenID Connect (OIDC) para Single Sign-On (SSO).

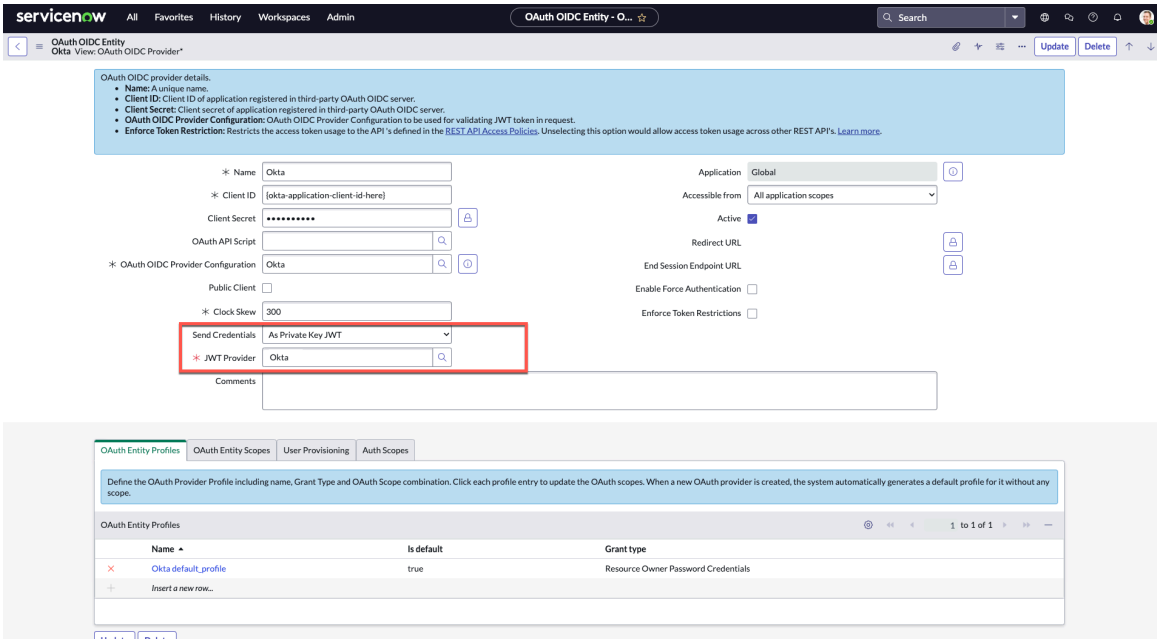
Procedimento

1. Navegue até **Todos** > **OAuth de Sistema** > **Registro de aplicações**.
2. Selecione o Provedor de identidade de OIDC que você criou.
3. Na parte superior do formulário, selecione **Configurar** > **Design de formulário**.

   Nota: Você deve adicionar os campos **Enviar credenciais** e **Provedor JWT** ao formulário para usar o JWT de chave privada para solicitações de autenticação do Provedor de identidade baseadas em OIDC.

4. Escolha **Como JWT de chave privada** para Enviar credenciais.
5. Selecione o **Provedor JWT**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Quando o usuário é autenticado, a página de autenticação conterá opções para fazer login por meio do Okta.

Configurar JWT de chave privada para OAuth de saída

Configure o JWT de chave privada para integrações de OAuth de saída.

Antes de Iniciar

Função necessária: administrador

Antes de configurar o JWT de chave privada para integrações de OAuth de saída, você deve executar as seguintes tarefas:

- Carregar certificado Java KeyStore: anexe um certificado JKS à sua instância para usar para habilitar a autenticação do cliente JWT.
- Configurar uma chave de assinatura JWT: crie uma chave de assinatura JWT para atribuir ao seu certificado Java KeyStore (JKS).

> **Nota:** Se você quiser adicionar o **Impressão digital SHA-1 do certificado X.509 (x5t)** ao cabeçalho como parte da chave JWT, deverá configurar o formulário e adicionar o campo **Impressão digital SHA-1 do certificado X.509 (x5t)**.

- Criar um provedor JWT com uma chave de assinatura JWT: adicione um provedor JWT à sua instância da ServiceNow.

Procedimento

1. Navegue até **Todos** > **Sistema OAuth** > **Registro de Aplicação** e, em seguida, clique em **Novo**.
2. Na página do interceptador, clique em **Conectar-se a um provedor OAuth de terceiros** e preencha o formulário.

> **Nota:** Você deve adicionar os campos **Enviar credenciais** e **Provedor JWT** ao formulário para usar o JWT de chave privada para solicitações de autenticação de OAuth de saída.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Nome	Nome exclusivo da conexão OAuth de terceiros.
ID de cliente	O ID de cliente da aplicação registrado no servidor OAuth de terceiros.
Segredo do cliente	O segredo do cliente da aplicação registrado no servidor OAuth de terceiros.
Script do API da OAuth	O script usado para personalizar solicitações e respostas ao provedor OAuth de terceiros.
URL de logotipo	O URL de logotipo da aplicação OAuth.
Tipo de concessão padrão	Escolha: **Credenciais do cliente**: ID do cliente e segredo do cliente, ambos usados para obter o token de acesso. Esse método não fornece atualização de tokens.
Tempo de vida do token de atualização	Tempo, em segundos, em que o token de atualização é válido. O tempo padrão é 8.640.000 segundos.
Cliente público	Permite que clientes públicos exijam o PKCE para uma autorização. **Nota:** Você pode usar somente o código de autorização como *Default Grant type* quando o PKCE estiver habilitado.
Comentários	Adicione comentários sobre o aplicativo OAuth.
Aplicação	Aplicação e escopo que contenham este registro.
Acessível de	Torne este aplicativo acessível a partir de todos os escopos de aplicativo ou somente a partir deste escopo.
Ativo	Marque a caixa de seleção para ativar o aplicativo.
URL de Autorização	O endpoint do código de autorização OAuth.
URL do token	O endpoint do token do servidor OAuth.
URL de revogação do token	O endpoint de revogação de token do servidor OAuth.
URL de redirecionamento	O endpoint de retorno de chamada do OAuth Se estiver em branco, a instância gerará uma entrada automaticamente.
Usar autenticação mútua	Marque a caixa para usar autenticação mútua para solicitação e revogação de token. Este recurso exige que um perfil de autenticação mútua seja especificado.
Enviar Credenciais	Escolha: **Como JWT de chave privada**
Provedor JWT	Detalhes do provedor JWT. Você pode usar a pesquisa para selecionar o provedor JWT.

O sistema cria um registro na tabela Registros da aplicação [oauth_entity] com o tipo Provedor OAuth que pode ser utilizado para autenticação JWT de chave privada.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Criar uma mensagem de REST de saída

Crie uma mensagem de REST de saída para autorizar que a instância atue como servidor de autorização.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Navegue até **Serviços Web do sistema** > **Saída** > **Mensagem REST** e, em seguida, clique em **Novo**.
2. Preencha os campos de formulário para o registro da aplicação OAuth conforme descrito em .
   Observe os seguintes valores de campos:
   - **Endpoint**: o URL da instância que é o servidor de autorização.
   - **Tipo de autenticação**: **OAuth 2.0**.
   - **Perfil OAuth**: o perfil OAuth que você criou para o servidor do cliente.
3. No registro da mensagem REST, clique em **Obter token OAuth**.
4. Faça a autenticação com a instância que fornece o token — o método depende da integração single sign-on.
   Você pode usar:
   - O nome de usuário e a senha que você usa para se autenticar na instância.
   - O nome de usuário e a senha do IdP se habilitado. Clique em **Usar login externo** para acessar a tela de login do IdP.

     Nota: Para ser redirecionado automaticamente para a página de login do IdP, você deve definir a propriedade de sistema glide.authenticate.external.

   - Seu código, se a MFA estiver habilitada.
5. Clique em **Permitir** ou **Negar** para concluir a autorização e emitir os tokens.
   O processo a seguir está descrito em Fluxo de concessão de código de autorização OAuth.

Registro automático na instância da ServiceNow

Use o registro pelo próprio usuário externo para integrar um grande volume de usuários externos em sua instância. Este recurso aprimora a verificação de identidade para melhorar as experiências do cliente e oferece suporte aos fluxos de registro usados com frequência.

Explorar

Ativar

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Conheça os recursos e o valor comercial do registro automático.	Entenda como ativar o Registro automático externo.
Configurar Configure o Registro automático.	Habilitar Conheça as propriedades do Registro automático.

Explorar o registro automático

Use o registro pelo próprio usuário externo para integrar um grande volume de usuários externos em sua instância. Este recurso aprimora a verificação de identidade para melhorar as experiências do cliente e oferece suporte aos fluxos de registro usados com frequência.

O Registro pelo próprio usuário externo permite que um grande grupo de usuários se registre em um app da ServiceNow sem a ajuda de um administrador. Por exemplo, uma universidade com um grande grupo de alunos precisando de estacionamento no campus pode se registrar no app de estacionamento do campus. Cada aluno receberia um conjunto limitado de privilégios específicos para estacionamento e concluiria um processo de registro automatizado. Este sistema pode gerar um número de estacionamento, exclusivo para cada aluno, e garantir que eles tenham uma vaga.

Um fluxo de registro automático consiste em um app da ServiceNow personalizado, neste caso, um app de estacionamento do campus. Depois de configurar um app com as tabelas necessárias, um administrador configuraria o registro, incluindo um fluxo de pré-registro, mapeamento de campo, mapeamento pós-registro, captcha, mapeamento de função e fluxo pós-registro.

Ativar Registro pelo próprio usuário externo

Você pode ativar o plug-in Registro pelo próprio usuário externo (com.snc.external_user_self_registration) se tiver a função de administrador.

Antes de Iniciar

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

Procedimento

1. Navegue até **Todos** > **Aplicações do sistema** > **Todas as aplicações disponíveis** > **Todas**.
2. Encontre o plug-in usando os critérios de filtro e a barra de pesquisa.

   Pesquise o plug-in pelo nome ou ID. Se não conseguir encontrar um plug-in, talvez seja necessário solicitá-lo ao pessoal ServiceNow.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Selecione **Instalar** para iniciar o processo de instalação.

   Nota: Quando a separação de domínio e o administrador delegado estão habilitados em uma instância, o usuário administrativo deve estar no domínio **global.** Caso contrário, será exibido o seguinte erro: `A instalação da aplicação não está disponível porque há outra operação em execução: ativação de plug-in para <plugin name>.`

   Você verá uma mensagem após a conclusão da instalação.

Funções externas no registro automático

Para impedir o fornecimento inadvertido de acesso a usuários externos, você pode atribuir a função snc_external a todos os usuários externos.

Usuários externos que se registram automaticamente devem ser atribuídos à função snc_external, que tem o mínimo de privilégios. A função snc_external indica que o usuário é externo à sua organização e não deve ter acesso aos recursos, a menos que seja explicitamente permitido por meio de ACLs para a função snc_external ou funções adicionais que herdam a função snc_external.

Por padrão, os usuários com a função snc_external não podem acessar:

- Recursos Scripted REST APIs que não estejam marcados como externos.
- Tabelas sem a função que herda a função snc_external ou a função pública.
- Recursos do tipo sem registro, como processadores e páginas de IU sem a função snc_external ou uma função que herda a função snc_external.
- Painéis Análise da plataforma.

Começando com a versão Paris, você deve habilitar uma propriedade exclude-list para impor a atribuição explícita de funções snc_external. Para obter informações sobre como habilitar a propriedade, consulte Impedir futuras atribuições de função interna para usuários externos.

Criar uma configuração de registro de usuário para usuários externos

Crie um registro de configuração de registro de usuário para inicializar o processo de integração de usuários externos em aplicações personalizadas da ServiceNow. Este formulário orienta os usuários externos durante o processo de registro automático.

Antes de Iniciar

- Função necessária: administrador
- Ativar Registro pelo próprio usuário externo

Procedimento

1. Navegue até **Todos** > **Registro pelo próprio usuário externo** > **Configurações de registro de usuário** e clique em **Novo**.
2. No formulário, preencha os campos.

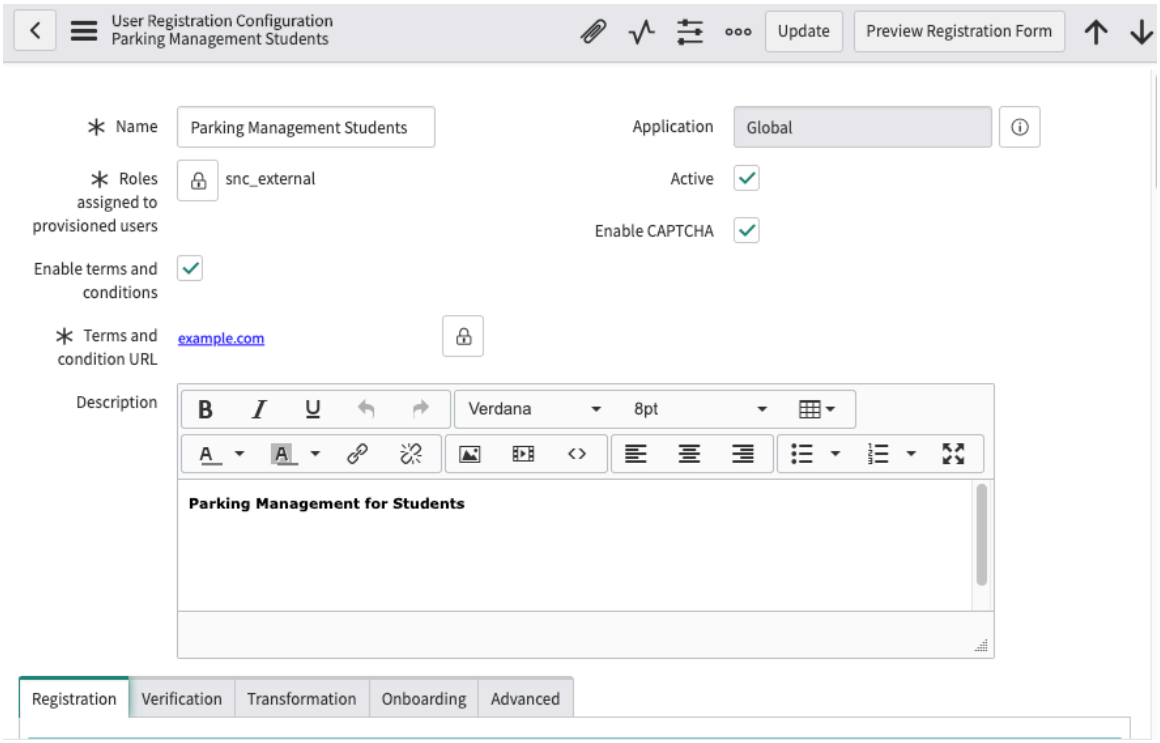
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formulário de configuração de registro de usuário

Campo	Descrição
Nome	Nome do formulário de registro. Por exemplo, o registro de estacionamento de aluno pode ser Estacionamento alunos de administração.
Funções atribuídas aos usuários provisionados	Funções atribuídas aos usuários provisionados. As funções especificadas devem estender ou conter a função `snc_external`. A função especificada também pode ser função `snc_external`. Para usuários externos, cada função deve ter um `snc_external` para notificar um usuário externo. Se você tiver funções pré-configuradas, elas deverão estar acessíveis ao desbloquear as funções e pesquisar usuários.
Habilitar termos e condições	Opção para adicionar um URL de termos e condições à página de registro.
URL de termos e condições	O URL publicamente acessível que contém os termos e condições do formulário de registro. Este campo aparece somente quando **Habilitar termos e condições** é selecionado.
Descrição	A descrição do formulário de inscrição. Este campo aparece somente quando você salva ou envia a configuração. Você pode adicionar mais informações sobre o formulário de registro neste campo. **Nota:** Você só pode adicionar uma descrição depois de salvar ou atualizar uma configuração de registro de usuário.
Aplicação	Aplicação que contém este registro. A aplicação é definida automaticamente como `Global`.
Ativo	Opção que ativa a configuração de registro de usuário. Esta opção é selecionada por padrão.
Habilitar CAPTCHA	Opção para adicionar um CAPTCHA ao formulário de registro. O provedor de CAPTCHA padrão é o Google reCAPTCHA. **Nota:** Para habilitar o CAPTCHA para o registro de usuário, siga as etapas em Configurar Google reCAPTCHA para registro pelo próprio usuário externo.

3. Clique em **Enviar**.
   Uma configuração de registro de usuário com as configurações padrão é criada.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



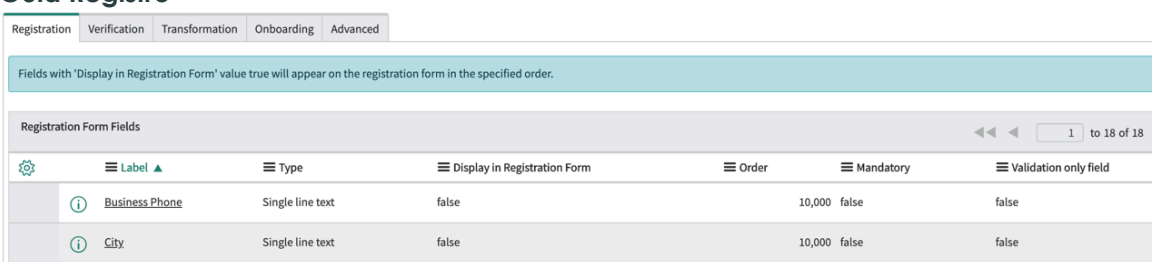
4. Opcional: Configure a guia **Registro** para mostrar os campos e a ordem em que eles aparecem:

Campos de formulário de registro

Coluna	Descrição
Exibir no Formulário de Registro	Defina qualquer campo que você deseja exibir como `Verdadeiro`.
Ordem	Defina um número de pedido para exibir campos no seu formulário.
Obrigatório	Defina qualquer campo que você deseja torná-lo obrigatório como `Verdadeiro`.
Campo somente validação	Defina qualquer campo que você deseja usar somente para validação. Por exemplo, código de registro.

Você pode optar por exibir os campos de formulário padrão ou adicionar campos de formulário personalizados ao Formulário de registro. Para obter mais informações, consulte Campos de formulário de registro padrão.

Guia Registro



© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

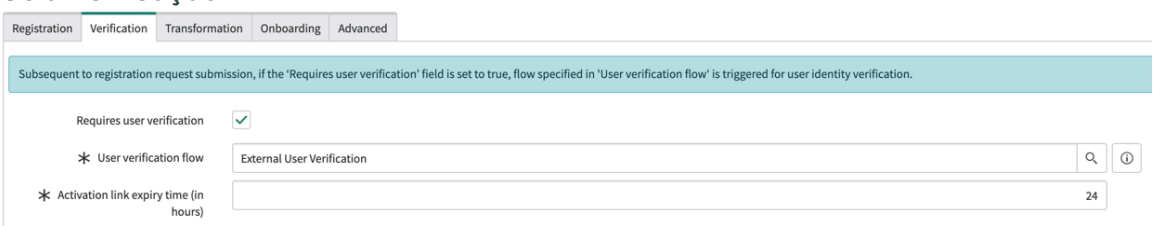
Você também pode adicionar campos de formulário de registro personalizados. Para obter mais informações, consulte Adicionar um campo personalizado ao formulário de registro.

5. Opcional: Configure a guia **Verificação** para verificar a identidade dos usuários registrados. Quando o fluxo de verificação do usuário é acionado, um link de ativação é enviado para o endereço de e-mail registrado do usuário.

Campos da guia Verificação

Campo	Descrição
Requer verificação de usuário	Opção para acionar um subfluxo de verificação de usuário que é executado após o registro de usuário. O subfluxo é para verificação de identidade do usuário.
Fluxo de verificação do usuário	O subfluxo usado para verificar a identidade do usuário. O subfluxo é acionado somente quando você habilita a verificação do usuário. (Optional) O subfluxo **Verificação de usuário externo** está disponível por padrão. Você pode criar uma cópia do subfluxo padrão em Flow Designer e modificá-lo de acordo com seus requisitos. Para obter mais informações, consulte Flow Designer. **Nota:** Para visualizar o subfluxo **Verificação de usuário externo** em uma nova guia, use os seguintes atalhos: ◦ Macintosh: Command + Clique ◦ Windows: Control + Clique
Tempo de expiração do link de ativação (em horas)	O número de horas após as quais um link de ativação expira. O valor padrão é 24.

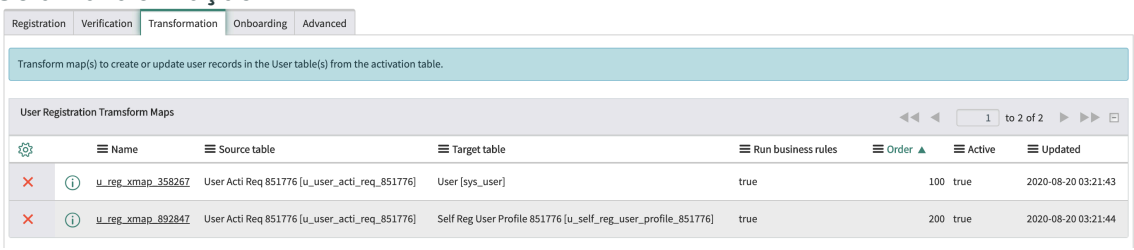
Guia Verificação



6. Opcional: Configure a guia **Transformação** para mapear usuários registrados automaticamente e usuários ativados.
Há dois mapas de transformação (u_reg_xmap_ [number]) que mapeiam automaticamente os usuários registrados da tabela Req. de ativ. de usuário [number] para a tabela Usuário registrado automaticamente [number]. Você pode criar uma cópia desses mapas de transformação padrão e modificar o mapa de acordo com seus requisitos. Para obter mais informações, consulte Mapas de transformação.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

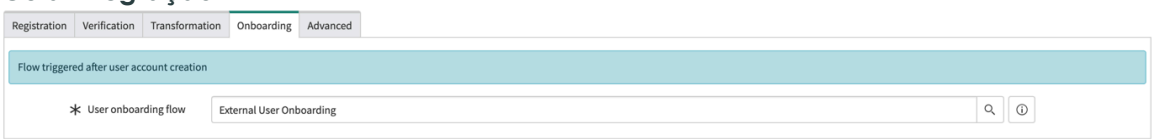
Guia Transformação



7. Configure a guia **Integração** para acionar subfluxos para integração de usuários ativados. O subfluxo **Integração de usuário externo** padrão envia um e-mail ao usuário que contém um link para redefinir a senha. Você pode criar uma cópia do subfluxo padrão e modificá-lo de acordo com seus requisitos.

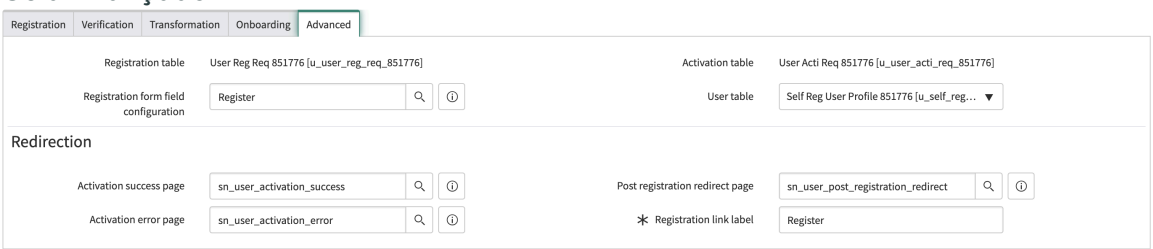
   Nota: Quando o subfluxo **Integração de usuário externo** é acionado, o subfluxo envia um e-mail para o usuário que contém um link para redefinir a senha.

Guia Integração



8. Opcional: Configure a guia **Avançado** para mapear tabelas de usuário e páginas de redirecionamento do formulário de registro.

Guia Avançado



Guia Avançado

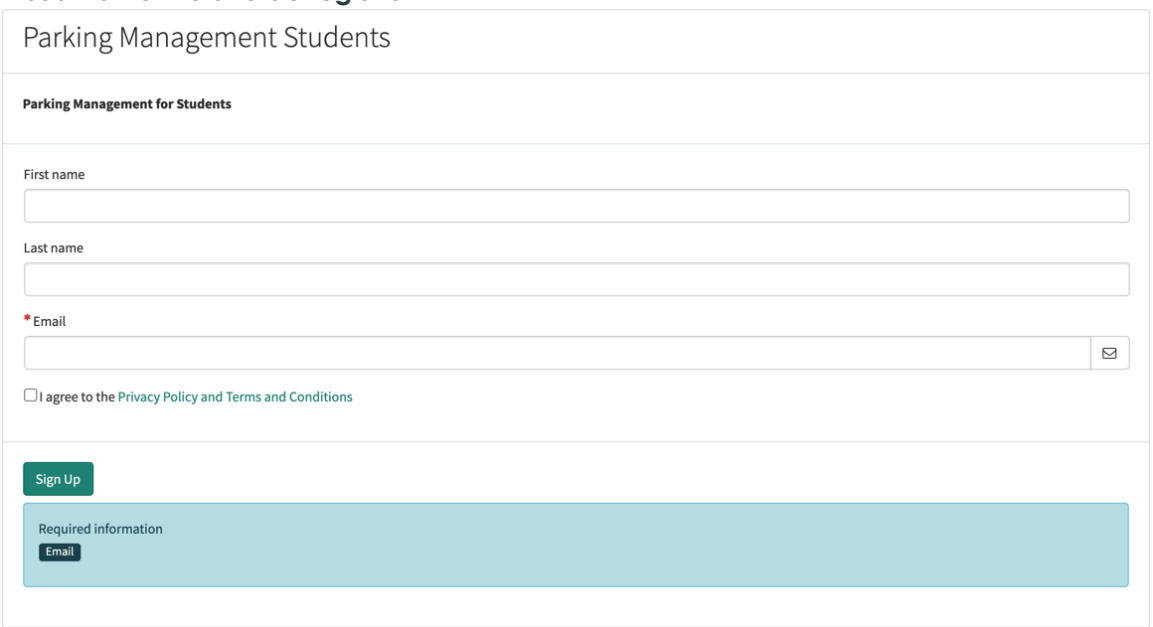
Campo	Descrição
Tabela de registro	Nome da tabela onde as informações do formulário de registro são salvas.
Configuração do campo de formulário de registro	O registro associado ao formulário de registro no Produtor de registro.
Tabela de ativação	Rótulo e nome da tabela usada para ativação do usuário. A tabela de ativação contém registros dos usuários que concluíram a verificação.
Tabela de Usuário	Rótulo e nome da tabela de perfil de usuário.
Página da ativação com êxito	A página para a qual um usuário é redirecionado após a ativação ser bem-sucedida.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Página de erro de ativação	A página para a qual um usuário é redirecionado quando a ativação falha.
Página de redirecionamento após o registro	A página para a qual o usuário é redirecionado após o registro.
Rótulo do link de registro	O nome do botão usado para registro do portal de serviços. O valor padrão é Registrar.

Ao fazer mudanças ou depois de concluir todas as mudanças na configuração de registro de usuário, você pode usar o botão **Visualizar formulário de registro** para visualizar as mudanças no formulário de registro.

Visualizar formulário de registro



Configurar Google reCAPTCHA para registro pelo próprio usuário externo

Para usar o serviço Google reCAPTCHA, você deve solicitar um par de chaves de API do Google e configurar as propriedades do sistema relacionadas.

Antes de Iniciar

- Solicite um par de chaves de API (uma chave de site e um segredo) do Google em https://www.google.com/recaptcha.
- Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

Procedimento

1. Navegue até **Todos** > **Propriedades do sistema** > **Todas as propriedades**.
2. Pesquise pelas seguintes propriedades e defina os valores:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Propriedade	valor
glide.user.registration.google.recaptcha.secret	O segredo autoriza a comunicação entre a aplicação e o servidor reCAPTCHA. Digite: password2
glide.user.registration.google.recaptcha.site_key	A chave do site usada para invocar o serviço reCAPTCHA em sua página de registro. Tipo: cadeia de caracteres
glide.user.registration.captcha.widget	O Sys_ID do Widget Captcha. Tipo: cadeia de caracteres

Campos de formulário de registro padrão

Você pode usar os campos de formulário de registro padrão ou criar campos de formulário de registro personalizados.

Campos de formulário de Registro

Os seguintes campos de formulário são adicionados ao formulário de Registro por padrão.

Rótulo do Campo	Tipo
Telefone comercial	Texto de linha única
Cidade	Texto de linha única
País	Selecionar Caixa
Status EDU Usado para diferenciar funcionários, alunos e visitantes. **Nota:** Este campo é útil quando o formulário de registro é para uma instituição educacional.	Selecionar Caixa
E-mail	E-mail
Nome	Texto de linha única
Sexo	Texto de linha única
Telefone residencial	Texto de linha única
Idioma	Selecionar Caixa
Sobrenome	Texto de linha única
Nome do meio	Texto de linha única

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Rótulo do Campo	Tipo
Telefone celular	Texto de linha única
Nome	Texto de linha única
Prefixo Título do usuário. Por exemplo, Sr., Dr. e assim por diante.	Selecionar Caixa
Estado/província	Texto de linha única
Rua	Texto de Linha Única Larga
Título - Cargo	Selecionar Caixa
CEP	Texto de linha única

Nota: Não é possível excluir os campos de formulário de registro padrão.

Adicionar um campo personalizado ao formulário de registro

Você pode adicionar campos personalizados no formulário de registro pelo próprio usuário.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Navegue até **Todos** > **Registro pelo próprio usuário externo** > **Configurações de registro de usuário**.
2. Abra o registro da configuração de registro de usuário necessária.
3. Navegue até o final da seção Campos de formulário de registro e clique em **Inserir uma nova linha...**
4. Insira o nome do campo na coluna **Rótulo** e clique na marca de seleção.
   Uma nova linha é adicionada com os valores padrão. Você pode configurar o campo de formulário de registro personalizado com base em seus requisitos.

Colunas do campo de formulário de Registro

Coluna	Descrição
Rótulo	O nome do campo que aparece no formulário de registro.
Tipo	O tipo de elemento da interface do usuário. A seguir estão os tipos compatíveis: ◦ Texto de linha única ◦ E-mail ◦ Data ◦ Date/hora ◦ Sim/Não ◦ Texto de Linha Única Larga ◦ Múltipla Escolha ◦ Selecionar Caixa

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Coluna	Descrição
Exibir no Formulário de Registro	Opção para exibir o campo no formulário de registro.
Ordem	A sequência na qual os campos de formulário aparecem no formulário de registro. O campo com o valor de ordem mais baixo aparece primeiro e o campo com o valor de ordem mais alto aparece por último. O valor padrão é 10.000.
Obrigatório	Opção para tornar um campo obrigatório no formulário de registro.
Campo somente validação	Opção de usar um campo somente para fins de validação. Por exemplo, código de registro. Quando definido como verdadeiro, este campo não é salvo na tabela Usuário (sys_user).

5. Salve ou atualize as mudanças.

Habilitação do registro pelo próprio usuário externo para Portal de serviços

Permita que usuários externos se registrem em um app de ServiceNow por meio de Portal de serviços.

Antes de Iniciar
Função necessária: administrador

Procedimento

1. Navegue até **Todos** > **Portal de serviços** > **Portais**.
2. Abra um registro do portal.
3. No formulário, preencha o campo **Configuração de registro de usuário externo**.

   Selecione uma configuração de registro de usuário.
4. Clique em **Atualizar**.

Resultados
O widget de login inclui um link para o formulário de registro que você configurou anteriormente.

Verificar solicitações de Registro pelo próprio usuário

Depois que um usuário se registra no Portal de serviços , um registro de usuário é adicionado ao módulo Solicitações de registro. Você pode exibir a lista de usuários registrados que foram registrados com sucesso no Portal de serviços .

Antes de Iniciar
Função necessária: administrador

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegue até **Todos** > **Registro pelo próprio usuário externo** > **Solicitações de registro**. A lista de registros do usuário é exibida.
2. (Opcional) Revise os registros de usuário individuais e os modifique de acordo com seus requisitos. Por exemplo, você pode alterar o status de um formulário de registro de usuário de **Pendente** para **Processado**.

Autenticação baseada em tokens (logins de usuários)

Aprimore o mecanismo de segurança para que os usuários acessem uma rede usando a autenticação baseada em token.

Autenticação com limite de tempo	Autenticação do token Digest
A autenticação baseada em token é um protocolo que permite que os usuários verifiquem sua identidade e, em troca, recebam um token de acesso exclusivo. Isso ajuda a aprimorar o mecanismo de segurança para que os usuários acessem uma rede.	A autenticação de token de resumo passa as credenciais do usuário e um token de resumo em um cabeçalho HTTP não criptografado.

Autenticação com limite de tempo

Suporte à autenticação com limite de tempo para sua instância da ServiceNow.

Explorar	Ativar
Conhecer os recursos e o valor comercial da autenticação com limite de tempo.	Entender como ativar a autenticação com limite de tempo.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tutorial: autenticação com limite de tempo

Conheça as propriedades do Zero Trust Access.

Explorar autenticação com limite de tempo

Suporte à autenticação com limite de tempo para sua instância da ServiceNow.

Nota: A autenticação com limite de tempo é muito específica para a instância da ServiceNow. Os links personalizados para usuários só podem ser criados na ServiceNow.

Os administradores podem configurar a autenticação baseada em link na instância da ServiceNow. O link configurado pode ser compartilhado com o usuário por e-mail ou SMS e o usuário pode usar esses links para fazer login na instância.

O login na instância com este esquema de autenticação é controlado por meio das políticas de Autenticação adaptável configuradas na instância da ServiceNow.

A autenticação baseada em tempo permite que você execute o seguinte:

- O administrador pode configurar a autenticação baseada em link para usá-la dentro de um tempo de expiração.
- A equipe da aplicação pode buscar o nonce a ser usado com o link para o item de configuração específico usando a API passível de script exposta. A geração de link será feita pela equipe da aplicação.
- A equipe da aplicação pode gerar o link e enviar para o usuário por meio de um canal existente.
- O usuário com o link pode fazer login na instância uma vez e dentro do tempo de expiração especificado como parte da configuração.
- Os administradores podem configurar as funções com poucos privilégios para o esquema de autenticação.
- Os administradores podem impor a MFA para o esquema de autenticação como um segundo fator para autenticação com o link TLA.

Ativar a autenticação com limite de tempo

A autenticação com limite de tempo é ativada por meio do plug-in Integration - Multiple Provider Single Sign-On Installer.

Antes de Iniciar

Função necessária: administrador

Nota: A autenticação com limite de tempo é muito específica para a instância da ServiceNow. Os links personalizados para usuários só podem ser criados na ServiceNow.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegue até **Todos** > **Aplicações do sistema** > **Todas as aplicações disponíveis** > **Todas**.
2. Encontre o plug-in Autenticação com limite de tempo (*com.snc.authenticate.time_limited_authentication*) usando os critérios de filtro e a barra de pesquisa.

   Pesquise o plug-in pelo nome ou ID. Se não conseguir encontrar um plug-in, talvez seja necessário solicitá-lo ao pessoal ServiceNow.
3. Selecione **Instalar** para iniciar o processo de instalação.

   Nota: Quando a separação de domínio e o administrador delegado estão habilitados em uma instância, o usuário administrativo deve estar no domínio **global.** Caso contrário, será exibido o seguinte erro: `A instalação da aplicação não está disponível porque há outra operação em execução: ativação de plug-in para <plugin name>.`

   Você verá uma mensagem após a conclusão da instalação.

Autenticação com limite de tempo com SMS - Tutorial da Twilio

Configure a autenticação com limite de tempo com fatores de MFA, como SMS usando Twilio.

Antes de Iniciar

Função necessária: administrador

Plug-ins necessários:

- *com.snc.authenticate.time_limited_authentication* (Autenticação com limite de tempo)
- *com.snc.authentication.sms_mfa* (Autenticação multifator com SMS)

Nota: A TLA (time limited authentication, autenticação com limite de tempo) é muito específica para a instância da ServiceNow. Os links personalizados para usuários só podem ser criados na ServiceNow.

As instruções do tutorial fornecidas permitem que o administrador forneça um login baseado em link com SMS como segundo fator (MFA) para usuários com uma função específica.

Após uma configuração bem-sucedida, o sistema gera um link e, em seguida, compartilha o link com o usuário por meio do canal de notificação (e-mail/SMS). Ao clicar no link, o usuário é solicitado a especificar o fator de OTP enviado para e-mail ou SMS com base na função do usuário (configuração).

Nota:

- A TLA deve ser sempre seguida por MFA e a MFA deve ser habilitada pelo administrador usando a Autenticação adaptável para login de TLA. Para saber mais sobre como configurar a MFA com Autenticação adaptável, consulte Contexto de MFA (autenticação multifator).
- A TLA deve ser usada para os usuários que têm privilégios limitados.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Criar uma configuração da Twilio.
   a. Crie uma conta de teste na Twilio. Para obter mais informações, consulte Twilio.
   b. Navegue até **Todos** > **Notify** > **Administração** > **Configuração da Twilio Direct**.
   c. Forneça o **SID da conta** e o **Token de autenticação** (criado a partir da Twilio) e salve o registro.

   Nota: Você pode criar sua própria configuração de provedor e usá-la para a TLA. Neste exemplo, é Twilio. Para saber mais sobre como criar uma configuração de provedor de MFA, consulte Configuração de provedor MFA.

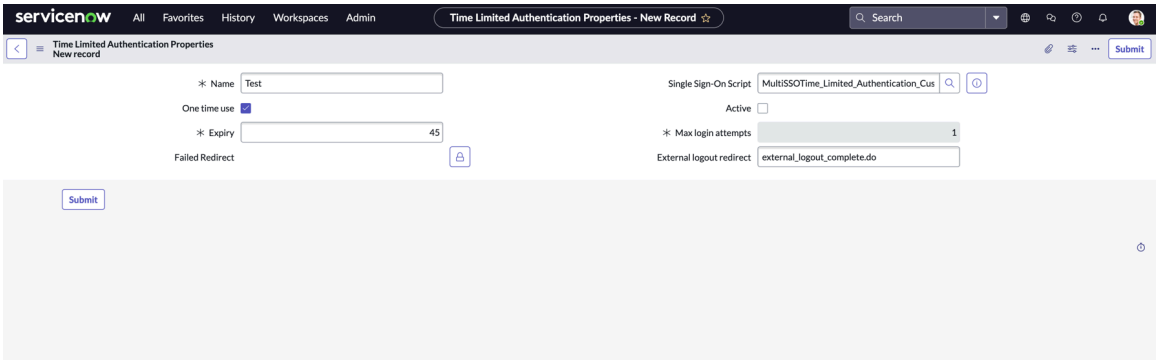
2. Configurar e habilitar o registro de autenticação com limite de tempo (TLA).
   a. Navegue até **Todos** > **Registros de configuração de autenticação com limite de tempo** e clique em **Novo**.
   b. No formulário, preencha os campos.

Propriedades da autenticação com limite de tempo

Campo	Descrição
Nome	Nome do registro.
Uso único	Habilite para usar o link da TLA uma vez.
Vencimento	Especifique os segundos para a expiração do link. O padrão é 45 minutos.
Falha no redirecionamento	Insira o URL para redirecionar os usuários após uma autenticação com falha.
Script de Single Sign-on	Detalhes do script SSO que você deseja usar.
Ativo	Opção para ativar a configuração.
Máximo de tentativas de login	Especifique o número de tentativas permitidas com o link de TLA gerado para login. Desmarque a caixa de seleção **Uso único** para fornecer o número máximo de tentativas.
Redirecionamento de logout externo	Insira o URL para redirecionar os usuários após o logout.

   c. Clique em **Enviar**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



d. Navegue até **Todos** > **SSO de vários provedores** > **Administração** > **Propriedades**, habilite a propriedade **Habilitar SSO de vários provedores** e clique em **Salvar**.

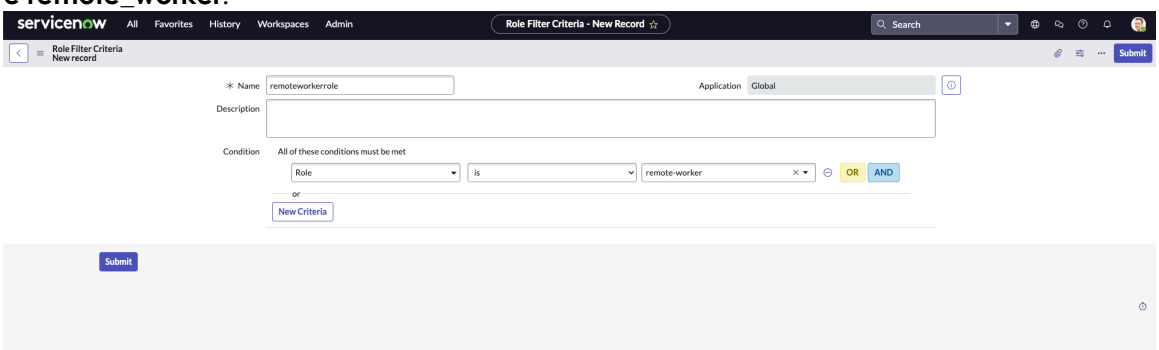
3. Permitir TLA somente para uma persona de usuário específica usando a política de contexto de pós-autenticação.

a. Navegue até **Funções** e crie uma função. Por exemplo: remote_worker.

b. Crie um usuário com id de e-mail e número de celular válidos. Para saber como criar um usuário, consulte Criar um usuário.

c. Atribua a função ao usuário. Para saber como atribuir a função ao usuário, consulte Atribuir uma função a um usuário.

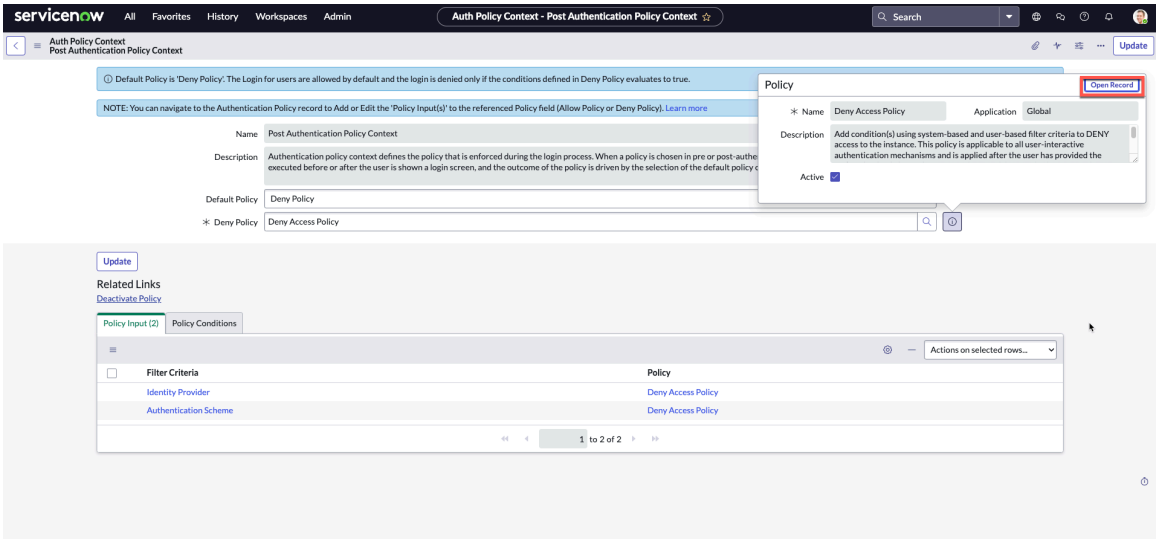
d. Para criar um critério de filtro de função, navegue até **Todos** > **Autenticação adaptável** > **Critérios do filtro de função**, crie um novo filtro **remoteworkerrole** e a condição **Função é remote_worker**.



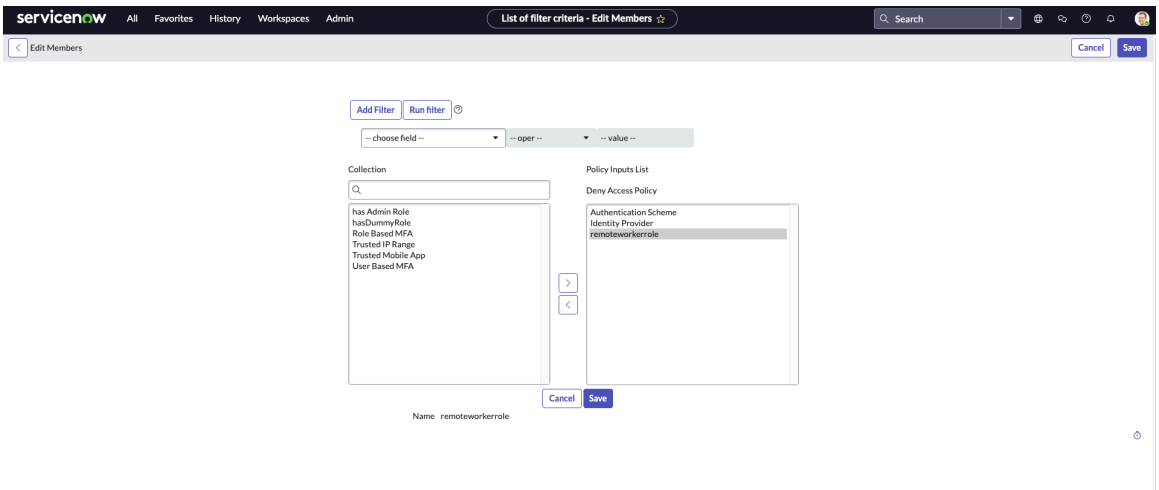
e. Para adicionar a condição de política com base no contexto de política de negação baseada nos critérios de filtro de IdP e função, navegue até **Todos** > **Autenticação adaptável** > **Contexto pós-autenticação**.

f. Clique no ícone de informações e **Abrir o registro**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



g. Na Entrada de política, clique em **Editar**, adicione a função (remotworkerrole) e clique em **Salvar**.



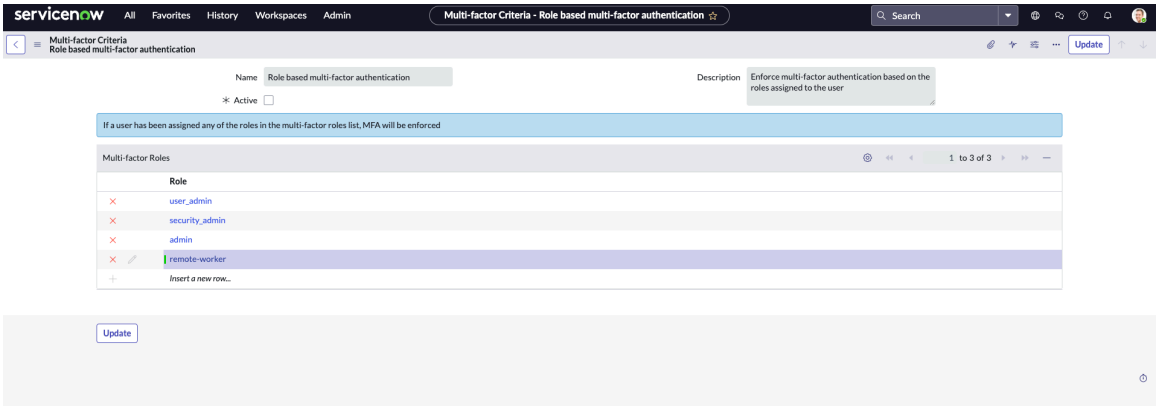
h. Na Condição de política, adicione a condição para a entrada de política e **envie** o registro.

4. Configurar a política de autenticação em etapas - Contexto de MFA.

a. Navegue até **Todos** > **Critérios multifator**.

b. Selecione a **Autenticação multifator baseada em função**, adicione a função na seção Funções multifator e clique em **Atualizar**. Neste exemplo: **remote_worker**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

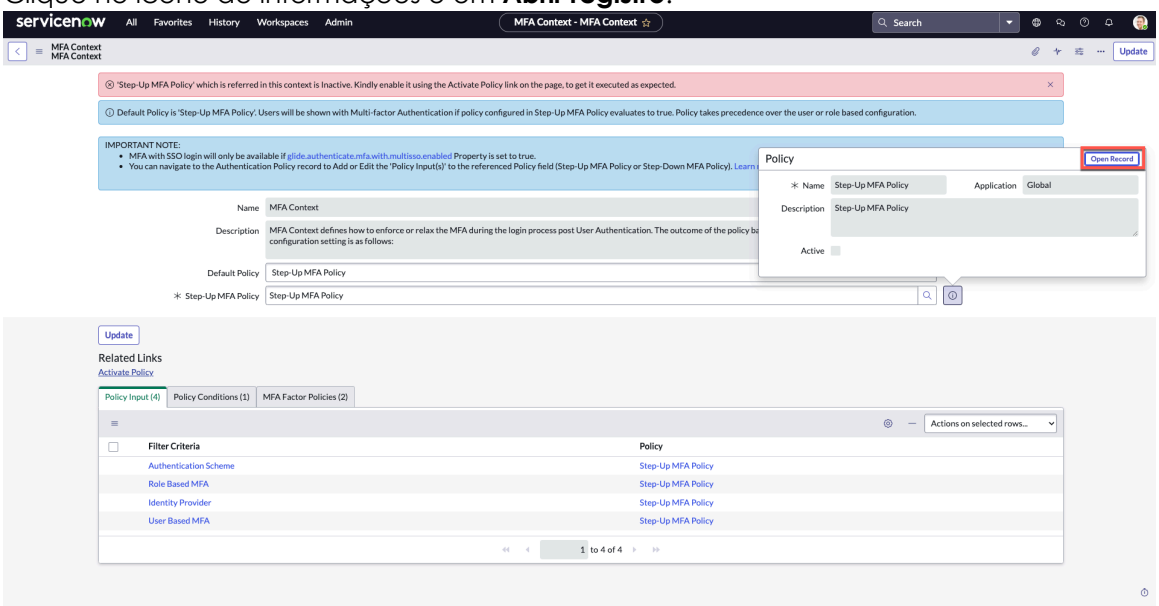


c. Navegue até **Todos** > **Autenticação adaptável** > **Contexto MFA**.

d. Verifique o seguinte:

- O campo Política padrão é **Política de MFA em etapa crescente**
- Política de MFA em etapa crescente é **Política de MFA em etapa crescente**

e. Clique no ícone de informações e em **Abrir registro**.



f. No formulário Política de MFA em etapa crescente, nas Entradas de política, clique em **Editar**.

g. Adicione a **Autenticação multifator baseada em função** à lista e clique em **Salvar**. Neste exemplo, **remotworkerrole**.

h. Na Condição de política, clique em **Impor MFA se as configurações de MFA baseada na função ou no usuário forem verdadeiras**.

i. Na página Impor MFA se as configurações de MFA baseada na função ou no usuário forem verdadeiras, certifique-se de que a **MFA baseada na função** seja **verdadeira**.

5. Impor a MFA para usar SMS como uma política de fator de MFA.

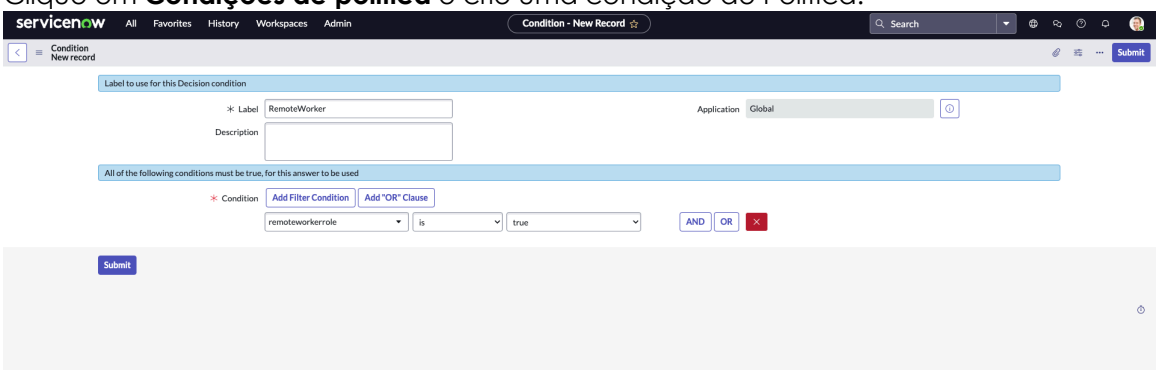
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Navegue até **Todos** > **Autenticação adaptável** > **Contexto MFA**.

b. Na página Contexto MFA, clique em **Políticas de fator de MFA** e na política **Exibir OTP de SMS como uma Política de fator de MFA**.

c. Clique em **Editar** e adicione **remoteworkerrole** em **Entradas de política**.

d. Clique em **Condições de política** e crie uma condição de Política.



e. Clique em **Enviar**.

O link para TLA gerado e compartilhado com os usuários atribuídos com a função **remoteworkerrole** será promovido para usar o código SMS como um segundo fator para fazer login na instância.

6. Habilitar as outras propriedades necessárias.

a. Navegue até **Todos** > **Autenticação multifator** > **Propriedades**.

b. Habilite as seguintes caixas de seleção.

- **Habilitar autenticação multifator**
- **Habilitar a autenticação multifator com SSO**

c. Salve o registro.

d. Navegar até **Todos** > **Autenticação adaptável** > **Políticas de autenticação** > **Propriedades**.

e. Habilite a caixa de seleção **Habilitar política de autenticação**

f. Salve o registro.

7. Gerar um link de TLA - Exemplo.

a. Navegue até **Todos** > **Definição do sistema** > **Scripts – Plano de fundo**.

b. Use a API a seguir, fornecendo o sysid e o id de config do usuário.

```
var tla=new global.TimeLimitedAuthentication();
gs.info(tla.generateNonce("user_sysid", "config1_sys_id","IAR2"));
```

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: A origem (IAR2) não é um parâmetro obrigatório.

c. O parâmetro de consulta é retornado conforme mostrado:
`nonce=VCeinfboDt0M&glide_sso_id=b3277f1b44351110f8779b5a2d9909f3&user=3b0277d3443511`

d. Crie um URL no formato abaixo:
`https://<instance-url> /login_with_sso.do?uri=<encoded url>&`
`nonce=2olIQSxdgkjs&glide_sso_id=0c15bf09c3711110c5ec4e483c40dd7a&user=62826bf0371020`

8. Clique no URL, a tela da MFA a seguir será exibida para login.

Autenticação do token Digest

A autenticação de token de resumo passa as credenciais do usuário e um token de resumo em um cabeçalho HTTP não criptografado.

Explorar	Configurar
Conhecer os recursos e o valor comercial da autenticação do token Digest.	Entender como configurar a autenticação do token Digest.

Explorar autenticação do token Digest

A instância lê o valor do cabeçalho HTTP e compara o valor de hash calculado do token de resumo. Se o valor de hash calculado corresponder ao valor do token de resumo, a instância pesquisará um valor correspondente na tabela Usuário. Se houver um valor correspondente na tabela Usuário, a instância considerará o usuário pré-autenticado e o fará login.

A autenticação de token de resumo é mais segura do que simples cabeçalhos HTTP não criptografados porque qualquer mudança acidental ou intencional no cabeçalho HTTP não criptografado produz um valor de hash diferente. Se o valor de hash não corresponder, a instância negará o acesso do usuário à instância solicitada. Isso evita que os usuários tentem fazer login com as credenciais de outro usuário.

Para saber mais sobre a expiração do link de resumo, consulte este artigo da base de conhecimento.

Nota: Use a TLA (Time Limited Authentication, autenticação com limite de tempo) para configurar links de expiração baseados em tempo. Para saber mais, consulte Autenticação com limite de tempo.

Requisitos de integração

Uma integração de Autenticação de token de resumo requer:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Um servidor Web
- SiteMinder ou outra aplicação de single sign-on para pré-autenticar o usuário na rede local
- Uma página da Web ou portal que passa as credenciais do usuário para a instância de destino em um desses formatos
  - Cabeçalho HTTP
  - Parâmetro de URL
  - Cookie
- Uma página da Web ou portal que cria e passa um token de resumo para a instância de destino usando uma dessas técnicas de codificação
  - SHA1
  - MD5
  - SHA 256 (recomendado)

Configurar as propriedades de resumo do Single Sign-on (SSO) de vários provedores

Depois de habilitar um script existente de instalação de resumo, configure as propriedades do SSO de vários provedores.

Antes de Iniciar

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

Se você não estiver usando o single sign-on de vários provedores, configure as propriedades de single sign-on padrão.

Procedimento

1. Navegue até **Todos** > **SSO de vários provedores** > **Provedores de identidade**.
2. Preencha os campos do formulário Propriedades de resumo.

Opção	Descrição
Nome	Insira o nome do token de resumo.
Usuário	Insira o campo sys_user que contém os dados correspondentes para o cabeçalho de entrada.
Nome do cabeçalho do resumo HTTP	Insira o cabeçalho HTTP gerado. Por exemplo, `DE_USER`.
Nome do cabeçalho HTTP	Insira o cabeçalho HTTP gerado para o token de resumo criado. Por exemplo, `SM_USER`.
Senha secreta	Insira a chave secreta a ser usada para codificar chaves de resumo. Por exemplo, `32 ou mais caracteres`.
Campo de redirecionamento de SSO com falha	Insira o URL para redirecionar os usuários após uma autenticação com falha.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
Redirecionamento de logout externo	Digite o URL para redirecionar os usuários após um logout.
Script de Single Sign-on	Selecione **MultiSSO_DigestedToken**.
Tipo de Cliente	Escolha o tipo de cliente com base no tipo do seu cliente. Opções:**Iframe integrado**. **Nota:** Se o campo de tipo de cliente for necessário para sua configuração, você poderá editar o formulário e adicionar o campo. Para saber mais, consulte Como configurar o tipo de cliente para registros de OAuth e SSO.

3. Clique em **Atualizar**.
4. Defina o padrão do seu Token resumido como verdadeiro.
   Quando você define o padrão como verdadeiro, isso substitui o registro de token de resumo padrão do sistema associado ao SSO. Depois que o primeiro registro de IdP relacionado ao SSO de vários provedores for ativado, somente os registros associados ao SSO de vários provedores serão usados.

   Registros de token de resumo que existem na tabela de propriedades de resumo podem ser chamados individualmente ao anexar o Sys_ID do IdP. Por exemplo, um registro de token de resumo no seguinte URL de autenticação:
   `https://<instance_name>.service-now.com/login_with_sso.do?glide_sso_id=<sys_id_of_Digest_token_record>&SM_USER=<user_name>&DE_USER=<digested_tok`

Exemplos de implementações de token de resumo

Aqui estão vários exemplos de criação de um token de resumo.

Exemplos de implementações da Autenticação Digest

Resumo criado com	Valor da chave secreta	Método hash	Exemplo
Java	32 e mais caracteres	SHA256	Exemplo de algoritmo resumido do Java para criptografia
C	Valor do parâmetro sharedKey	Valor do parâmetro strEncryptionMethod (SHA256 ou MD5)	Amostra C

Exemplo de algoritmo resumido do Java para criptografia

Este algoritmo Java ilustra a criação de um token de resumo a partir de um cabeçalho HTTP.

Este exemplo pressupõe:

- Que o servidor Web é compatível com Java
- Que o método de cálculo de hash é SHA1

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Que o valor da chave secreta é abc123
- Que o nome do cabeçalho HTTP não criptografado é user_name

Mude o código Java para usar outro mecanismo de computação de hash (como MD5), mude o valor da chave secreta ou o nome do cabeçalho HTTP.

```
public class DigestTest
{
    private static final String MAC_ALG = "HmacSHA256";
       fKey  = {32 or more characters};
    public byte[] getDigest(String acct) {
        try {
            byte[] bkey = fKey.getBytes();
            byte[] data = acct.getBytes();
            Mac mac = null;
            try {
                mac = Mac.getInstance(MAC_ALG);
                mac.init(new SecretKeySpec(bkey, MAC_ALG));
            } catch (Exception e) {
                e.printStackTrace();
            }
            byte[] sig = mac.doFinal(data);
            String signature = new String(sig);
            System.out.println("value:" + acct);
            System.out.println("digested value:  " + signature);
            return sig;
        } catch (IllegalStateException e) {
            e.printStackTrace();
        }
        return null;
    }
    public static void main(String[] args) {
        BASE64Encoder encoder = new BASE64Encoder();
        DigestTest test = new DigestTest();
        String userName = "user_name";
        System.out.println("base 64 digest username: " +
 encoder.encode(test.getDigest(userName)));
    }
}
```

Amostra C

Esta classe C ilustra a criação de um token de resumo a partir de três parâmetros de entrada.

- strEncryptionMethod - lista o método de cálculo de hash (SHA1, SHA256 ou MD5)
- mensagem - lista o valor a ser convertido em um token de resumo
- sharedKey - lista a chave secreta

Nota: Use um algoritmo de hash seguro mais forte, como SHA256, para a geração de token de resumo.

Este exemplo pressupõe:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Que o servidor web é compatível com C
- Que outro código chama esta classe e passa os parâmetros esperados

Código de amostra

```
 private stringdigestData(string strEncryptionMethod , string message ,
string sharedKey ) {
           UnicodeEncoding myUnicodeEncoding  = new UnicodeEncoding
( ) ;

           byte [ ] messageBytes  = System. Text. Encoding. ASCII.
GetBytes (message ) ;
           byte [ ] sharedKeyBytes  = System. Text. Encoding. ASCII.
GetBytes (sharedKey ) ;
           byte [ ] hashedMessage ;

           string b64SHA1Message ;

            if (this. DEBUG ) {
               TextBoxMessage. Text = message ;
               TextBoxSecret. Text = sharedKey ; }

            switch ( (strEncryptionMethod ) )

            { case "SHA1" :

                  HMACSHA1 hmacsha1  = new HMACSHA1 ( ) ;
                  hmacsha1. Key = sharedKeyBytes ;
                  hashedMessage  = hmacsha1. ComputeHash
(messageBytes ) ;
                  b64SHA1Message  = Convert. ToBase64String
(hashedMessage ) ; if (this. DEBUG ) TextBoxDigest. Text = Convert.
ToString (hashedMessage ) ; break ;

               case "MD5" :

                  HMACMD5 hmacmd5  = new HMACMD5 (sharedKeyBytes ) ;
                  hashedMessage  = hmacmd5. ComputeHash
(messageBytes ) ;
                  b64SHA1Message  = Convert. ToBase64String
(hashedMessage ) ; if (this. DEBUG ) TextBoxDigest. Text = Convert.
ToString (hashedMessage ) ; break ;

               default :

                  b64SHA1Message  = "Unknown Encryption Method" ;
break ;

            }


           TextBoxBase64. Text = b64SHA1Message ; return
b64SHA1Message ;

        }
```

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Segurança de serviços da Web

Aplique a segurança usando autenticação básica, autenticação mútua ou WS-Security.

Explore a segurança da Web	Configure a autenticação mútua
Conheça os recursos e os valores comerciais da segurança de serviços da Web.	Use a autenticação mútua para estabelecer confiança, trocando certificados de SSL (Secure Sockets Layer).

Explorar a segurança de serviços da web

Aplique a segurança usando autenticação básica, autenticação mútua ou WS-Security.

Autenticação básica

Para impor a autenticação básica a cada solicitação de um documento WSDL ou publicação de mensagens de SOAP, é necessário definir a propriedade *glide.basicauth.required* como `verdadeira`. Se você fizer isso, cada solicitação WSDL ou SOAP terá que conter o cabeçalho "Autorização", conforme especificado no protocolo Autenticação básica. Uma vez que a solicitação não é interativa, o cabeçalho **Autorização** é sempre necessário durante uma solicitação.

O fornecimento de informações de autenticação básica, necessárias ou não, tem a vantagem adicional de que os dados criados ou atualizados como resultado da invocação do serviço Web são feitos em nome do usuário fornecido nas credenciais de autenticação básica. Como exemplo, ao criar um Registro de incidente, os campos de diário têm a ID do usuário autenticado básico, em vez do usuário **Convidado** padrão.

Para que o cabeçalho de autorização ignore as regras de capitalização, use a propriedade *glide.security.script.include.name.case.insensitive.list*. É possível modificar esta propriedade na tabela Propriedades do sistema [sys_properties] e adicionar as inclusões de script necessárias para processar a autenticação. Por padrão, esta propriedade tem os valores:

- BasicAuth
- CustomAuth

Adicione outras inclusões de script conforme necessário.

É possível implementar a seguinte função para fornecer autenticação básica ao usar as bibliotecas Perl e SOAP::Lite:

```
sub SOAP :: Transport :: HTTP :: Client :: get_basic_credentials { return
 'user_name' => 'password' ; }
```

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Ao usar o C# .NET versão 2005 ou anterior, é possível aproveitar as vantagens do objeto Credenciais, por exemplo:

```
System.Net . ICredentials cred  = new System.Net . NetworkCredential
 ( "user_name",  "password" ) ;

service . ServiceNow proxy  = new service . ServiceNow ( ) ;
service . get getService  = newservice . get ( ) ;
service . getResponse getServiceResponse  = new service . getResponse
 ( ) ;

 try {
  proxy . Credentials = cred ;
  getService . sys_id = "bf522c350a0a140701972dbf876f1610" ;
  getServiceResponse  = proxy . get (getService ) ; catch (Exception
 ex ) { }
```

- Ao usar o C# .NET versão 2008, é possível aproveitar as vantagens do objeto ClientCredenciais, por exemplo:

```
Demo_Incident. ServiceNowSoapClient client  = new Test08WebService .
 Demo_Incident . ServiceNowSoapClient ( ) ;
client . ClientCredentials . UserName . UserName = "admin" ;
client . ClientCredentials . UserName . Password = "admin" ;
```

Em seguida, no arquivo app.config, procure o seguinte e altere `Nenhum` para `Básico`:

```
<transport clientCredentialType= "None" proxyCredentialType= "None"
 realm= "" />
```

- Ao usar o VB .NET, aproveitar as vantagens do objeto Credenciais seria algo como:

```
Sub Main()
         Dim cred  As New System.Net.NetworkCredential( "user_name",
 "password")

         Dim proxy  As New VB_Democm.incident.ServiceNow
         Dim getIncident  As New VB_Democm.incident. get Dim
 getResponse  As New VB_Democm.incident.getResponse

        proxy.Credentials = cred

        getIncident.sys_id =  "[your sysID here]"

        getResponse = proxy. get(getIncident)

     End Sub
```

A resposta resultante quando a autenticação básica é ativada e nenhuma credencial é fornecida é algo como:

```
<html> <head > <title >Apache Tomcat/5.0.28
 - Error report </ title > <style > <!--H1
 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525
D76;font-size:22px;}    H2
 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525
D76;font-size:16px;}    H3
 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525
```

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

```
D76;font-size:14px;}    BODY
 {font-family:Tahoma,Arial,sans-serif;color:black;background-color:whit
e;}    B
 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525
D76;}    P
 {font-family:Tahoma,Arial,sans-serif;background:white;color:black;fo
nt-size:12px;}   A {color : black;}   A.name {color : black;}
   HR {color : #525D76;}--> </ style > </ head > <body > <h1 >HTTP
 Status 401 -\ </ h1 > <HR size = "1" noshade = "noshade" > <p >< b
 >type </ b > Status report </ p > <p >< b >message </ b > <u >< / u
 >< / p > <p >< b >description </ b > <u >This request requires HTTP
 authentication (). </ u >< / p > <HR size = "1" noshade = "noshade" >
 <h3 >Apache Tomcat/5.0.28 </ h3 > </ body > </ html >
```

Configurar autenticação mútua

A autenticação mútua estabelece confiança por meio da troca de certificados SSL (Secure Sockets Layer).

Durante o handshake de SSL, o servidor apresenta seu certificado ao cliente. Posteriormente, dependendo da configuração do servidor, ele pode solicitar um certificado do cliente. O servidor e o cliente executam procedimentos de validação de certificado para garantir a autenticidade e a integridade dos certificados apresentados.

Após uma validação bem-sucedida, se trocam confirmações antes de iniciar a conexão HTTPS.

Os administradores fazem o trabalho preliminar de configurar o armazenamento de chaves do cliente e gerar certificados antes que as solicitações de certificação sejam atendidas.

Aviso: Este recurso permite a autenticação mútua somente em conexões https de saída.

Criação do armazenamento de chaves

No momento|, a instância oferece suporte ao carregamento de um arquivo de armazenamento de chaves Java, que contém uma chave privada e um par de certificados públicos. O certificado público inclui a cadeia completa, inclusive o certificado raiz.

Para configurar o armazenamento de chaves do cliente:

- Você precisa de um certificado assinado por uma autoridade de certificação (CA) de confiança.
- Seu provedor de endpoint de API pode ajudar você a gerar o armazenamento de chaves.

Se você precisar gerar o armazenamento de chaves, o processo envolverá várias etapas usando comandos de interface de linha de comando para gerar um novo arquivo de armazenamento de chaves, criar uma solicitação de assinatura de certificado (CSR) e importar certificados assinados. Antes de importar o certificado primário para o seu domínio, é necessário importar primeiro quaisquer certificados raiz ou intermediários. Veja uma instrução detalhada:

1. Gere um armazenamento de chaves Java e um par de chaves.

```
keytool -genkey -alias mydomain -keyalg RSA -keystore my.keystore
```

2. Gere um CSR para um armazenamento de chaves Java existente.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

```
keytool -certreq -alias mydomain -keystore my.keystore -file
 mydomain.csr
```

3. Envie o CSR para a autoridade de assinatura do CA assinar e retornar os arquivos de certificado, o que inclui certificados intermediários e raiz junto com o certificado assinado.
4. Importe um certificado CA de autoridade de certificação raiz ou intermediária para um armazenamento de chaves Java existente.

```
keytool -import -trustcacerts -alias root -file Thawte.crt -keystore
 my.keystore
```

Nota: Você pode agrupar todos os certificados em um arquivo e importar. Esta é a opção preferencial. Se você fizer isso, poderá ignorar a etapa 5

```
keytool -import -alias mydomain -file merged.crt -keystore
 my.keystore
```

5. Importe um certificado primário assinado para um armazenamento de chaves Java existente.

```
keytool -import -trustcacerts -alias mydomain -file mydomain.crt
 -keystore my.keystore
```

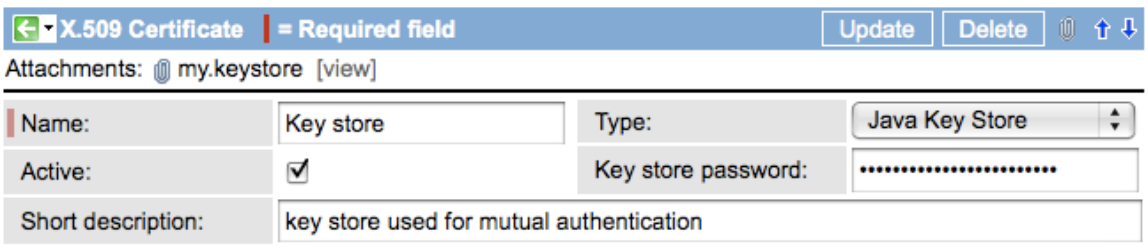
Configuração do armazenamento de chaves

Agora que o armazenamento de chaves foi criado, ele pode ser carregado para a tabela Certificados. Na página **Definição do sistema** > **Certificados**, clique em **Novo** e defina os seguintes campos:

- Insira um **Nome** de certificado.
- Armazene o armazenamento de chaves como **Ativo**.
- Defina **Tipo = Java Key Store**.
- Forneça uma **senha de armazenamento de chaves**. Esta é a senha usada para criar o armazenamento de chaves.

Clique em **Enviar** para criar a entrada de armazenamento de chaves Java.

Armazenamento de chave



Especificação de um certificado de servidor confiável

Durante uma conexão SSL de saída (que é uma chamada de serviço Web HTTPS), é possível especificar um certificado fornecido pelo provedor de serviços para garantir a validade do provedor de serviços durante a conexão SSL. Por exemplo, um navegador que tenta se conectar a um serviço seguro com identificação por um certificado.

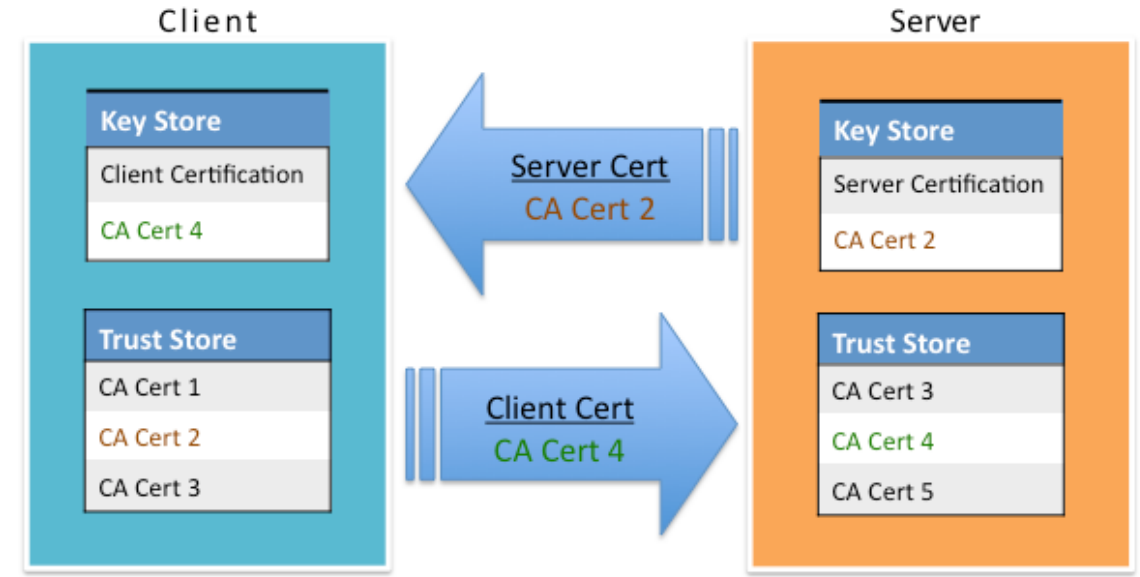
Ao carregar o certificado de servidor confiável, ServiceNow garante que o serviço ao qual ele está se conectando é válido e seguro.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Crie uma nova entrada de certificado com o tipo de "Certificado de armazenamento confiável" e anexe um certificado formatado DER ou copie e cole seu formato PEM no campo **Certificado PEM**.

Perfil de Protocolo

Troca de certificados



- Quando um cliente solicita o certificado do servidor para autenticação, uma solicitação de assinatura de certificado (CSR) é gerada.
- Para responder a um CSR, o servidor gera duas chaves criptográficas exclusivas: uma pública, usada para criptografar mensagens para o servidor e outra privada, usada para descriptografar mensagens. Ambas as chaves são mantidas no armazenamento de chaves.
- As chaves são usadas para descriptografar as mensagens seguras do cliente para que possam ser lidas pelo servidor. Qualquer conexão de saída a resultar em HTTPS verifica a certificação ao validar o armazenamento de chaves oferecendo sua certificação pública e usa os certificados de armazenamento de confiança para, por sua vez, verificar a confiança mútua.
- Para concluir o link seguro entre o cliente e o servidor, o servidor combina o certificado à chave privada correspondente. Uma vez que somente o servidor tem acesso à chave privada, ele pode descriptografar os dados do cliente.

Este é um exemplo de um comando que registra o MYHTTPS com a fábrica de soquetes `com.glide.certificates.DBKeyStoreSocketFactory` na porta 443. A fábrica de armazenamento de chaves do banco de dados é usada durante o processo de troca de SSL para oferecer um certificado de cliente para autenticação mútua.

```
glide.httpclient.protocol.myhttps.class =
 "com.glide.certificates.DBKeyStoreSocketFactory"
glide.httpclient.protocol.myhttps.port = "443"
```

A configuração acima afeta qualquer URL `myhttps://host.domain.com/target` de saída para uso da fábrica de soquete personalizada e troca de certificados durante o SSL.

Nota: Substituir a fábrica de soquetes do protocolo HTTPS padrão afeta todas as conexões HTTPS de saída. Em geral, isso não é desejável.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O servidor responde com o envio de um certificado. Este é um certificado aceito pelo cliente? Em caso afirmativo, uma mensagem será enviada ao servidor, que aceita o certificado, e um canal seguro será iniciado. Se a certificação não for aceita, poderá significar que a autoridade raiz é necessária para a certificação.

Regras da lista de controle de acesso

As regras das listas de controle de acesso (ACLs) restringem o acesso aos dados exigindo que os usuários passem por um conjunto de requisitos antes de interagir com eles.

Explorar Saiba mais sobre a ACL.	Configurar Configurar ACL.
Referência Veja os detalhes sobre o Gerenciador Contextual de Segurança.	Avançado Saiba mais sobre a ACL avançada.

Como explorar listas de controle de acesso

Explore as ACLs (Access Control Lists, listas de controle de acesso).

Todas as regras da lista de controle de acesso especificam:

- O tipo de decisão, o tipo de regra e a operação que definem a ACL
- O objeto que está sob proteção
- As condições necessárias para acessar o objeto

Componentes da ACL

O tipo de decisão define se os usuários terão permissão para acessar o objeto se as condições forem atendidas ou negará o acesso ao objeto, a menos que as condições sejam atendidas.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tipo de decisão	Descrição
Deny-Unless	Restrinja o acesso ao recurso, negando o acesso explicitamente a menos que as condições sejam aprovadas. Para obter mais informações, consulte #unique_1366_Connect_42_section_qnd_snl_zbc.
Allow-If	Permita o acesso ao recurso se as condições forem aprovadas.

O objeto é o destino para o qual o acesso precisa ser controlado. Cada objeto consiste em um tipo e nome que identificam exclusivamente uma tabela, campo ou registro específicos. Com o campo Aplica-se a, os usuários têm controle granular sobre os registros específicos aos quais essa ACL se aplicará.

Por exemplo, todas estas entradas especificam um objeto:

Tipo	Nome	Objeto protegido
registro	[incident].[--None--]	A tabela de incidente.
registro	[incidente].[ativo]	O campo "Ativo" na tabela "Incidente".
registro	[incident] Aplica-se a: Prioridade = P1	Somente incidentes de prioridade 1 na tabela de incidentes.
REST_Endpoint	user_role_inheritance	O registro para a Scripted REST API user_role_inheritance.

Cada operação descreve uma ação válida que o sistema pode executar no objeto especificado. Alguns objetos, como registros, oferecem suporte a várias operações, enquanto outros objetos, como REST_Endpoint, oferecem suporte somente a uma operação.

Por exemplo, todas essas entradas especificam uma operação:

Tipo	Nome	Operação	Operação protegida
registro	[incidente].[--Nenhum --]	criar	Criando registros na tabela de incidente.
registro	[incidente].[ativo]	gravar	Atualizando o campo Ativo na tabela de Incidente.
REST_Endpoint	user_role_inheritance	executar	Executar a Sripted REST API user_role_inheritance.

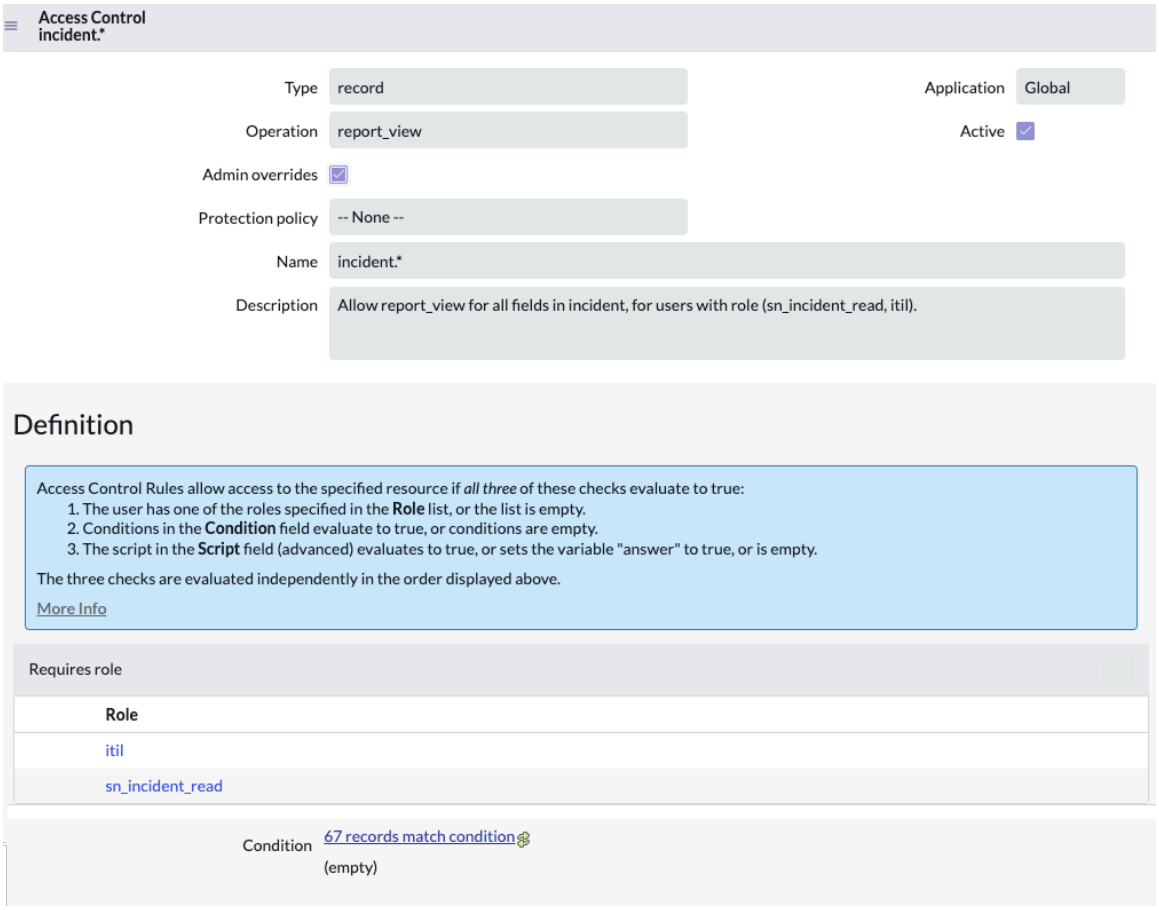
As condições especificam em que momento alguém pode acessar a operação e o objeto nomeados. Os administradores de segurança podem especificar requisitos das condições adicionando:

- Uma ou mais funções do usuário na lista **Requer função**.
- Um ou mais atributos de segurança que precisam ser avaliados como verdadeiros.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Uma ou mais condições de dados.
- Um script que é avaliado como verdadeiro ou falso ou define a variável `answer` como verdadeira ou falsa.

Para ter acesso a um objeto e uma operação, um usuário deve ser aprovado em todas as condições relacionadas em um controle de acesso. Por exemplo, este controle de acesso restringe o acesso às operações de exibição na tabela de incidentes.



Para atualizar um registro na tabela de incidentes, um usuário deve ter as funções listadas e o registro deve atender à condição.

Tipo de condição	Requisito	Descrição
Requer função	**Requer função**:itil	Permita que somente usuários com a função itil atualizem incidentes.
Atributos de segurança	UserIsAuthenticated	Somente usuários autenticados podem atualizar incidentes.
Condição de dados	[Incident state] [is not] [Closed]	Permita atualizações somente em registros de incidentes ativos.

Comportamento padrão de negação

Por padrão, o mecanismo de ACL negará o acesso completamente se uma ACL estiver vazia ou for inválida. As ACLs vazias são definidas como ACLs sem um ou mais destes componentes:

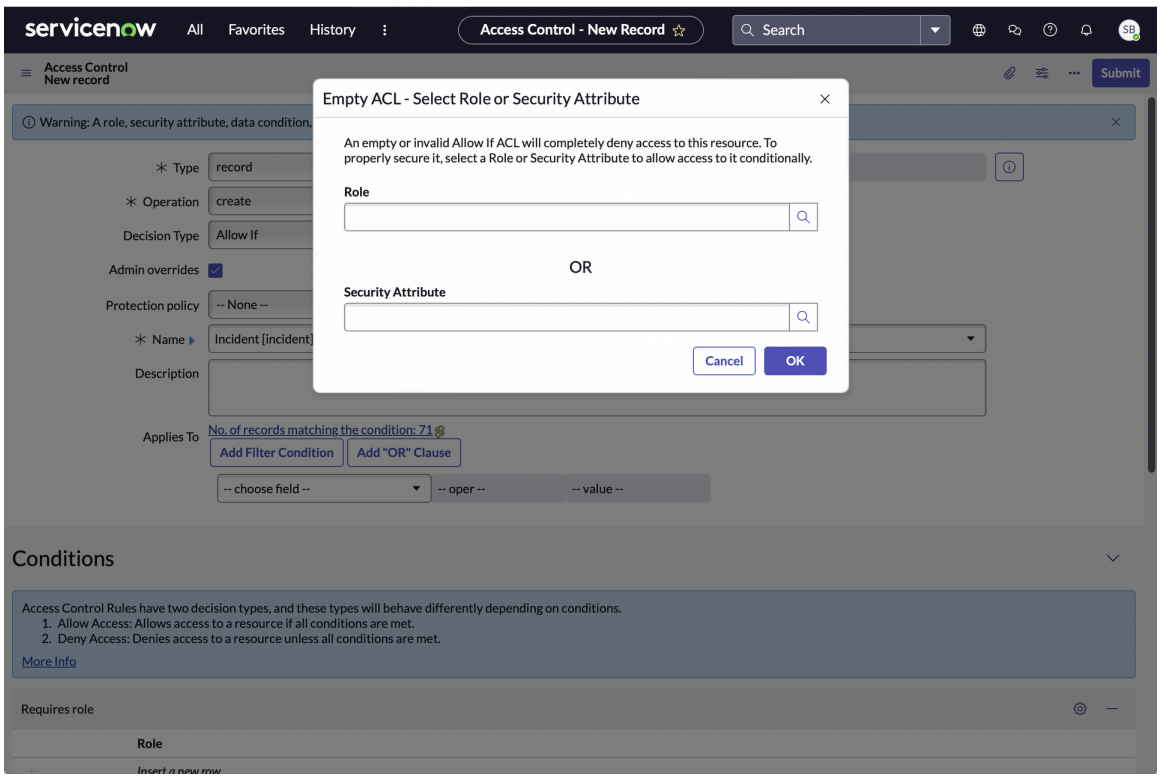
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Função definida
- Atributo de segurança
- Condição de dados
- Script

As ACLs inválidas são definidas como:

- ACLs com funções que não existem (por exemplo, não têm uma linha no banco de dados)
- ACLs com atributos de segurança que não existem (por exemplo, não têm uma linha no banco de dados)
- ACLs com um script que contém "answer=true" ou "true"

Se o sistema detectar que o usuário está criando uma ACL, ele solicitará que o usuário selecione uma função ou um atributo de segurança existente.



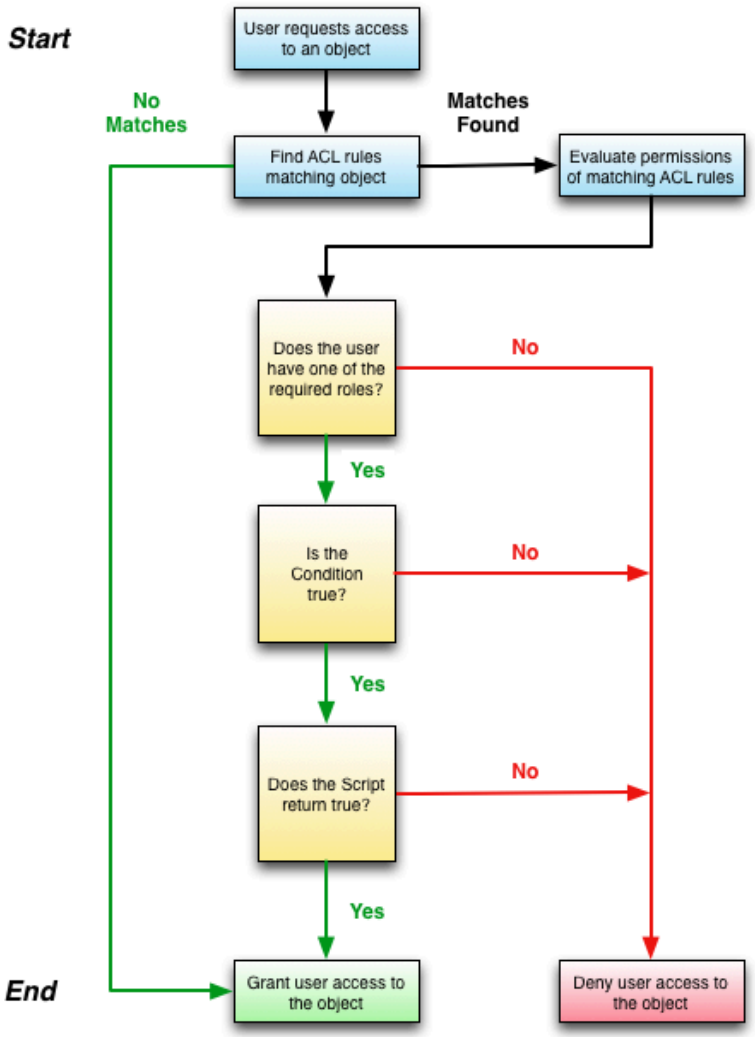
Processo de avaliação da ACL

Uma regra de ACL somente concederá ao usuário o acesso a um objeto se ele atender a todas as condições exigidas pela regra de ACL correspondente.

- A condição deve ser avaliada como *verdadeira*.
- O script deve ser avaliado como *verdadeiro* ou retornar uma variável de resposta com o valor *verdadeiro*.
- O usuário deve ter uma das funções na lista de funções necessárias. Se a lista estiver vazia, esta condição será avaliada como *verdadeira*.
- [Somente regras de ACL de registro] As regras de ACL correspondentes em nível de tabela e de campo devem ser avaliadas como *verdadeiras*.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Condições de avaliação da ACL



Sempre que uma sessão solicita dados, o sistema pesquisa regras de controle de acesso que correspondam ao objeto e à operação solicitados. Se houver uma regra de controle de acesso correspondente, o sistema avaliará se o usuário possui as condições necessárias para acessar o objeto e a operação. Se uma regra de controle de acesso especificar mais de uma condição, o usuário deverá atender a todas as condições para ter acesso ao objeto e à operação. A falha em cumprir qualquer condição impedirá que o usuário acesse o objeto e a operação correspondentes.

Se um usuário não atender às condições da primeira regra correspondente, o sistema avaliará as condições da próxima regra correspondente, conforme as especificações da ordem de processamento do controle de acesso. Se o usuário não atender às condições de nenhuma regra de controle de acesso correspondente, o sistema negará o acesso ao objeto e à operação solicitados.

Nota: Se não houver regras de controle de acesso correspondentes para o objeto e a operação solicitados, o sistema concederá ao usuário o acesso a eles. Na prática, é raro o sistema não encontrar regras correspondentes porque o sistema tem um conjunto de regras de controle de acesso padrão que protegem todas as operações de registro.

Os efeitos de ter o acesso negado a um objeto dependem da regra de ACL em que o usuário falhou. Por exemplo, a falha em uma regra de ACL de operação de leitura impede

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

que o usuário veja o objeto. Dependendo do objeto protegido, a regra de ACL oculta um campo em um formulário, oculta linhas de uma lista ou impede que um usuário acesse uma página de IU. A tabela a seguir contém a lista completa de resultados de falha de uma regra de ACL para uma determinada operação e tipo de objeto.

Verificações de ACL de antes e depois da consulta

Sua instância verifica as regras de ACL antes e depois que um usuário faz uma consulta. Uma vez que informações diferentes estão disponíveis antes e depois de uma consulta, os resultados podem ser diferentes.

Verificação de ACL antes da consulta

Antes que a sua instância execute uma consulta ao banco de dados, ela verifica as regras de ACL para cada campo na tabela consultada para determinar quais campos um usuário pode acessar. Esta verificação examina somente as funções do usuário e verifica se essas funções permitem o acesso aos campos. Como essa verificação é executada antes da consulta, a ACL não tem acesso aos registros na tabela, portanto, não pode levar esses dados em conta. Scripts e condições que dependem do conhecimento do conteúdo de um registro não são avaliados.

Se o usuário não tiver acesso de leitura neste ponto, o valor do campo não será mostrado para o usuário.

Verificação de ACL depois da consulta

Após a consulta, sua instância verifica cada registro retornado pela consulta. Durante esta verificação, existe o contexto para a ACL; portanto, as partes de função, condição e script da ACL são avaliadas. Se o usuário não tiver acesso de leitura neste ponto, o valor do campo não será mostrado para o usuário; no entanto, o usuário verá o rótulo do campo se suas funções permitirem o acesso ao campo.

Operação	Resultados da falha de uma regra de ACL no objeto
execute	O usuário não pode executar scripts em um registro ou página de IU.
criar	O usuário não pode ver a ação de IU **Novo** nos formulários. O usuário também não pode inserir registros em uma tabela usando protocolos de API, como serviços da Web. Uma ACL de **criação** com uma condição que exige que um campo contenha um valor específico sempre é avaliada como falsa. Os campos em novos registros são considerados vazios até que o registro seja salvo.
lido	O usuário não pode ver o objeto em formulários ou listas. O usuário não pode recuperar os registros usando protocolos de API como serviços da Web.
gravar	O usuário vê um campo somente leitura em formulários e listas e não pode atualizar registros usando protocolos de API, como serviços da Web.
excluir	O usuário não pode ver a ação de IU **Excluir** a partir dos formulários. O usuário também não pode remover os registros de uma tabela usando os protocolos de API como serviços da Web.
edit_task_relations	O usuário não pode definir relacionamentos entre tabelas de tarefas.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Operação	Resultados da falha de uma regra de ACL no objeto
edit_ci_relations	O usuário não pode definir relacionamentos entre tabelas Item de configuração [cmdb_ci].
save_as_template	Usado para controlar os campos que devem ser salvos quando um modelo é criado.
add_to_list	O usuário não pode exibir ou personalizar colunas específicas na mecânica da lista.
list_edit	O usuário não pode atualizar registros (linhas) de uma lista.
report_on	O usuário não pode criar um relatório na tabela de ACL. Para obter mais informações, consulte Restringir criação de relatório com uma regra de ACL.
report_view	O usuário não pode exibir o conteúdo de um relatório na tabela de ACL ou no campo de ACL. Para obter mais informações, consulte Relatórios.
personalize_choices	O usuário não pode clicar com o botão direito do mouse em um campo de lista e selecionar **Configurar opções**.

Requisitos de correspondência da ACL para objetos

Tipo de objeto	Regras de ACL correspondentes necessárias para acessar o objeto	Regras de ACL curinga existentes
Inclusões de script acionáveis pelo cliente Processadores	Os usuários devem atender às condições de duas regras de ACL: **1.** Todas as regras de ACL curinga para o objeto (se houver alguma regra de ACL para a operação). **2.** A primeira regra de ACL que corresponde ao nome do objeto (se houver alguma regra de ACL para a operação).	Por padrão, não há regras de curinga (*) para esses tipos de objeto. Se você criar uma regra de ACL curinga para um desses objetos, então a regra de ACL se aplica a todos os objetos deste tipo.
Páginas de IU Registro	Os usuários devem atender às condições de duas regras de ACL: **1.** A primeira regra de ACL que corresponde ao campo do registro (se houver alguma regra de ACL para a operação). **2.** A primeira regra de ACL que corresponde à tabela	Por padrão, existem regras de tabela curinga (*) para as operações de criação, leitura, gravação e exclusão e regras de campo curinga (*.*) para as operações personalize_choices, create e save_as_template. Ao criar uma tabela, crie regras de ACL para a tabela, a menos

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tipo de objeto	Regras de ACL correspondentes necessárias para acessar o objeto	Regras de ACL curinga existentes
	de registro (se houver alguma regra de ACL para a operação).	que queira usar as regras de ACL curinga fornecidas.

Nota: A propriedade (*glide.sm.default_mode*) de comportamento padrão do gerenciador de segurança determina se os usuários podem acessar objetos que correspondem apenas a regras de ACL da tabela curinga. Quando essa propriedade for definida para *Negar acesso*, apenas os administradores poderão acessar os objetos que correspondem às regras de ACL da tabela curinga.

Nota: A regra de ACL do campo curinga (*.*) para a operação de criação reutiliza as mesmas condições da operação de gravação. Isso significa que as condições de criação são iguais às de gravação, a menos que você defina uma regra explícita de ACL para a operação de criação.

Várias regras de ACL no mesmo ponto da ordem de processamento

Se duas ou mais regras corresponderem ao mesmo ponto da ordem de processamento, o usuário deverá cumprir qualquer uma das condições de regras de ACL para acessar o objeto. Por exemplo, se você criar duas regras de ACL de campo para *incident.number*, um usuário que for aprovado em uma regra terá acesso ao campo de número, independentemente de ter falhado em qualquer outra regra de ACL de campo no mesmo ponto da ordem de processamento.

Função necessária

Usuários administradores normais podem exibir e depurar regras de controle de acesso. No entanto, para criar ou atualizar regras de controle de acesso existentes, os administradores devem elevar os privilégios para a função security_admin. Consulte Elevação para uma função privilegiada para obter instruções.

Regras de ACL em aplicações com escopo

É possível criar regras de ACL para objetos que estejam no mesmo escopo que a regra de ACL. Também é possível criar regras de ACL para tabelas com pelo menos um campo que esteja no mesmo escopo que a regra de ACL.

Para tabelas que estão em um escopo diferente do registro de regra da ACL, os tipos de regras são limitados.

- É possível criar uma regra de ACL para qualquer tabela, página de IU ou outro objeto que esteja no mesmo escopo da regra de ACL.
- É possível criar uma ACL para um campo que esteja no mesmo escopo que a regra de ACL.
  - Se a tabela estiver no mesmo escopo, será possível usar um script para avaliar as condições.
  - Se a tabela estiver em um escopo diferente, não será possível usar um script para avaliar as condições.
- Não é possível criar nem modificar regras de ACL para objetos que estão em um escopo diferente da aplicação que você selecionou no seletor de aplicações, inclusive a adição de uma função a uma ACL que está um escopo diferente.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- É possível criar regras de tabela curinga (*) somente no escopo global.
- É possível criar regras de campo curinga (*) somente para tabelas no mesmo escopo da regra de ACL.

Tipos de regra de ACL

Crie regras de ACL em diferentes componentes do sistema.

Regras de ACL de registro

As regras de ACL de registro consistem em nomes de tabela e campo.

- O nome da tabela é a tabela que você deseja proteger. Se outras tabelas se estendem a partir desta tabela, a tabela será considerada uma tabela primária. As regras de ACL para tabelas primárias se aplicam a qualquer tabela que estenda a tabela primária.
- O nome do campo é o campo que você deseja proteger. Alguns campos fazem parte de várias tabelas por causa da extensão da tabela. As regras de ACL para campos em uma tabela primária se aplicam a qualquer tabela que estenda a tabela primária.

As regras de ACL podem proteger as seguintes operações de registro:

Operação	Descrição
criar	Permite que os usuários insiram novos registros (linhas) em uma tabela.
ler	Permite que os usuários exibam registros de uma tabela.
gravar	Permite que os usuários atualizem registros em uma tabela.
excluir	Permite que os usuários removam registros de uma tabela ou eliminem uma tabela.
edit_task_relations	Permite que os usuários estendam a tabela Tarefa [task].
edit_ci_relations	Permite que os usuários estendam a tabela Item de configuração [cmdb_ci].
save_as_template	Permite que os usuários salvem um registro como modelo.
add_to_list	Impede que os usuários exibam ou personalizem colunas específicas na mecânica da lista. **Nota:** Condições e scripts não são compatíveis.
list_edit	Permite que os usuários atualizem registros (linhas) de uma lista.
report_on	Permite que os usuários façam relatórios sobre tabelas.
report_view	Permite que os usuários façam relatórios no campo ACLs.
personalize_choices	Permite que os usuários configurem a tabela ou o campo.
query_exact	Permite que os usuários enviem consultas de correspondência ("é", "não é", "está vazio", etc).
query_range	Permite que os usuários enviem consultas de intervalo ("começa com", "termina com", "contém", etc.) e a classificação é irrestrita.

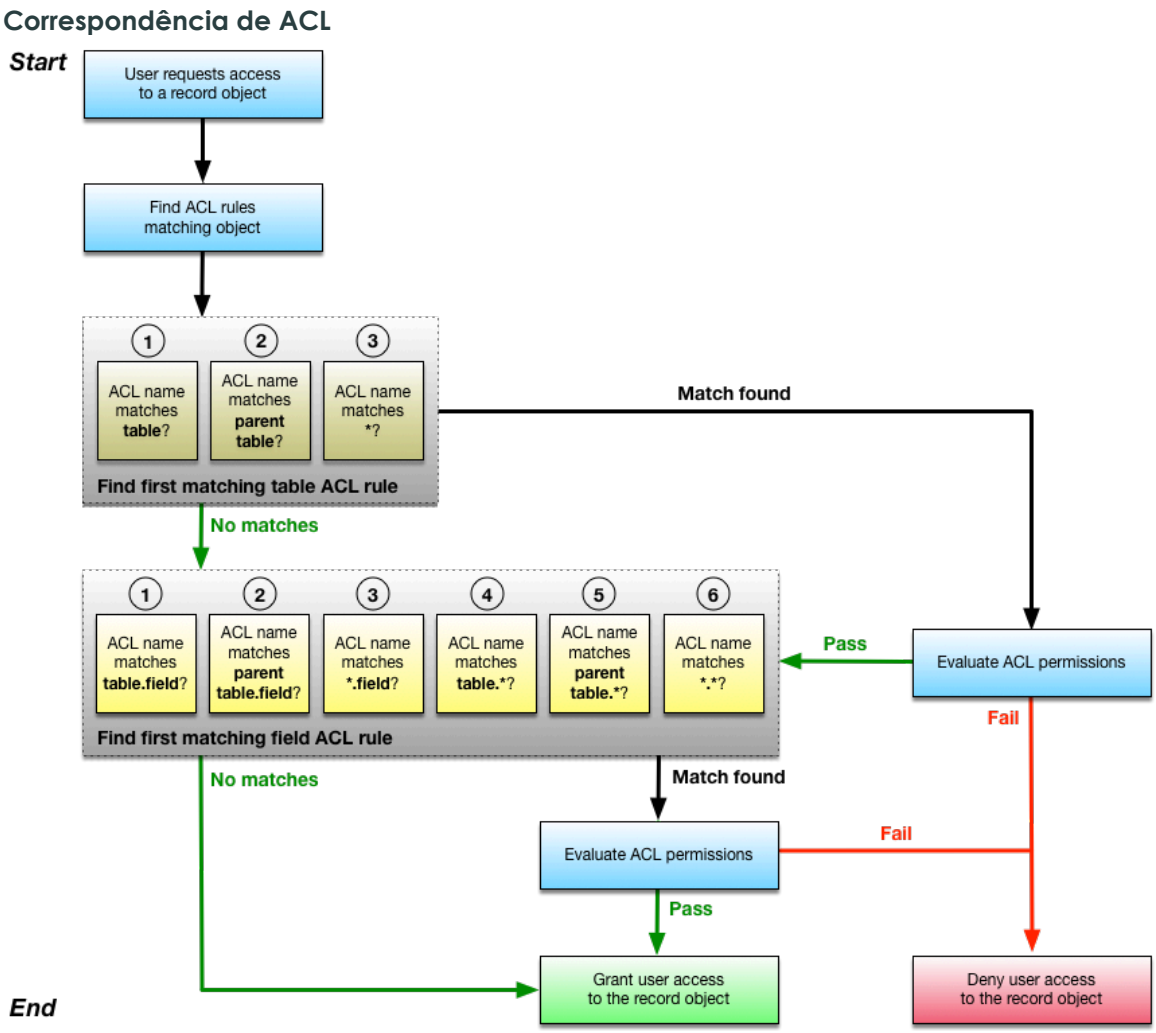
As regras de ACL de registro são processadas na seguinte ordem:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Corresponda o objeto às regras de ACL de tabela.
- Corresponda o objeto às regras de ACL de campo.

Esta ordem de processamento garante que os usuários tenham acesso a objetos mais específicos antes de obter acesso a objetos mais gerais. Um usuário deve passar nas regras de ACL de tabela e de campo para acessar um objeto de registro.

- Se um usuário falhar em uma regra de ACL de tabela, o usuário terá acesso negado a todos os campos da tabela, mesmo se o usuário passar em uma regra de ACL de campo.
- Se um usuário passar em uma regra de ACL de tabela, mas falhar em uma regra de ACL de campo, o usuário não poderá acessar o campo descrito pela regra de ACL de campo.



Regras de ACL do processador

As regras de ACL do processador especificam o processador que você deseja proteger. Para obter uma lista de processadores disponíveis, navegue até **Definição do sistema** > **Processadores**.

Por padrão, uma regra de ACL para EmailClientProcessor é incluída para restringir o cliente de e-mail a usuários com a função itil.

As regras de ACL do processador respeitam a regra STAR (*) se não puderem encontrar uma ACL mais específica para esses recursos.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Regras de ACL da tabela

Primeiro o usuário deve passar na regra de ACL da tabela. Uma vez que o sistema de base inclui regras de ACL de tabela STAR (*) que correspondem a cada tabela, o usuário sempre deve passar pelo menos em uma regra de ACL de tabela. O sistema de base fornece regras de ACL de tabela adicionais para controlar o acesso a tabelas específicas.

As regras de ACL de tabela são processadas na seguinte ordem:

1. Corresponda ao nome da tabela. Por exemplo, incidente.
2. Corresponda ao nome da tabela primária. Por exemplo, tarefa.
3. Corresponda a qualquer nome de tabela (*). Por exemplo, *.

Se um usuário falhar em todas as regras de ACL da tabela, ele não poderá acessar nenhum campo da tabela. Se um usuário passar em uma regra de ACL de tabela, o sistema avaliará as regras de ACL de campo.

Regras de ACL de campo

Depois que um usuário passa em uma regra de ACL de tabela, as regras de ACL de campo são processadas na seguinte ordem:

1. Corresponda ao nome de tabela e de campo. Por exemplo, incident.number.
2. Corresponda ao nome de campo e tabela primária. Por exemplo, task.number.
3. Corresponda a qualquer nome de tabela (*) e de campo. Por exemplo, *.number.
4. Corresponda à tabela e a qualquer campo (*). Por exemplo, incident.*.
5. Corresponda à tabela primária e qualquer campo (*). Por exemplo, task.*.
6. Corresponda a qualquer tabela (*) e qualquer campo (*). Por exemplo, *.*.

Um usuário deve passar na regra de ACL de tabela para ter acesso aos campos da tabela. Por exemplo, primeiro o usuário deve passar na regra de ACL da tabela para que a tabela de incidentes acesse o campo **Número** na tabela de incidentes.

A primeira avaliação de ACL de campo bem-sucedida interrompe o processamento da regra de ACL no nível do campo. Quando um usuário passa em uma regra de ACL de campo, o sistema para de pesquisar outras regras de ACL de campo correspondentes. Por exemplo, se um usuário passar na regra de ACL de campo para incident.number, o sistema interromperá a pesquisa de outras regras de ACL que protegem o campo **Número** na tabela de incidentes.

O acesso às informações de consulta de dados inferidos é restrito a campos protegidos, evitando o retorno de informações previstas.

Regras de ACL da página da IU

As regras de ACL da página da IU especificam a página da IU a ser protegida. Para obter uma lista de páginas de IU disponíveis, navegue até **IU do sistema** > **Página da IU**. Ao definir uma regra de ACL para uma página de IU, use o nome de página com escopo completo. Por exemplo, **x_myapp_mypage**.

Nota: Você pode usar o caractere STAR (*) no campo **Nome** em ACLs de tipo **ui_page** para corresponder a quaisquer páginas de IU.

As regras de ACL da página da IU respeitam a regra STAR (*) se não puderem encontrar uma ACL mais específica para esses recursos. Por exemplo, se você tiver uma página de IU

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

denominada `mysecretpage`, mas não definir uma ACL para esta página de IU, a regra STAR (*) para o processador da página de IU é usada para a verificação de acesso.

As regras de ACL podem proteger a seguinte operação de página de IU:

Operação	Descrição
ler	Permite que os usuários exibam a página da IU.

Script chamável pelo cliente inclui regras de ACL

As regras de ACL de inclusão de script especificam a inclusão de script chamável pelo cliente a ser protegida. Para obter uma lista de inclusões de script disponíveis, navegue até **Definição do sistema** > **Inclusões de script**. Você pode personalizar a lista para mostrar a coluna *Cliente chamável*.

O sistema de base não inclui qualquer regra de ACL para inclusões de script chamável pelo cliente.

As regras de ACL de inclusão de script chamável pelo cliente respeitam a regra STAR (*) se não puderem encontrar uma ACL mais específica para esses recursos.

Controle da ACL de campos de função

Ao avaliar o acesso a um campo de função, além de verificar o acesso ao campo de função em si, o sistema também verifica o acesso aos campos de contribuição da função. Campos de contribuição são aqueles usados como argumentos em uma determinada definição de função.

Para obter mais informações sobre campos de função, consulte Campo de função.

Em Rome e anteriores, o sistema simplesmente verifica o acesso ao campo de função em si (assim como em qualquer outro campo). Se as ACLs nesse campo permitirem o acesso, o usuário receberá o valor resultante, independentemente de ter acesso aos campos de contribuição.

No Xanadu e em versões posteriores, o sistema também requer acesso a todos os campos de contribuição para permitir acesso ao campo da função. Se uma ou mais das ACLs de campo de contribuição recusarem o acesso, o campo de função também recusará o acesso.

As únicas operações afetadas pelo novo requisito são leitura e report_view. Report_view tem seus próprios requisitos adicionais.

Operação	Descrição
operação de leitura	Um usuário tem acesso de leitura a um campo de função somente se as seguintes condições forem verdadeiras: • O usuário tem acesso de leitura ao campo da função. • O usuário tem acesso de leitura a todos os campos de contribuição usados na função.
operação report_view	Um usuário tem acesso report_view a um campo de função somente se todas seguintes condições forem verdadeiras:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Operação	Descrição
	• O usuário tem acesso report_view ao campo da função. • O usuário tem acesso report_view a cada um dos campos de contribuição. • Há uma ACL de leitura habilitada somente por função, sem condições e sem um script, e o usuário tem essa função. • O usuário tem acesso de leitura somente de função aos campos de contribuição, de forma que somente ACLs sem condição ou script podem permitir.

Exemplos

Considerando:

- Tabela: salário
- Colunas: base, bônus, total (todos são números inteiros neste exemplo)
- Campo de função: a coluna total é marcada como um campo de função, com a definição de função `glidefunction:add(base, bonus)`.
- Campos de contribuição: base e bônus, uma vez que já são usados na definição da função
- Funções: salary_admin, bonus_admin

Exemplo 1: todos os campos permitem acesso

ACLs	Resultado
total, base, bônus: leitura e report_view para a função salary_admin, sem condições ou scripts	Um usuário com a função salary_admin recebe acesso de leitura e report_view ao total porque eles possuem a função necessária.

Exemplo 2: o campo de contribuição recusa o acesso de leitura

ACLs	Resultado
• total, base: leitura e report_view para a função salary_admin, sem condições ou scripts • bônus: report_view para função salary_admin , sem condições ou scripts • bônus: leitura para função bonus_admin, sem condições ou scripts	Foi recusado a um usuário com a função salary_admin o acesso de leitura e report_view para total, porque bônus recusa acesso de leitura a suas funções.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exemplo 3: ACL de campo de contribuição possui script

ACLs	Resultado
• total, base: leitura e report_view para a função salary_admin, sem condições ou scripts • bônus: report_view para a função bonus_admin, sem condições ou scripts • bônus: leitura para a função salary_admin, com um script (observe que não importa o que está no script, apenas que ele está lá)	Um usuário com a função salary_admin recebe acesso de leitura para total, porque eles possuem a função necessária para todos os campos. Mas o mesmo usuário com salary_admin não recebe acesso ao report_view, porque a ACL de leitura com o script recusa o acesso por padrão para este caso, mesmo que ele tenha a função necessária.

Security jump-start - Plug-in de regras de ACL

O plug-in de nível de controle de acesso Security Jump Start (regras de ACL) é instalado automaticamente em todas as novas instâncias. Use o plug-in para proteger rapidamente várias tabelas do sistema e agilizar o processo de inicialização da produção de sua organização.

Este plug-in não é destinado a instâncias existentes, já que pode modificar o acesso de segurança a tabelas já em uso em um ambiente de produção. Se um administrador quiser instalar este plug-in em uma instância existente, você deveria realizar testes completos em uma instância de teste primeiro. Isso ajuda a verificar a compatibilidade com a implementação atual da organização.

Se um administrador estiver interessado nas novas regras de ACL fornecidas pelo plug-in, poderá criar manualmente uma ou mais delas em uma instância existente, usando a lista de ACLs como diretriz.

As seguintes ACLs estão incluídas neste plug-in. Selecione o ícone em uma linha de cabeçalho para classificar a coluna em ordem crescente ou decrescente. A chave de operação é a seguinte:

- R=leitura
- W=gravação
- D=excluir
- C=criar

Nome	Operação	Descrição
`cmdb_ci`	WCD	requer função de ativo ou itil para gravar, criar ou excluir registros de Itens de configuração
`cmn_department`	WD	requer função user_admin para gravar ou excluir registros do departamento
`cmn_location`	WC	Requer função user_admin para gravar ou criar registros de local

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome	Operação	Descrição
core_company	WD	requer função user_admin para gravar ou excluir registros da empresa
kb_knowledge	criar	requer função de conhecimento para criar registros de conhecimento
ldap_ou_config	RWCD	requer função user_admin para ler, gravar, criar ou excluir registros de definição OU LDAP
ldap_server_config	RWCD	requer função user_admin para ler, gravar, criar ou excluir registros de servidor LDAP
process_guide	WCD	requer função de administrador para gravar, criar ou excluir registros do Guia de processo
process_step	WCD	requer função de administrador para gravar, criar ou excluir registros da etapa de processo
sc_category	criar	requer função catalog_admin para criar registros de Categoria do catálogo de serviços
sc_category	excluir	requer função catalog_admin para excluir registros da Categoria do catálogo de serviços
sc_category	gravar	requer função catalog_admin para gravar registros de Categoria do catálogo de serviços
sc_cat_item	gravar	requer função catalog_admin para gravar registros de Item do catálogo
sc_cat_item	excluir	requer função catalog_admin para excluir registros de Item do catálogo
sc_cat_item	criar	requer função catalog_admin para criar registros de Item do catálogo
sysevent_email_action	ler	todos os usuários podem ler registros de notificação por e-mail (para fins de assinatura)
sysevent_register	RWCD	requer função de administrador para ler, gravar, criar ou excluir registros do Registro de eventos
sysevent_script_action	RWCD	requer função de administrador para ler, gravar, criar ou excluir registros de Ação de script
syslog	RWCD	requer administrador para ler, gravar, criar ou excluir registros de Entrada de log
sysrule	RWCD	requer administrador para ler, gravar, criar ou excluir registros de regra (notificações por e-mail, ações de e-mails de entrada, regras de aprovação e assim por diante)
sysrule	ler	todos os usuários podem ler registros de notificação por e-mail para (notificações baseadas em assinatura)
sys_app_application	WCD	requer administrador para gravar, criar ou excluir registros da aplicação

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome	Operação	Descrição
sys_app_category	WCD	requer função de administrador para gravar, criar ou excluir registros de Categoria da aplicação
sys_app_module	WCD	requer administrador para gravar, criar ou excluir registros de Módulo
sys_audit	RWCD	requer administrador para ler, gravar, criar ou excluir registros de Auditoria
sys_dictionary	RWC	requer função personalize_dictionary para ler, gravar e criar registros de Dicionário
sys_dictionary.*	ler	a função personalize_dictionary pode ler campos de Dicionário
sys_documentation	excluir	Função personalize_dictionary necessária para excluir registros de Rótulo do Campo
sys_documentation	criar	requer função personalize_dictionary para criar registros de Rótulo do campo
sys_documentation	gravar	Função personalize_dictionary necessária para gravar registros de Rótulo do Campo
sys_gauge	RWCD	requer função de administrador para ler, gravar, criar e excluir registros de Medidor
sys_gauge_count	RWCD	requer função de administrador para ler, gravar, criar ou excluir registros de Contagem de medidor
sys_group_has_role	ler	requer função de itil para visualizar registros de Função do grupo
sys_home	WCD	requer função itil_admin para gravar, criar ou excluir registros da Seção da página de boas-vindas
sys_installation_exit	WCD	requer função de administrador para gravar, criar ou excluir registros de Saída de instalação
sys_job	WCD	requer função de administrador para gravar, criar ou excluir registros de Trabalho do sistema
sys_nav_link	WCD	requer função de administrador para gravar, criar ou excluir registros de Link de navegação
sys_perspective	WCD	requer função de administrador para gravar, criar ou excluir registros da Lista de menus
sys_portal	RWCD	requer função de administrador para ler, gravar, criar ou excluir registros do Portal
sys_portal_page	RWCD	requer função de administrador para ler, gravar, criar ou excluir registros da Página inicial
sys_portal_preferences	RWCD	requer função de administrador para ler, gravar, criar ou excluir registros de Preferências do portal

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome	Operação	Descrição
sys_processor	WC	requer função de administrador para gravar ou criar registros do Processador
sys_properties	WC	requer função de administrador para gravar/ criar registros de Propriedade do sistema
sys_properties_category	WCD	requer função de administrador para gravar, criar ou excluir registros de Categoria da propriedade
sys_report	excluir	funções que podem excluir registros de Relatório (não restringe a exclusão por meio da IU de relatório)
sys_report	gravar	funções que podem gravar registros de Relatório (não restringe a edição por meio da IU de relatório)
sys_report	ler	os usuários podem ler seus próprios registros de Relatório, os de seus grupos e os GLOBAIS (não afeta a exibição na IU de Relatório)
sys_report	ler	funções que podem ler registros de relatório (não restringe a exibição por meio da IU de relatório)
sys_reportroles	ler	requer função de administrador para ler registros de Funções de relatório
sys_script	WCD	requer função de administrador para gravar, criar ou excluir registros de Regra de negócio
sys_script_ajax	WCD	requer função de administrador para gravar, criar ou excluir registros de script AJAX
sys_script_client	WCD	requer função de administrador para escrever, criar ou excluir registros de Script de cliente
sys_script_include	WCD	requer função de administrador para gravar, criar ou excluir registros de Inclusão de script
sys_security_acl	gravar	requer função de administrador para gravar registros de Controle de acesso
sys_security_acl_role	criar	requer função de administrador para criar registros de Funções de acesso
sys_security_acl_role	excluir	requer função de administrador para excluir registros de Funções de acesso
sys_security_acl_role	gravar	requer função de administrador para gravar registros de Funções de acesso
sys_security_operation	excluir	requer função de administrador para excluir registros de Operações de segurança
sys_security_operation	criar	requer função de administrador para criar registros de Operações de segurança
sys_security_operation	gravar	requer função de administrador para gravar registros de Operações de segurança
sys_security_operation	query_range	

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome	Operação	Descrição
sys_security_operation		
sys_security_type	gravar	requer função de administrador para gravar registros de Tipo de segurança
sys_security_type	criar	requer função de administrador para criar registros de Tipo de segurança
sys_security_type	excluir	requer função de administrador para excluir registros de Tipo de segurança
sys_status	criar	requer função de administrador para criar registros de Status do sistema
sys_status	excluir	requer função de administrador para excluir registros de Status do sistema
sys_status	gravar	requer função de administrador para gravar registros de Status do sistema
sys_template	gravar	requer função de template_editor para gravar registros de Modelo
sys_template	criar	requer função template_editor para criar registros de Modelo
sys_template	excluir	requer função template_editor para excluir registros de Modelo
sys_template	ler	requer função template_editor para ler registros de Funções de modelo
sys_ui_action	criar	requer função de administrador para criar registros de ação de IU
sys_ui_action	excluir	requer função de administrador para excluir registros de ação de IU
sys_ui_action	gravar	requer função de administrador para gravar registros de ação de IU
sys_ui_action_view	gravar	requer função de administrador para gravar registros de Ação de exibição de IU
sys_ui_action_view	criar	requer função de administrador para criar registros de Ação de exibição de IU
sys_ui_action_view	excluir	requer função de administrador para excluir registros de Ação de exibição de IU
sys_ui_policy	criar	requer função de administrador para criar registros de Política de IU
sys_ui_policy	excluir	requer função de administrador para excluir registros de Política de IU
sys_ui_policy	gravar	requer função de administrador para gravar registros de Política de IU
sys_ui_policy_action	criar	requer função de administrador para criar registros de Ação de política de IU
sys_ui_policy_action	excluir	requer função de administrador para excluir registros de Ação de política de IU

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome	Operação	Descrição
sys_ui_policy_action	gravar	requer função de administrador para gravar registros de Ação de política de IU
sys_ui_script	gravar	requer função de administrador para gravar registros de Script de IU
sys_ui_script	excluir	requer função de administrador para excluir registros de Script de IU
sys_ui_script	criar	requer função de administrador para criar registros de Script de IU
sys_user	gravar	Usuários sem função só podem atualizar seus próprios registros de usuário
sys_user_grmember	excluir	requer função user_admin para excluir registros de Membro do grupo
sys_user_grmember	gravar	requer função user_admin para gravar registros de Membro do grupo
sys_user_group	criar	Somente funções itil e superiores podem criar registros de grupo
sys_user_group	gravar	Somente funções itil e superiores podem gravar registros de grupo
sys_user_has_role	ler	requer função de itil para visualizar registros de Função do usuário
sys_user_role	criar	requer função de administrador para criar registros de Função
sys_user_role	excluir	requer função de administrador para excluir registros de Função
sys_user_role	gravar	requer função de administrador para gravar registros de Função
sys_user_role_contains	ler	requer função de itil para visualizar registros de Função contida
sys_user_role_contains	gravar	requer função de administrador para gravar registros de Função contida
sys_user_token	RWCD	requer função de administrador para ler, gravar, criar ou excluir registros de Token do usuário

Nota: Para saber mais sobre este plug-in, consulte Security jump start (regras de ACL) (proteção de segurança da instância) em Configurações de proteção de segurança da instância.

Configuração de uma regra de ACL

Configure uma regra de ACL personalizada para proteger o acesso a novos objetos ou para mudar o comportamento de segurança padrão.

Antes de Iniciar

Função necessária: security_admin

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

Para criar regras de ACL, você deve elevar os privilégios para a função security_admin.

Para tabelas que estão em um escopo diferente do registro de regra da ACL, os tipos de regras são limitados. Para que as tabelas Mestre de escopo derivem e executem ACLS com escopo, defina a *glide.enforce_security_scope.<scope_name>* propriedade como **true**. Isso garante que as ACLs no escopo global não correspondam quando houver ACLs específicas do escopo criadas na tabela relevante. Os exemplos ocorrem ao proteger dados em tabelas de aplicação compartilhadas no escopo Global, como tabelas sys_attachment ou question_answer.

Procedimento

1. Eleve funções de privilégios para a função security_admin.
2. Navegue até **Segurança do sistema** > **Controle de acesso (ACL)**.
3. **Dica:** Ao criar uma nova ACL, é útil revisar a Deny-Unless ACL.

   Clique em **Nova**.
4. Preencha o formulário.

Campos de controle de acesso

Campo	Descrição
Tipo	Selecione o tipo de objeto que esta regra de ACL protege. O tipo de objeto determina como o objeto é nomeado e quais operações estão disponíveis. Este campo se torna leitura somente depois que a regra de ACL é criada. Se você quiser mudar o tipo, deve excluir a ACL e criar uma nova com o tipo correto.
Operação	Selecione a operação que esta regra de ACL protege. Cada tipo de objeto tem sua própria lista de operações. Uma regra de ACL só pode proteger uma operação. Para proteger várias operações, crie uma regra de ACL separada para cada uma.
Sobreposições do administrador	Marque esta caixa de seleção para que os usuários com a função de administrador sejam aprovados automaticamente na verificação de permissões desta regra de ACL. Os usuários administradores são aprovados independentemente das restrições de script ou função aplicáveis. No entanto, a função **nobody**, que apenas o ServiceNow pessoal pode atribuir, tem precedência sobre a opção de substituição do administrador. Se uma ACL for atribuída à função **nobody**, os usuários administradores não poderão acessar o recurso mesmo quando as **Sobreposições do administrador** forem selecionadas. Consulte Funções do sistema base. Desmarque esta caixa de seleção se os administradores tiverem que atender às permissões definidas nesta regra de ACL para obter acesso ao objeto protegido. Como os administradores sempre são aprovados nas verificações de função (consulte a descrição do campo **Requer função**), use o construtor de condição ou campo **Script** para criar uma verificação de permissão na qual os administradores deve estar aprovados.
Ativo	Marque esta caixa de seleção para aplicar esta regra de ACL.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Avançado	Marque esta caixa de seleção para exibir o campo **Script**. **Importante:** Se houver script no campo **Script**. Este script é executado mesmo se o campo não for exibido no formulário.
Nome	Insira o nome do objeto que está sendo protegido, o nome do registro ou os nomes da tabela e do campo. Quanto mais específico for o nome, mais específica será a regra da ACL. É possível usar o caractere curinga de asterisco (*) no lugar de um registro, tabela ou nome de campo para selecionar todos os objetos que correspondem a um tipo de registro, todas as tabelas ou todos os campos. Você não pode combinar um caractere curinga e uma pesquisa de texto. Por exemplo, inc* não é um nome de regra de ACL válida, mas incident.* e *.number são nomes de regra de ACL válidos. **Nota:** Clique no triângulo azul para inserir manualmente o nome do registro ou os nomes de tabela e campo do objeto sendo protegido. Use esta opção para proteger um objeto que não aparece na lista suspensa.
Descrição	Insira uma descrição do objeto ou das permissões que esta regra de ACL protege.
Requer função	Use esta lista para especificar as funções que um usuário deve ter para acessar o objeto. Se você listar várias funções, um usuário com qualquer uma das funções listadas poderá acessar o objeto. A lista *Requer função* aparece como uma lista relacionada. **Nota:** Os usuários com a função de administrador sempre passam nesta verificação de permissões porque a função de administrador concede automaticamente aos usuários todas as outras funções.
Condição	Use este construtor de condição para selecionar os campos e valores que devem ser verdadeiros para que os usuários acessem o objeto.
Script	Insira um script personalizado que descreva as permissões necessárias para acessar o objeto. O script pode usar os valores das *atuais* e *anteriores* Variáveis globais em regras de negócio bem como propriedades do sistema. O script deve gerar uma resposta verdadeira ou falsa de uma de duas maneiras: ◦ retornar um conjunto de variáveis de *resposta* definida como um valor verdadeiro ou falso ◦ avaliar como verdadeiro ou falso Em ambos os casos, os usuários só ganham acesso ao objeto quando o script é avaliado como verdadeiro e o usuário atende a todas as condições da regra de ACL. As condições e o script devem ser avaliados como verdadeiros para que um usuário acesse o objeto.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: Se o item avaliado estiver em uma lista relacionada, o **atual** apontará para o item no qual está a lista relacionada, não para o item atual ao qual a ACL se destina. No entanto, se o item para o qual você está avaliando a ACL não estiver em uma lista relacionada, o **atual** apontará para o item real.

5. Clique com o botão direito no cabeçalho do formulário e selecione **Salvar**.

Deny-Unless ACL

Conheça os detalhes sobre as ACLs Deny-Unless.

As ACLs Deny-Unless são avaliadas com uma abordagem de "negar, a menos que". Elas definem os usuários que NÃO serão negados. Em outras palavras, o usuário terá o acesso negado, **a menos que** atenda aos requisitos de função, condição e script.

Importante: Na avaliação de ACL, as ACLs Deny-Unless terão prioridade em relação às ACLs Allow-If, já que serão avaliadas primeiro.

Uma ACL Deny-Unless produz dois resultados

Resultado da avaliação	Resultado
Aprovado	Houve o atendimento dos requisitos definidos de funções, condições de dados, atributos de segurança e script. A ACL prossegue para avaliação adicional **Importante:** As ACLs Allow-If ainda devem conceder acesso para que o indivíduo possa acessar o recurso.
Falha	A ACL Deny-Unless é marcada como falha e o acesso será negado.

Abaixo, há um exemplo explicativo de uma ACL Deny-Unless:

- A ACL tem as funções `sn_hr_core.manager` e `itil`
- A condição tem o campo "ativo" = `verdadeiro`
- O script tem a resposta = `gs.isLoggedIn();`

O usuário terá o acesso negado, a menos que atenda a todos os três requisitos dessa ACL. Para que essa ACL Deny-Unless seja aprovada, um usuário precisa das funções `sn_hr_core.manager` ou `itil`, estar acessando um registro que tenha o campo "ativo" = `verdadeiro` e estar conectado. A ACL Deny-Unless apresentará falhará se qualquer um dos três requisitos não for atendido.

ACLs de consulta

As ACLs de consulta permitem que você defina um controle de acesso mais granular, definindo explicitamente quem pode consultar os dados.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O que é uma ACL de consulta

As ACLs de consulta têm sua operação definida como `query_range` ou `query_match`. As ACLs de consulta permitem um controle mais específico das consultas do usuário, restringindo ou habilitando o acesso com base na configuração. As ACLs de consulta são ferramentas poderosas contra ataques de consulta ocultos, em que um invasor consulta os dados de maneira oculta para extrair informações dos resultados, mesmo quando não consegue ver os valores.

Quando usar uma ACL de consulta

Sempre que uma coluna tiver valores confidenciais e permitir acesso parcial/condicional aos dados, uma ACL de consulta deve ser considerada e implementada conforme necessário com base na confidencialidade dos dados. Sempre que houver um acesso parcial/condicional às linhas e suas colunas nas tabelas, principalmente quando esse acesso não for imposto por filtros de dados, as ACLs de consulta devem ser implementadas conforme necessário com base na confidencialidade dos dados.

Nota: Considere ACLs de consulta quando alguns usuários tiverem acesso a algumas linhas ou colunas e não a outras.

Example: Controle de consulta de folha de pagamento

Posso ver uma linha na tabela de folha de pagamento com o meu salário, mas não há motivo para eu poder emitir consultas de intervalo para consultar usuários com um salário dentro de 2 limites. Uma ACL `query_range` no salário me impediria de emitir essa consulta.

Example: Controle de consulta de RH

Posso ver todos os hr_profiles, mas só posso ver o SSN por conta própria. Não tenho nenhum negócio consultando SSN e as ACLs de consulta devem me impedir de executar consultas em SSN de outros perfis de RH para tentar extrair mapeamentos de SSN.

Comportamento das ACLs de consulta

As ACLs de consulta usam as operações `query_match` e `query_range` para um comportamento de consulta de tabela seguro e granular. Os comportamentos são descritos abaixo:

`query_match`

`query_match` é composto por: EQUAL, NOT_EQUALS, IN, NOT_IN, SAMEAS, NSAMEAS, ANYTHING, ISEMPTYSTRING, ISEMPTY, ISNOTEMPTY, ISNULL, ISNOTNULL. `query_match` é composto pelos "operadores seguros", no sentido de que são criados para buscar registros específicos e não podem ser explorados para retornar outros.

Resultado da avaliação	Resultado
Aprovado	O usuário pode enviar consultas de correspondência
Falha	O usuário não poderá enviar consultas de correspondência: • EQUALS • NOT_EQUALS • IN

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países. Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resultado da avaliação	Resultado
	• NOT_IN • SAMEAS • NSAMEAS • ANYTHING • ISEMPTYSTRING • ISEMPTY • ISNOTEMPTY • ISNULL • ISNOTNULL

`query_range`

`query_range` é composto por todos os outros (STARTS_WITH, CONTAINS, >=, <= etc), que são mais perigosos, pois permitem que os usuários consultem mais registros ajustando os valores de limite.

Resultado da avaliação	Resultado
Aprovado	O usuário pode enviar consultas de intervalo e a classificação é irrestrita
Falha	O usuário não poderá enviar consultas de intervalo com (STARTS_WITH, CONTAINS, >=, <= etc. A classificação por coluna é restrita

Importante:

As ACLs de consulta (query_match e query_range) têm como padrão uma ACL star.star que delega acesso de leitura. Isso significa que, onde as ACLs são aplicadas em consultas, se nenhuma ACL de consulta tiver sido criada, o acesso de leitura à coluna será avaliado; se as ACLs de consulta forem definidas, elas substituirão o comportamento padrão.

Proteja os registros em uma lista integrada

Para aplicar segurança aos registros em listas integradas, limite a edição e a exclusão de registros em listas integradas a funções específicas.

Antes de Iniciar

Função necessária: security_admin

Procedimento

1. Navegue até **Todos** > **Segurança do sistema** > **Controle de Acesso (ACL)**.
2. Abra o registro **Gravar** ou **Excluir** para a tabela apropriada.
3. Na seção Requer Função do formulário, adicione as funções com permissão de gravação ou exclusão para essa tabela.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Salve as mudanças.
   Quando os registros da tabela associada aparecem em uma lista integrada, as opções de edição e exclusão ficam disponíveis somente para usuários com as funções especificadas.

Contextual Security Manager

O Contextual Security Manager protege seus dados ao controlar a autorização de leitura, gravação, criação e exclusão.

Vantagens principais

O Contextual Security Manager reconhece a hierarquia da tabela do sistema, permitindo que você crie regras de segurança específicas para um campo com base em onde ele é exibido na hierarquia. Os benefícios do Contextual Security Manager incluem:

- **Segurança contextual**: proteja um registro com base no conteúdo do registro.
- **Segurança hierárquica**: aplique regras de segurança a qualquer nível na hierarquia de objetos.

Protegendo campos e tabelas

Com o Simple Security Manager legado, você pode proteger campos e tabelas adicionando funções à entrada de dicionário apropriada. Com o Contextual Security Manager, essas funções de dicionário não são mais testadas. Em vez disso, o sistema procura pelas regras de ACL em campos e tabelas.

⚠ **Aviso:** Depois de instalar o Contextual Security Manager, você deve proteger campos e tabelas por meio de regras de ACL. Mesmo se você configurar o layout do formulário e o formulário de dicionário e adicionar funções a uma entrada de dicionário, não ocorrerá nenhuma mudança nos direitos.

Segurança contextual e funções

Você pode conceder funções a usuários ou grupos. No entanto, depois de instalar o Gerenciador de segurança contextual, o campo de **funções** no registro do usuário não é mais verificado e não aparece mais nos formulários de usuário e grupo. Em vez disso, você deve adicionar funções à lista relacionada em vez de ao registro de usuário ou grupo.

As aplicações e os módulos contêm listas das funções necessárias para exibi-los. Por exemplo, para exibir a aplicação de definição do sistema, a função de administrador é necessária. Direitos de segurança para aplicações e módulos ainda são definidos usando matrizes de função.

Os itens do catálogo e as variáveis do catálogo contêm listas das funções necessárias para exibi-los. Direitos de segurança para itens do catálogo e variáveis do catálogo ainda são definidos por meio dessas matrizes de função.

No Gerenciador de segurança contextual, um grupo ainda herda automaticamente qualquer função concedida ao grupo quando o sinalizador de herança da função estiver definido como *verdadeiro*.

Ativando o Contextual Security Manager

O Gerente de segurança contextual está ativo no sistema de base. Se houver muitas entradas duplicadas na tabela Funções do usuário, talvez seja necessário fazer upgrade

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

para a Segurança contextual: Role Management V2 para eliminar funções duplicadas. Os plug-ins incluem:

Contextual Security: Role Management [com.glide.role_management]

Fornece funcionalidade de segurança contextual. Este plug-in é instalado automaticamente.

Contextual Security: Role Management V2 [com.glide.role_management.inh_count]

Impede entradas duplicadas causadas por funções herdadas na tabela Funções do usuário [sys_user_has_role]. Este plug-in é instalado automaticamente em novas instâncias e pode ser ativado para upgrades. O plug-in Segurança contextual: Role Management Enhancements é uma versão anterior deste plug-in. O plug-in Role Management Enhancements não inclui o script RoleManagementVerify(). Este script retorna uma lista de mudanças que um upgrade executará, permitindo que você monitore as mudanças feitas pelo plug-in.

Nota: Depois de ativar o Role Management V2, você deve definir a propriedade de sistema glide.role_management.v2.audit_roles para permitir que a tabela Funções de auditoria crie registros de auditoria relacionados às funções do usuário. Para saber mais sobre como definir esta propriedade e sobre a tabela Funções de auditoria, consulte:

- Habilite a auditoria de função com a Contextual Security: Role Management V2.
- Plug-in Contextual Security: Role Management em Configurações de proteção de segurança da instância
- Funções do usuário de auditoria

Impedir entradas duplicadas com Contextual Security: Role Management V2

As funções herdadas de outras funções são adicionadas como entradas individuais na tabela Funções do usuário [sys_user_has_role], podendo fazer com que uma função tenha entradas duplicadas. Contextual Security: Role Management V2 elimina essas entradas duplicadas e evita duplicações futuras.

Elimine as entradas duplicadas por meio da contagem de herança

O Contextual Security: Role Management V2 usa a coluna Contagem de herança (inh_count) para rastrear o número de vezes que uma função é herdada de outra função ou grupo. Na tabela Funções do usuário [sys_user_has_role], um usuário pode herdar uma função específica apenas uma vez, eliminando entradas duplicadas. A coluna Contagem de herança (inh_count) é somente leitura e calcula o número de vezes que o usuário herda uma função.

Mudanças de ativação

O Contextual Security: Role Management V2 é instalado automaticamente em novas instâncias e pode ser ativado para upgrades. Quando ativado, o Contextual Security: Role Management V2 substitui a Contextual Security e a Contextual Security: Role Management Enhancements.

Quando o Contextual Security: Role Management V2 está ativado, as seguintes colunas são descontinuadas, mas permanecem na tabela Funções do usuário para compatibilidade com versões anteriores

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

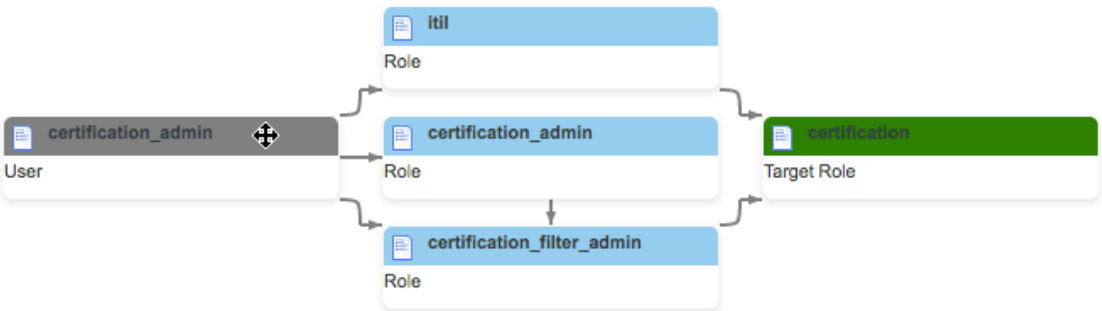
- granted_by (usado apenas pela Delegação de função)
- included_in_role
- included_in_role_instance

Aviso: Se essas colunas estiverem em uso em algum script personalizado em sua instância, não faça upgrade para o Role Management V2.

Visualize a herança da função por meio do mapa de herança de função

O Mapa de herança de função exibe uma representação visual das funções herdadas. Você pode usar este mapa para entender as funções representadas na coluna Contagem de herança (inh_count). Para exibir o mapa de herança de função, configure a tabela Funções do usuário [sys_user_has_role] para exibir a coluna Mapa de herança de função.

Mapa de Herança de função



Faça upgrade para Contextual Security: Role Management V2

A Contextual Security: Role Management V2 é instalada automaticamente em novas instâncias. Você pode fazer upgrade da Contextual Security: Role Management para a Contextual Security: Role Management V2 para eliminar funções duplicadas na tabela Funções do Usuário e evitar duplicações futuras.

Antes de Iniciar

Função necessária: admin, security_admin
Você deve ter função de administrador e Elevação para uma função privilegiada para obter a função security_admin efetiva.

Nota: Antes de atualizar para Contextual Security: Role: Management V2, é necessário habilitar a tabela Funções de auditoria para criar registros de auditoria relacionados às funções do usuário. Para saber mais sobre como definir a propriedade do sistema necessária, consulte Habilite a auditoria de função com a Contextual Security: Role Management V2.

Por Que e Quando Desempenhar Esta Tarefa

Este procedimento descreve como fazer o upgrade da sua função de Segurança contextual e como ativar os plug-ins relacionados descritos na tabela a seguir.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Plug-ins para Contextual Security: Role Management V2

Plug-in	Descrição
Contextual Security: Role Management V2 [com.glide.role_management.inh_count]	Impede entradas duplicadas na tabela Funções do usuário [sys_user_has_role]. A função security_admin ou um usuário com privilégios elevados é necessário para ativar o plug-in ou entrar em contato com Suporte e atendimento ao cliente.
Contextual Security: Role Management V2 REST API [com.glide.role_management.inh_count.rest_api]	Habilita a funcionalidade de API para gerenciamento de funções.

Antes de atualizar a Contextual Security: Role Management para Contextual Security: Role Management V2, teste os resultados de up upgrade executando o script. O script retorna uma lista de mudanças que um upgrade executará. Se as mudanças forem aceitas, instale o plug-in Segurança contextual: Role Management V2. Se as mudanças não forem aceitas, não instale o plug-in Segurança contextual: Role Management V2. Como alternativa, você pode executar o upgrade e fazer as mudanças necessárias manualmente.

Procedimento

1. Teste o impacto de um upgrade antes de atualizar, executando o script a seguir.

a. Navegue até **Definição do sistema** > **Scripts - Plano de fundo**.

b. Execute o script a seguir no escopo global.

```
new RoleManagementVerify().verifyInheritedRoles();
```

Para tabelas sys_user_has_role grandes, a execução pode levar várias horas para ser concluída. Não edite ou adicione funções de usuário durante esse tempo.
Exemplo de resultado com base em dados de teste:

```
*** Script: 2016-12-01 19:58:54 Starting checking of inherited roles
 for all users...
*** Script: User: itam, inherited roles to be ADDED:
 financial_mgmt_user
*** Script: User: bernard.laboy, inherited roles to be DELETED:
 api_analytics_read,pa_viewer,rest_api_explorer,a123
*** Script: User: bernard.laboy, inherited roles to be ADDED:
 dependency_views
*** Script: Number of inherited-role records in sys_user_has role,
 current: 260, after re-calculation: 258
*** Script: Number of users with discrepancies for inherited roles: 2
*** Script: 2016-12-01 19:58:55 Finished checking of inherited roles
 for all users!
```

c. Avalie os resultados do script para determinar se as mudanças propostas são aceitáveis.

2. Ative o plug-in Contextual Security: Role Management V2.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Importante: A função security_admin ou um usuário com privilégios elevados é necessário para ativar o plug-in ou entrar em contato com Suporte e atendimento ao cliente.

a. Navegue até **Definição do sistema** > **Plug-ins**.

b. Encontre e clique no nome do plug-in.

c. No formulário Plug-in do sistema, revise os detalhes de plug-in e, em seguida, clique no link relacionado **Ativar/Fazer upgrade**.

d. Clique em **Ativar**.

Resultados

Depois de ativar o Role Management V2,, as mudanças descritas no resultado do script são aplicadas. A coluna Contagem de herança (inh_count) na tabela Funções do usuário é somente leitura e automaticamente reflete o número de vezes que o usuário herda uma função.

Habilite a auditoria de função com a Contextual Security: Role Management V2

Defina uma propriedade do sistema para habilitar a tabela Funções de auditoria para criar registros de auditoria relacionados às funções do usuário.

Antes de Iniciar

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

Quando habilitada, a tabela Funções de auditoria [sys_audit_role] mantém as mudanças nos registros do usuário. Para obter mais informações sobre as auditorias de função, consulte Funções do usuário de auditoria. Se o plug-in Segurança contextual: Role Management V2 [com.glide.role_management.inh_count] estiver instalado, você deve definir uma propriedade de sistema para **true** para habilitar a auditoria da função.

Procedimento

1. Navegue até a tabela Propriedades do sistema [sys_properties].
2. Adicione a *glide.role_management.v2.audit_roles* propriedade do sistema e defina-a como **true**.

   Se o plug-in Segurança contextual: Role Management V2 [com.glide.role_management.inh_count] estiver instalado, configurar esta propriedade como **true** habilitará a tabela Funções de auditoria [sys_audit_role] para criar registros quando as funções do usuário mudarem.

Verifique novamente o envio do formulário

Quando o sistema determina que um campo específico (como task.number) não deve ser gravado pelo usuário atual, o sistema renderiza esse campo em um modo somente leitura, que é o motivo pelo qual o campo de número não é gravável na maioria dos incidentes.

Se você definir que o sistema verifique novamente os valores de qualquer campo de entrada quanto à capacidade de gravação, o sistema aplicará o mesmo conjunto de regras de segurança ao trecho de entrada de uma transação. Quando você envia um incidente, por exemplo, o sistema verifica duas vezes para determinar se o campo de número pode ser gravado antes de publicar qualquer mudança.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Se você informar ao sistema para não verificar novamente as transações de entrada, o sistema permitirá que você grave em um campo nominal somente para leitura se essa for a transação que o cliente envia de volta. Em muitas implantações, este realmente é um comportamento desejável se, por exemplo, você estiver usando scripts de cliente para definir campos nominalmente somente leitura em resposta às seleções do usuário em outros, campos graváveis.

Propriedade	Local	Padrão
Verifique novamente a segurança em transações de entrada durante o envio do formulário (direitos sempre são verificados na geração do formulário)	**Propriedades do sistema** > **Segurança**	Desabilitado (sem verificação dupla)

Propriedade de negação padrão

A propriedade de negação padrão (`glide.sm.default_mode`) controla o comportamento padrão do gerenciador de segurança quando as únicas regras de ACL correspondentes forem as regras de ACL da tabela curinga.

Um conjunto de regras de ACL de tabela curinga para as operações baseadas em registro mais comuns está disponível: ler, gravar, criar e excluir. Um número significativo de ACLs para fornecer acesso baseado em função a tabelas do sistema também está disponível. Por exemplo, há ACLs que concedem acesso sys_script à função business_rule_admin porque essa função está documentada como capaz de gerenciar regras de negócios.

Use a propriedade `glide.sm.default_mode` para negar ou permitir estas operações em todas as tabelas:

- **Negar acesso**: as regras de ACL da tabela curinga restringem as operações de leitura, gravação, criação e exclusão em todas as tabelas, a menos que o usuário tenha a função de administrador ou atenda aos requisitos de outra regra de ACL de tabela. Outras operações, como report_on e personalize_choices, não são afetadas por esta configuração.
- **Permitir acesso**: as regras de ACL de tabela curinga permitem as operações de leitura, gravação, criação e exclusão em todas as tabelas, a menos que haja regras de ACL de tabela específicas em vigor para restringir essas operações.

Não é possível redefinir `glide.sm.default_mode` para **Permitir acesso** depois que ele for definido para **Negar acesso**.

Nota: Por padrão, as regras de ACL da tabela curinga são as únicas regras de ACL que verificam o valor da propriedade `glide.sm.default_mode`. Se você quiser controlar outras operações com esta configuração, crie suas próprias regras de ACL para verificar o valor desta propriedade.

Para aprender mais sobre essa propriedade, consulte Negação padrão nas Configurações de proteção de segurança de instância.

Configuração de ACL avançada

Além de criar novas ACLs ou modificar as existentes, é possível configurar outros aspectos da funcionalidade da ACL.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Regras da ACL de negação

Deny-Unless

Regras da ACL de consulta

Tarefa	Descrição
Aplique as condições de script de ACL aos campos de referência	Habilite uma propriedade para permitir que as condições de script se apliquem aos campos de referência se quiser controlar o acesso aos dados que um campo de referência exibe em um formulário ou em uma lista. Pode haver um impacto no desempenho da sua instância, se você habilitar isso.
Aplicar ACLs ao AJAXGlideRecord (registro Glide do lado do cliente)	Aplique ACLs às chamadas de API do `GlideAjax` para que o sistema consulte somente os dados aos quais o usuário atualmente conectado tem direitos de acesso.
Avaliar a substituição do administrador no nível de acesso	Forçar avaliação de ACL para substituições de administrador no nível de acesso. Por padrão, os usuários com a função de administrador são aprovados automaticamente na verificação de permissões desta regra de ACL quando a opção Substituições de administrador é selecionada no formulário de regras de ACL.
Use ferramentas de depuração e resolução de ACL	Use ferramentas como o observador da ACL, a depuração no nível do campo e as mensagens de saída da regra da ACL para ajudá-lo a solucionar problemas e depurar as ACLs.

Forneça aos usuários externos acesso a uma tabela

Para permitir que usuários apenas com a função snc_external acessem a exibição de lista de uma tabela, você deve criar uma série de ACLs.

Antes de Iniciar

Função necessária: security_admin

Procedimento

1. Elevar para uma função privilegiada.
2. Criar uma regra de ACL com as seguintes configurações:
   - **Tipo**: ui_page
   - **Operação**: ler
   - **Nome**: {table_name}_list
   - **Função necessária**: snc_external
3. Na ACL de **leitura** padrão para a tabela, adicione **snc_external** na lista de função necessária.
   Crie a ACL, se ela ainda não existir.
4. Use estas configurações para criar outra ACL:
   - **Tipo**: ui_page
   - **Operação**: ler

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- **Nome**: {table_name}
- **Função necessária**: snc_external

5. Use essas configurações para criar outra ACL para conceder ao usuário acesso de gravação a um campo na tabela:
   - **Tipo**: registro
   - **Operação**: criar
   - **Nome**: {table_name} {column_name}
   - **Função necessária**: snc_external

   Repita esta etapa para cada campo ao qual deseja conceder acesso de gravação ao usuário. Use um asterisco ***** em vez do nome da coluna para conceder acesso a todos os campos de uma vez.

Aplique as condições de script de ACL aos campos de referência

Use a *glide.sys_reference_row_check* propriedade do sistema para habilitar as condições de script para os campos de referência.

O comportamento padrão tem por objetivo melhorar o desempenho da instância. Se deseja habilitar as condições de script para os campos de referência, adicione as seguintes propriedades do sistema.

Nota: Para obter mais informações sobre como criar propriedades do sistema, consulte Adicionar uma propriedade do sistema.

Propriedade do sistema

Propriedade	Descrição
glide.sys_reference_row_check	Controla se as condições de script das Regras de controle de acesso se aplicam aos campos de referência de uma tabela. • Tipo: verdadeiro | falso • Valor padrão: **falso** • Local: Adicionar uma propriedade do sistema à tabela Propriedades do sistema [sys_properties]

Nota: Se a *glide.sys_reference_row_check* propriedade do sistema não estiver presente ou tiver sido configurada como falsa, as condições de script para as Regras de controle de acesso não serão aplicadas. Isso significa que uma ACL que contém condições de script será aprovada na verificação, desde que os outros critérios da ACL sejam atendidos (como requisitos de função).

Aplicar ACLs ao AJAXGlideRecord (registro Glide do lado do cliente)

Use a propriedade do sistema para realizar a validação de regra da lista de controle de acesso (ACL) quando os registros do lado do servidor (por exemplo, tabelas) forem acessados usando as APIs GlideAjax em um script de cliente.

Se optar por aplicar as listas de controle de acesso a chamadas de API *GlideAjax*, então será possível apenas consultar dados aos quais o usuário atualmente conectado tenha direitos de acesso. Por exemplo, se o usuário efetuou login como um usuário ESS que não

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

tem direitos de ler a tabela `cmn_location`, então qualquer chamada de API *`GlideAjax`* pelo usuário falhará.

Se você executar o sistema sem que uma ACL verifique em chamadas *`GlideAjax`*, então a API pode retornar informações que o usuário atualmente com login efetuado não poderia então acessar através da IU.

Nota: Configure esta propriedade em **Propriedades do sistema** > **Segurança**.

Propriedade	Padrão
Aplique ACLs de segurança padrão a chamadas *`AJAXGlideRecord`*	Verificação de ACL imposta

Aviso: O `sys_class_name`, `sys_id` e `sys_domain` são ignorados para as verificações de ACL.

Para aprender mais sobre essa propriedade, consulte Habilitar a verificação de ACL de AJAXGlideRecord nas Configurações de proteção de segurança de instância.

Avaliar a substituição do administrador no nível de acesso

Se quiser forçar a avaliação da ACL para substituições de administrador no nível de acesso, é possível adicionar uma propriedade do sistema.

Antes de Iniciar

Função necessária: security_admin

Por Que e Quando Desempenhar Esta Tarefa

As ACLs são avaliadas cumulativamente. Se houver um número de ACLs em qualquer campo e a opção **Substituições de Administrador** for **falsa** (não selecionada) em um deles, as substituições de administrador efetivas para todas as ACLs serão consideradas **falsas**. Isso faz com que os administradores não consigam passar mesmo na ACL em que a substituição deva estar em vigor.

Procedimento

Adicione a seguinte propriedade à tabela de propriedades do sistema:

Propriedade	Descrição
`glide.security.admin.override.accessterm`	Avalia a condição de substituição do administrador no nível do termo de acesso. • Tipo: verdadeiro | falso • Valor padrão: **verdadeiro** para novas instâncias, **falso** para upgrades • Local: adicione à tabela *`[sys_properties]`* de Propriedades do sistema **Nota:** Se a propriedade não estiver definida na instância, o valor será avaliado como falso.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

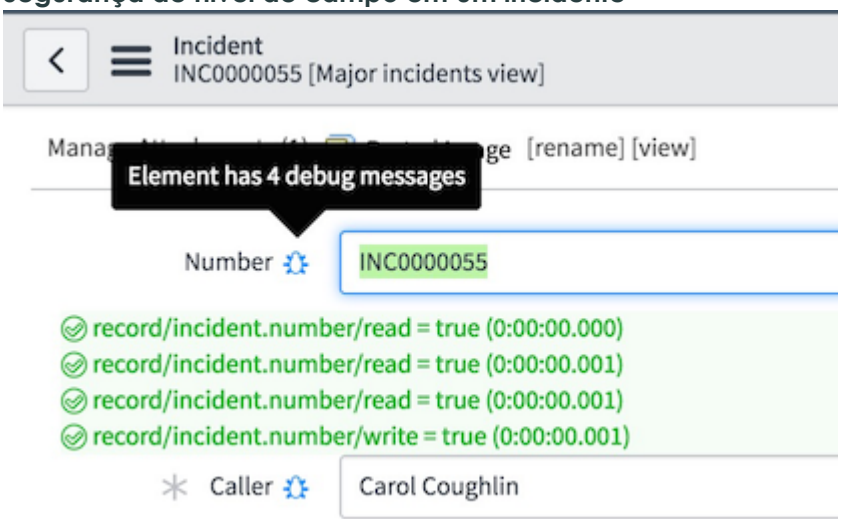
Ferramentas de depuração de ACL

As mensagens de saída de regra de ACL de acesso e depuração de nível de campo ficam disponíveis para ajudar na solução e depuração de ACLs. O observador de configuração de ACL permite que você saiba quais ACLs relacionadas existem quando você modifica um.

Depuração no nível de campo

Quando a depuração é habilitada, um pequeno ícone de erro (#) aparece ao lado de cada campo com uma regra de ACL. Clicar no ícone lista as regras de ACL que se aplicam ao campo e aos resultados da avaliação. Habilite a depuração navegando até **Segurança do sistema** > **Depuração** > **Regras de segurança de depuração**.

Segurança de nível de campo em um incidente



Depois de habilitar a depuração de ACL, é possível representar outro usuário para ver quais regras de ACL o usuário passa e falha. Ao representar um usuário, é possível ver apenas o que esse usuário tem permissão para ver. Por exemplo, você não pode exibir um registro que uma ACL impede que o usuário veja. Para facilitar a depuração, o acesso somente leitura a determinadas tabelas relacionadas à ACL é habilitado por padrão, mesmo ao representar um usuário que não tem acesso de leitura às tabelas. Para mudar esta funcionalidade, defina a seguinte propriedade como **falsa**.

Para habilitar a depuração de regra de ACL, navegue até **Segurança do sistema** > **Regras de segurança de depuração**.

Propriedade do sistema	Descrição	Configurações padrão
glide.security.access_acl_impersonate	Permite acesso de leitura às seguintes tabelas ao representar um	verdadeiro

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Propriedade do sistema	Descrição	Configurações padrão
	usuário: sys_security_acl, sys_security_operation, sys_security_type e sys_user_role. Como resultado, o usuário que representa pode ler dados que o usuário representado não pode ler.	**Nota:** Quando a propriedade é definida como falsa, o usuário representado pode ser impedido de ler os dados relacionados à ACL. Nesse caso, uma segunda sessão conectada como administrador ou security_admin pode ser necessária para depurar ACLs.

Mensagens de saída da regra de ACL

A depuração de ACL exibe mensagens de saída de regra de ACL na parte inferior de cada lista e formulário. A mensagem de saída exibe o seguinte:

Elemento de mensagem	Descrição
HORa	O tempo total usado para processar esta regra de ACL.
CAMINHO	As informações que identificam exclusivamente cada regra de ACL no formato: `<tipo de regra de ACL>/<nome de regra de ACL>/<Operação>`.
CONTEXTO	O objeto sendo avaliado pela regra da ACL.
RC	O código de retorno da regra da ACL. Um valor verdadeiro é aprovado na regra da ACL. Um valor falso causa falha na regra da ACL.
REGRA	Um breve resumo de processadores e scripts, seguidos por resultados de ACL para cada avaliação de ACL em nível de tabela e de campo. A maioria das avaliações de ACL mostra um resultado geral de aprovação ou reprovação seguido por um detalhamento dos resultados para cada tipo de critério de ACL: • iAccessHandler: uma verificação do sistema interno que usa código fonte oculto na plataforma. Esta é uma verificação de segurança do sistema que você não pode modificar. IAccessHandler pode conceder ou negar acesso a um recurso sem avaliar ACLs. Se IAccessHandler for ignorado, então as ACLs serão avaliadas. Não é possível modificar as verificações IAccessHandler de forma alguma. Por exemplo, uma implementação IAccessHandler é usada para verificações de acesso em recursos da aplicação e isso não pode ser alterado. Isso está disponível a partir da versão Istanbul. • Funções: verificação de que o usuário tem a função correta.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Elemento de mensagem	Descrição
	• Condição: verificação de que o usuário foi aprovado na condição especificada na regra de ACL (se houver). • Script: Verificação de que o usuário passou no script especificado na regra de ACL (se houver).

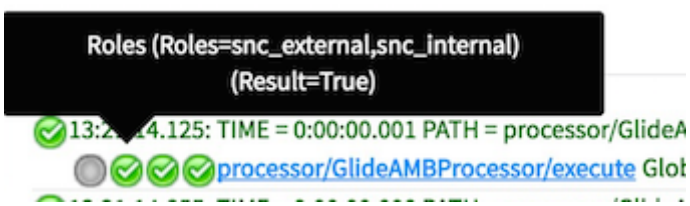
Os ícones que aparecem mostram como a ACL foi avaliada:

Ícone	Descrição
Uma marca de seleção verde (#)	Indica que a tabela ou o campo indicado passou nos critérios.
Um ícone x vermelho ( )	Indica que a tabela ou o campo não foi aprovado.
Um ícone de círculo cinza vazio (#)	Indica que a avaliação do ACL não precisou ser realizada.
Uma marca de seleção azul, x ou um círculo vazio	Indica que a ACL foi obtida de um resultado armazenado em cache de uma verificação de ACL anterior. Os ícones têm o mesmo significado que os anteriores.

É possível executar estas ações na saída de depuração de ACL:

- Marque ou desmarque estas caixas de seleção na parte superior da saída de depuração:
  - **Regras de segurança**: mostre ou oculte os resultados das verificações de ACL.
  - **Outros**: mostre ou oculte outros avisos ou mensagens.
- Clique no nome da ACL ao lado de qualquer uma das mensagens de saída para abrir esse registro de ACL.

- Passe o cursor sobre qualquer um dos ícones das quatro verificações de ACL para ver mais informações.



© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Referência de solução de problemas de ACL

Uma lista de erros de regra de ACL comuns e suas soluções.

Habilite a depuração para ajudar a solucionar um problema.

Solução de problemas

Erro ou sintoma	Solução
Não é possível acessar registros de uma tabela personalizada.	Crie uma regra de ACL de tabela para a tabela personalizada concedendo aos usuários acesso à tabela. Sem uma regra de ACL de tabela explícita, os usuários devem passar as permissões na regra de ACL de tabela curinga (*), que por padrão restringe o acesso somente a administradores. Habilite a depuração e determine quais regras de ACL são avaliadas para a tabela personalizada.
Você cria uma regra de ACL personalizada que não funciona corretamente.	Os problemas mais prováveis são que outra regra tenha precedência sobre sua regra personalizada na ordem de processamento ou que o usuário não atenda a todos os requisitos de permissão para o tipo de objeto. Habilite a depuração e verifique se a regra de ACL está sendo avaliada.
Sua regra de ACL de campo não funciona corretamente.	Provavelmente há uma regra de ACL de tabela que o usuário não atendeu. Habilite a depuração e determine quais regras de ACL são avaliadas para o campo. Verifique se não há uma regra de ACL de tabela conflitante ou regra de ACL de campo duplicada.
Sua regra de ACL de tabela não funciona corretamente.	Existe uma regra de ACL superior no pedido de processamento ou uma regra de ACL de tabela duplicada interferindo na regra de ACL da tabela. Habilite a depuração e determine quais regras de ACL são avaliadas para a tabela.
É possível ver um campo em uma lista, mas não no formulário.	É possível que as condições da regra da ACL ou o script estejam sendo acionados na lista, mas não no formulário. Habilite a depuração e determine quando as regras de ACL são avaliadas para verdadeiro. Atualize as condições ou o script para que tenham o mesmo comportamento na lista e no formulário.
Você recebe uma mensagem de erro ao tentar executar um processador ou inclusão de script de cliente chamável.	Há uma regra de ACL para o processador ou inclusão de script de cliente chamável que o usuário não atendeu. Se o usuário tiver acesso ao objeto, habilite a depuração e determine quais regras de ACL são avaliadas para o processador ou a inclusão de script. Atualize a regra de ACL ou as funções do usuário conforme necessário para acessar o objeto.

Observador de configuração da ACL

O observador de configuração de ACL permite que você saiba quais ACLs relacionadas existem em uma tabela quando você insere, atualiza ou exclui uma ACL na mesma tabela.

O observador de configuração de ACL é uma janela de interceptador exibida sempre que você faz mudanças importantes na tabela de controle de acesso [sys_security_acl]. Ele exibe uma janela de resumo de regras de segurança na qual você pode exibir as ACLs relacionadas ao que está modificando. Não é possível modificar nenhuma ACL na janela de regras de segurança. Para fazer modificações, feche a janela do observador e acesse essas ACLs.

O observador de configuração da ACL não aparece nas seguintes situações:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Se você salvar ou atualizar um registro de ACL sem realmente fazer qualquer mudança.
- Se você fizer atualizações secundárias (não uma inserção ou exclusão), como atualizar scripts, condições e opção de substituições de administrador.
- Se o registro de ACL não estiver ativo.

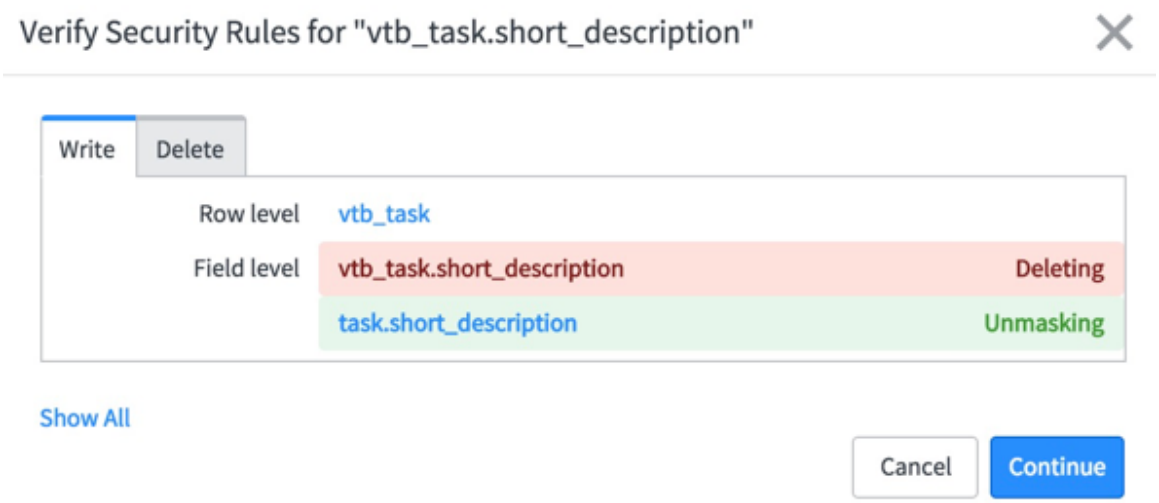
Janela de regras de segurança de ACL

O observador de configuração mostra o plano de execução de ACL. O plano de execução é exibido na janela pop-up de regras de segurança. É possível exibir este tipo de informação:

Elementos da janela de configuração da ACL

Item	Descrição
realce vermelho	Uma ACL que foi excluída ou desativada.
realce azul	Uma ACL que é modificada.
realce verde	Uma ACL que é adicionada ou se torna ativa.
Mascarado	Uma ACL que estava em vigor até você fazer uma mudança.
Desmascarado	Uma ACL que entrou vigor quando você fez uma mudança.

Exemplo de observador de configuração



Mostrar plano de execução de ACL

Os administradores podem exibir como as ACLs se relacionam entre si exibindo um plano de execução para qualquer ACL na instância.

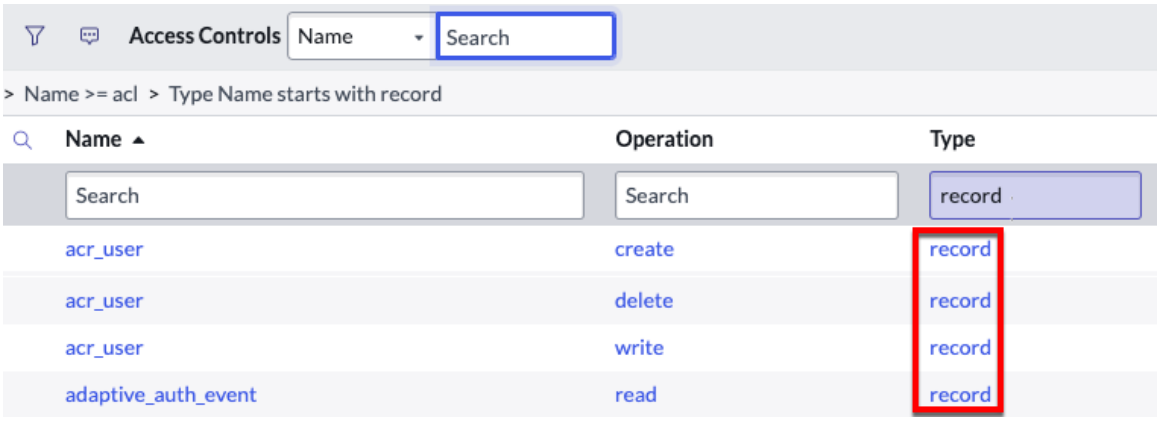
Antes de Iniciar

Função necessária: security_admin

Procedimento

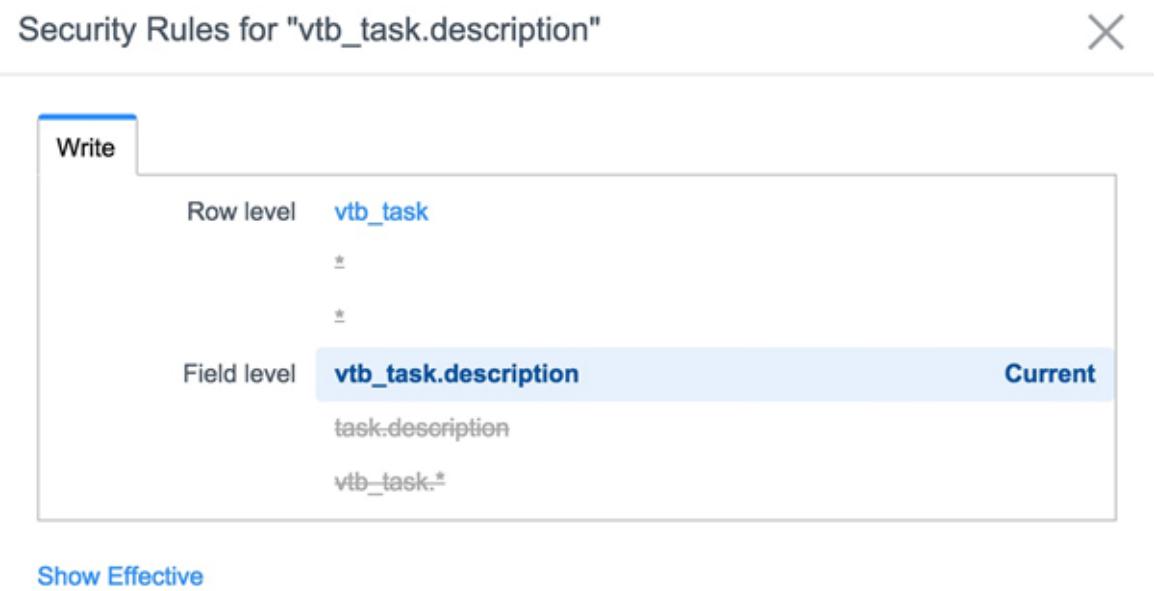
1. Elevação para uma função privilegiada.
2. Navegue até **Segurança do sistema** > **Controle de acesso (ACL)**.
3. Abra uma ACL com o tipo *record*.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Clique em **Mostrar plano de execução de ACL** na seção Links relacionados.

   A janela de regras de segurança aparece para a ACL. O exemplo exibe o plano de execução para "vtb_task".



Janela do plano de execução de ACL

Item de IU	Descrição
Título	O nome da ACL.
Nome da guia	Se a ACL for criar, ler, gravar ou excluir.
Nível de linha	As ACLs no nível de linha que são executadas nesta tabela.
Nível de campo	ACLs no nível de campo que são executadas somente neste campo (ou coluna na tabela).

5. Clique em **Mostrar tudo** para mostrar todas as ACLs relacionadas, incluindo as ACLs que são substituídas e as ACLs genéricas que se aplicam a todos os registros.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

As ACLs substituídas possuem uma linha no nome e as ACLs genéricas têm o asterisco de caractere curinga (*) no nome.

6. Clique em **Mostrar efetivo** para mostrar apenas as ACLs imediatas relacionadas à que você está exibindo e ocultar as ACLs nas tabelas das quais a tabela da ACL é estendida e as ACLs genéricas com caractere curinga (*).

Use o observador de configuração de ACL

Use o observador de configuração de ACL depois de você elevar para a função security_admin.

Antes de Iniciar

Função necessária: security_admin
Elevação para uma função privilegiada

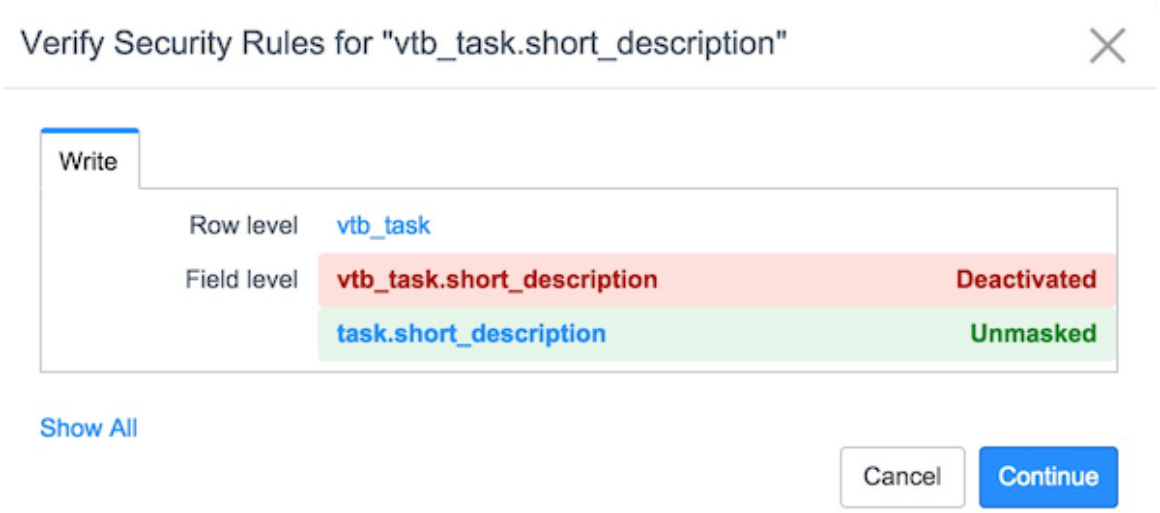
Procedimento

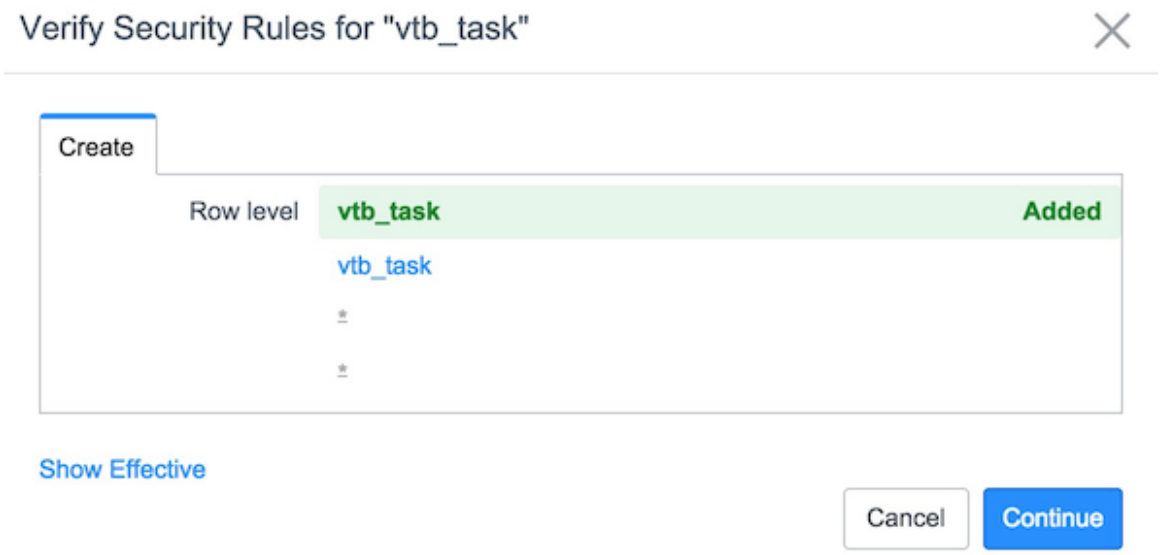
1. Abra uma ACL que é uma ACL de tipo de registro.
2. Execute uma ação na ACL, como modificá-la ou selecionando uma opção no menu contexto como **Inserção**.
3. Se você modificou algum valor no formulário Controle de acesso, clique com o botão direito no cabeçalho e selecione **Salvar** ou clique em **Atualizar** ou **Excluir**.

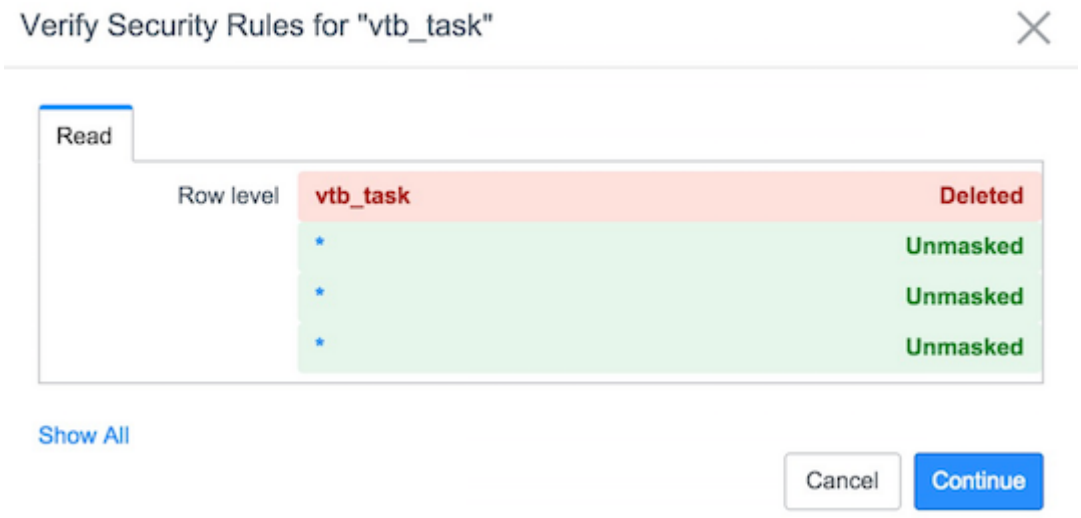
   A janela Regras de segurança aparece. O sistema ainda não realizou a ação do banco de dados na ACL, de modo que as mudanças ainda não foram salvas.

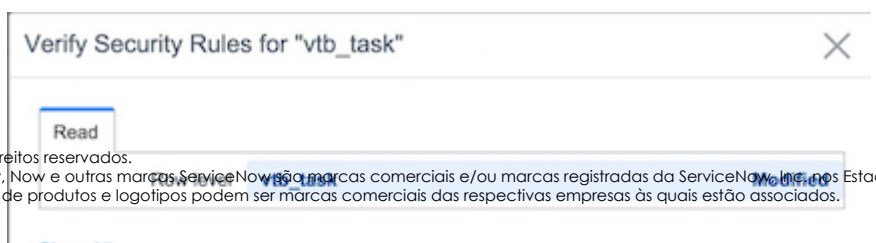
   Esses são exemplos de regras de segurança na tabela Tarefa privada [vtb_task] da aplicação Visual Task Board. Consulte Observador de configuração da ACL para obter uma descrição dos itens nesta janela.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.









© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Assim como com o plano de execução, é possível clicar em **Mostrar tudo** para mostrar todas as ACLs relacionadas, incluindo aquelas que são substituídas e ACLs genéricas que se aplicam a todos os registros ou clique em **Mostrar efetivo** para mostrar apenas as ACLs imediatas relacionadas ao que você está exibindo.
5. Passe o mouse sobre qualquer uma das ACLs para ver uma descrição.

Atributos de segurança

Os atributos de segurança oferecem uma alternativa flexível para acessar listas de controle.

Primeiros passos

Explore Atributos de segurança Conheça os fundamentos dos Atributos de segurança	Crie Atributos de segurança Crie novos Atributos de segurança
Atributos de segurança OOB (prontos para uso) Explicação dos Atributos de segurança OOB	Registro em log de Atributos de segurança Analise Registro em log de Atributos de segurança

Fundamentos dos atributos de segurança

Um Atributo de segurança é uma informação altamente configurável sobre um Assunto ou seu Ambiente. Quando usada em controles de acesso, permite uma configuração de segurança de granularidade fina e sem complexidade.

Visão geral

Os Atributos de segurança são um método alternativo de controle de acesso por meio de definições de função para a configuração de ACLs (Access Control Lists, listas de controle de acesso) atualmente em prática. Os Atributos de segurança oferecem várias vantagens para as configurações baseadas em ACLs:

Melhor segurança

A ofuscação de avaliação de permissões aprimorada garante que sua organização permaneça segura.

Legível

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Os atributos de segurança são projetados para simplificar a criação e a facilidade de uso de permissões de segurança.

Segurança flexível

Crie definições de persona a partir da configuração pronta para uso em combinação com as personas definidas pelo cliente.

Registro em log e auditoria

Os Atributos de segurança oferecem auditoria e registro em log detalhados para fornecer mais informações sobre as medidas de segurança e a teoria.

Criar atributos de segurança

Crie novos Atributos de segurança com um guia detalhado.

Antes de Iniciar

Função necessária: security_admin

Procedimento

1. Navegue até **Segurança do sistema** > **Atributos de segurança**.
2. Na lista Atributos de segurança, selecione **Novo**.
3. No formulário de campos de Atributos de segurança, preencha os campos.

Campos de Atributos de segurança

Campo	Descrição
Rótulo	Rótulo do Atributo de segurança.
Nome	Nome do Atributo de segurança.
Tipo	Tipo do Atributo de segurança. ◦ composto **Nota:** Para obter mais informações sobre os Atributos de segurança compostos, consulte Atributos de segurança compostos ◦ inteiro ◦ lista ◦ Cadeia de caracteres ◦ boolean(verdadeiro | falso)
É dinâmico	Se o valor do Atributo de segurança precisa ser reavaliado em cada
Descrição	Descrição do Atributo de segurança gerada pelo usuário
Aplicação	Campo estático, Escopo da aplicação.
Tabela de pesquisa	Faça referência a uma tabela externa para avaliação.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Pesquisar coluna da tabela	Faça referência a uma coluna da tabela para avaliação.
Script	Derive um valor de um script.

Atributos de segurança OOB (prontos para uso)

Funções de atributos de segurança generalizadas e usadas com frequência e prontas para uso.

Visão geral

Os Atributos de segurança OOB (Out-of-Box, prontos para uso) são uma maneira fácil de começar a usar e aprender os recursos dos Atributos de segurança com uma série de funções de Atributo de segurança pré-configuradas. As funções dos Atributos de segurança OOB são funções de controle de acesso usadas com frequência.

Para criar seu próprio Atributo de segurança ou expandir recursos dos Atributos de segurança OOB, consulte Atributos de segurança compostos

Atributos de segurança OOB

Atributo	Descrição
Grupo	O usuário é membro de um grupo especificado
GroupExplicit	O usuário é um membro explícito de um grupo específico
HasAdminRole	O usuário tem a persona de administrador
Representando	O usuário é representado
InteractiveSession	Sessão atual interativa
LoggedIn	O usuário está conectado e autenticado
NetworkCriteria	Critérios adicionais de rede
Função	O usuário tem uma função específica
RoleExplicit	O usuário tem uma função específica definida de forma explícita

Atributos de segurança da sessão do cliente

Os seguintes atributos de segurança são adicionados à sessão do cliente (plug-in: `com.glide.client_session_security_attributes`):

- **IsIframeEmbeddedSession**: o atributo é usado no iframe integrado em portais de terceiros. Por exemplo, App de mensagens de interação, Cliente web do Virtual Agent, Sessão integrada, entre outros.
- **IsIntegrationAsAServiceSession**: o atributo é usado em apps de mensagens como o Virtual Agent no Teams, o Virtual Agent no Slack e o Virtual Agent no WhatsApp.
- **IsIntegrationAsAUserSession**: o atributo é usado no usuário da conta de integração ou no usuário do serviço Web.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- **Is Servicenow Web Session**: o atributo é usado na sessão interativa para celular.
- **Is Mobile App Session**: o atributo é usado se a propriedade **mobile_client** for verdadeira no registro **oauth_entity**.

Sobre comportamento não explícito e explícito

Os Atributos de segurança atendem às necessidades de permissão diferenciadas com uma avaliação explícita ou não explícita (herdada) de permissões de funções.

Atributos de segurança compostos

Os Atributos de segurança compostos permitem criar perfis de Atributo de segurança consistentes e reutilizáveis que se adaptam às suas necessidades de negócios

Visão geral

Os Atributos de segurança compostos são definidos a partir de um ou mais Atributos de segurança pré-existentes para criar uma única combinação de referência de Atributos de segurança para avaliação de permissões.

Criar atributos de segurança compostos

Crie um Atributo de segurança composto para facilitar a reutilização.

Antes de Iniciar
Função necessária: security_admin

Procedimento

1. Navegue até **Segurança do sistema** > **Atributos de segurança**.
2. Na lista Atributos de segurança, selecione **Novo**.
3. Selecione `Composto` no campo **Tipo**.
4. No formulário de campos de Atributos de segurança, preencha os campos.

Campos de Atributos de segurança

Campo	Descrição
Rótulo	Rótulo do Atributo de segurança.
Nome	Nome do Atributo de segurança.
Descrição	Descrição do Atributo de segurança gerada pelo usuário
Condição	As condições específicas do Atributo de Segurança usadas para definir a avaliação dos Atributos de Segurança.
Novos critérios	Adicione um conjunto extra de condições **Or** para avaliação.

Escopo dos Atributos de segurança

Os Atributos de segurança oferecem suporte a recursos de escopo.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Escopo dos Atributos de segurança

O comportamento do escopo dos atributos de segurança é consistente com os comportamentos de escopo da plataforma. Os Atributos de segurança criados em um escopo só estão disponíveis em controles de acesso no mesmo escopo.

Atributos de segurança locais e existentes

Os Atributos de segurança locais e existentes permitem que os clientes reutilizem conjuntos de condições de Atributos de segurança.

Atributos locais e existentes

O Construtor de condições dos atributo de segurança de ACL permite que os clientes especifiquem se um atributo de segurança é existente ou local.

Nota: Por padrão, as condições de Atributos de segurança são definidas como locais.

Um Atributo de segurança definido como local somente é salvo na ACL única em que foi criado.

A opção existente permite que os usuários façam referência a condições de Atributos de segurança existentes no construtor de condições.

Funções e restrições da consulta de campos

Os atributos **Funções de consulta de campo** e **Restrições de consulta de campo** proporcionam um melhor controle de quais informações estão disponíveis aos usuários nas tabelas.

Visão geral

Os atributos **Funções de consulta de campo** e **Restrições de consulta de campo** proporcionam um controle mais refinado sobre as ações que os usuários podem realizar nas tabelas.

Funções de consulta de campo

Impede a consulta de campos confidenciais com base na função do usuário.

Restrições de consulta de campo

Restringirá o acesso ao registro se houver a negação de acesso ao campo aplicável.

Como configurar uma função de consulta de campo

Saiba como ativar e configurar um atributo de Função de consulta de campo.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Navegue até **Todos** > **Definição do sistema** > **Tabelas**.
2. Selecione uma **Tabela**.
3. Selecione um **Rótulo da coluna** para exibir a entrada de **Dicionário**.
4. Selecione a guia **Atributos**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. **Dica:** Se você não tiver o campo **Funções de consulta de campo**, selecione **Novo** para criar um

   Selecione o atributo **Funções de consulta de campo**.
6. Em **Valor**, insira as funções necessárias para exibir essa coluna da tabela
7. Selecione **Atualizar**

Resultados
Somente as funções definidas no atributo **Funções de consulta do campo** podem consultar a coluna da tabela. Se um usuário sem as funções definidas a consultar, ele terá o acesso negado à operação.

Como configurar restrições de consultas de campo

Saiba como configurar uma restrição de consulta de campo

Antes de Iniciar
Função necessária: administrador

Procedimento
1. Navegue até **Todos** > **Definição do sistema** > **Tabelas**.
2. Selecione uma **Tabela**.
3. Selecione um **Rótulo da coluna** para exibir a entrada de **Dicionário**.
4. Selecione a guia **Atributos**.
5. **Dica:** Se você não tiver o campo **Restringir o acesso a registros de consulta de campo**, selecione **Novo** para criar um

   Selecione o atributo **Restringir o acesso a registros de consulta de campo**.
6. Insira `verdadeiro` no campo **Valor** para restringir o acesso aos registros somente aos usuários que podem ver o campo; caso contrário, insira `falso`.
7. Selecione **Atualizar**

Resultados
A coluna da tabela restringirá os resultados de todas as consultas. Os usuários restritos saberão quantos resultados uma consulta exibiu, mas nenhuma informação adicional.

Filtragem de dados

Use a filtragem de dados para controlar o acesso a tabelas e registros com base nos atributos do assunto ao executar consultas de leitura.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Explore a Filtragem de dados Saiba mais sobre a Filtragem de dados.	Crie regras de Filtragem de dados Crie suas próprias regras de Filtragem de dados conforme suas necessidades.
Depure dados Saiba como depurar os resultados da Filtragem de dados.	

Explorando a filtragem de dados

Use a filtragem de dados para controlar o acesso a tabelas e registros com base nos atributos do assunto ao executar consultas de leitura.

A filtragem de dados é uma forma separada de controle de acesso projetada para funcionar com as Regras de controle de acesso (ACLs) existentes na instância. A filtragem de dados nega o acesso a tabelas e registros que não correspondem aos atributos de assunto definidos por um administrador. A filtragem de dados foi projetada para facilitar a auditoria, a emissão de relatórios e a solução de problemas.

Esse é um recurso opcional que os administradores podem ativar em sua instância.

Recursos de filtragem de dados

Filtros de dados Use filtros de dados para conceder acesso com base nas informações de um registro. Os filtros de dados usam dados em um campo de tabelas para determinar se um registro está disponível para os usuários.
Construtor de condições com base em atributo de assunto Use atributos de assunto para avaliar a função do usuário, o grupo, os critérios de assunto ou o endereço de rede IP.
A filtragem de dados usa um modelo com base em negação

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A filtragem de dados usa um modelo com base em negação para controlar o acesso aos registros. Com a filtragem de dados, a instância nega o acesso aos registros a menos que um registro atenda aos critérios definidos pela filtragem de dados.

Imposição de filtragem de dados

As regras de filtragem de dados são executadas após a consulta ao banco de dados para operações READ e são avaliadas antes das ACLs. Um registro negado por qualquer regra de filtragem de dados não continuará e será avaliado por regras de ACL.

- A imposição da regra de filtragem de dados é consistente com a das ACLs de READ.
- A filtragem de dados, como ACLs, funciona em conjunto com os comportamentos *Report_view access control list* existentes. Consulte Controle de acesso Report_view para obter mais detalhes sobre como configurar esses controles de relatório.

Depuração de sessão

A filtragem de dados é compatível com a depuração de sessão. Use a depuração de sessão para saber quais registros de filtragem de dados se aplicam a determinada consulta. Os administradores podem usar essas informações para solucionar problemas de acesso do usuário aos registros.

Componentes de filtragem de dados

A filtragem de dados funciona usando os seguintes tipos de registro:

Registros de filtragem de dados

Crie um registro de filtragem de dados [sys_df_data_filtration] para conceder acesso à tabela na instância. O registro de filtragem de dados contém as condições **Filtro de dados** e **Atributo de assunto** descritas acima para limitar o escopo da regra e os usuários afetados.

Registros de critérios de assunto

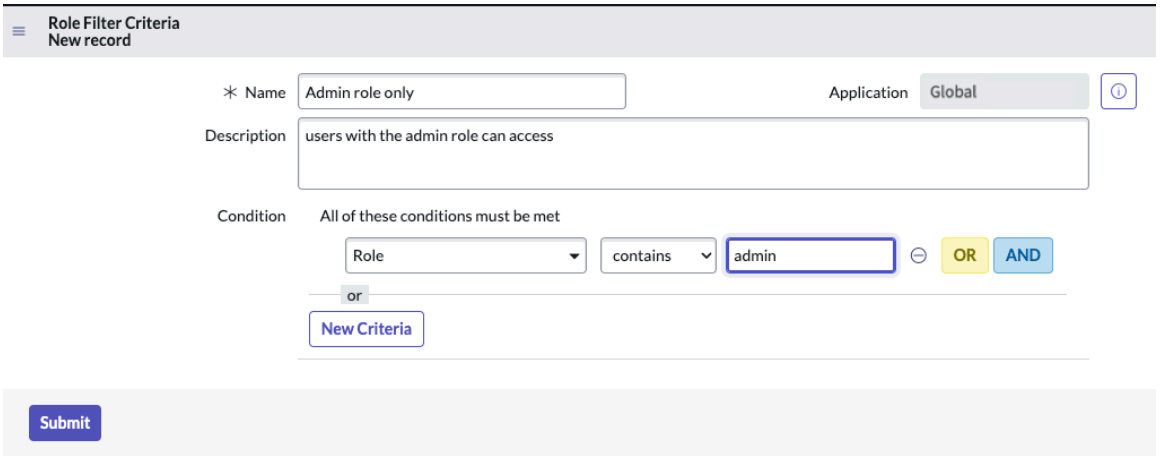
Os registros de critérios de assunto [sys_df_subject_criteria] representam atributos de usuário específicos que você pode usar para determinar se deve conceder acesso com uma regra de filtragem de dados. Esses atributos podem ser grupos, funções ou endereço IP de um usuário. Para criar um critério de assunto, você deve criar o registro de critérios de assunto, bem como registros de condições de critérios e de entrada. Para obter detalhes sobre esse processo, consulte Criando critérios de assunto.

Depois de criar registros de critérios de assunto, você pode aplicá-los a uma regra. Isso é feito na guia **Condição de assunto** da regra de filtragem de dados.

Exemplos de registros de entrada de critérios

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

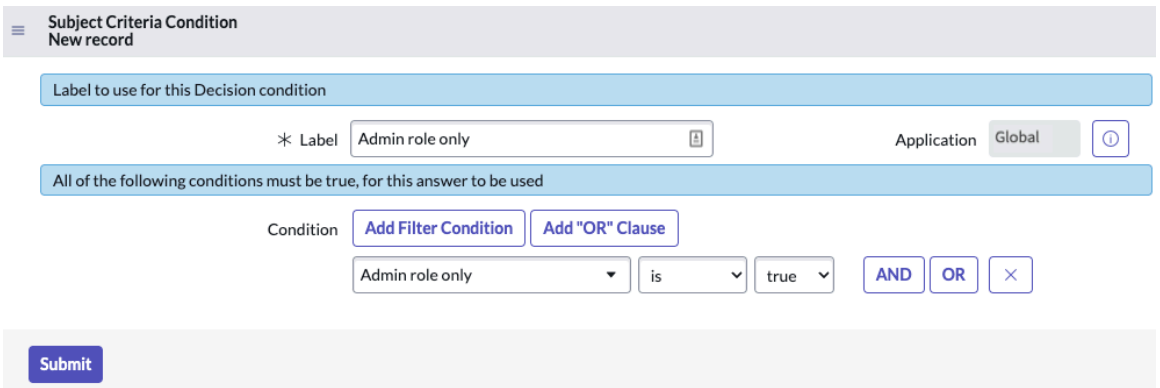
Exemplo de entrada de critérios para todas as funções que contêm administrador



Entradas de critérios [sys_df_subject_filter_criteria_m2m] são registros que contêm critérios para comparar ao usuário. Pode ser uma lista de grupos de usuários ou funções, um intervalo de endereços IP ou uma sub-rede de endereços IP. Esses registros são usados com registros de condição de critérios de assunto para avaliar em relação a grupos, funções ou endereço IP de um usuário para determinar o acesso a uma tabela ou seus registros.

Registros de condição de critérios de assunto

Exemplo de condição de critérios usando a entrada de critérios Somente administradores



Use registros de condição de critérios de assunto [sys_df_subject_criteria_condition] para definir como comparar os atributos do usuário às funções, grupos ou endereços IP definidos em suas entradas de critérios. Você pode usar várias entradas de critérios em uma única condição de critérios de assunto para restringir ainda mais o acesso aos registros.

Ativando filtragem de dados

Saiba como ativar a filtragem de dados em sua instância.

Antes de Iniciar

Função necessária: security_admin

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegue até **Todos** > **Definição do sistema** > **Plug-ins**.
2. Use o campo de pesquisa para encontrar o plug-in Data Filtration (com.glide.data_filtration).
3. Clique em **Instalar** e, na caixa de diálogo Ativar plug-in, clique em **Ativar**.

Criando regras de filtragem de dados

Saiba como criar regras de filtragem de dados para conceder acesso a registros em tabelas aos usuários.

Antes de Iniciar

Função necessária: security_admin

Nota: Para criar ou modificar regras de filtragem de dados, você deve elevar à função privilegiada. Para obter detalhes sobre esse processo, consulte Elevar para uma função privilegiada.

Procedimento

1. Navegue até **Tudo** > **Filtragem de dados** > **Registros de filtragem de dados**.
2. Clique em **Novo** na lista **Filtragem de dados**.
   Um novo formulário de filtragem de dados é exibido.
3. No formulário, preencha os campos conforme necessário.

Formulário Filtragem de dados

Campo	Descrição
Tabela	Tabela em que esta regra de filtragem de dados se aplica.
Ativa	Define a regra de filtragem de dados como ativa. **Nota:** Mantenha as regras de filtragem de dados inativas até que esteja pronto para testar a fim de evitar o bloqueio acidental de usuários fora dos registros.
Descrição	Descrição da regra de filtragem de dados.
Em cascata	Selecione para definir a regra de filtragem de dados a ser aplicada em tabelas estendidas. Por exemplo, você seleciona a tabela Tarefa[task] e ativa a cascata. Nesse caso, a regra de filtragem de dados também se aplica a todas as tabelas estendidas da tarefa, como Incidente[incident] e Solicitação de mudança[change_request]. Para obter detalhes sobre a extensão da tabela, consulte Extensão de tabela e classes **Nota:** Este campo está habilitado por padrão.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Selecione **Salvar** no menu do formulário.
   Depois de salvar a regra de filtragem de dados, ela se aplica automaticamente a todos os registros na tabela selecionada. Você pode restringir o escopo dessa regra a registros específicos na tabela usando condições nas guias **Filtro de dados** e **Condição de assunto**.

Como adicionar um filtro de dados para a regra de filtragem de dados

Opcionalmente, você pode usar um filtro de dados para restringir o escopo da regra de filtragem de dados para aplicar somente aos registros específicos em uma tabela.

Antes de Iniciar

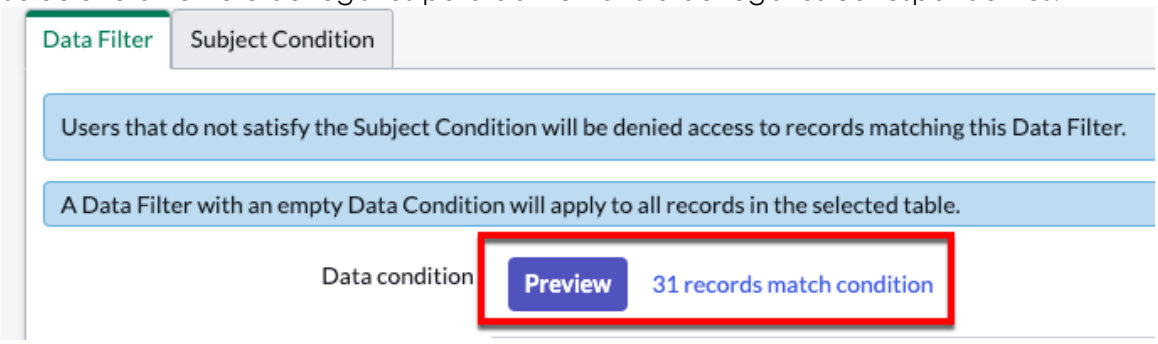
Função necessária: administrador

Procedimento

1. No registro de filtragem de dados, abra a guia **Filtro de dados**.
2. Use o Construtor de condições para filtrar os registros da tabela em seus valores de campos.
   O filtro de dados usa o mesmo Construtor de condições usado em outras partes da plataforma. Para obter detalhes sobre como usar essa interface, consulte Construtor de condições.

   Importante: A guia **Filtro de dados** aparece vazia até que você selecione uma tabela no campo **Tabela**.

3. Use o botão **Visualizar** para ver uma contagem de quantos registros correspondem ao filtro de dados.
4. Selecione o número de registros para abrir uma lista de registros correspondentes.

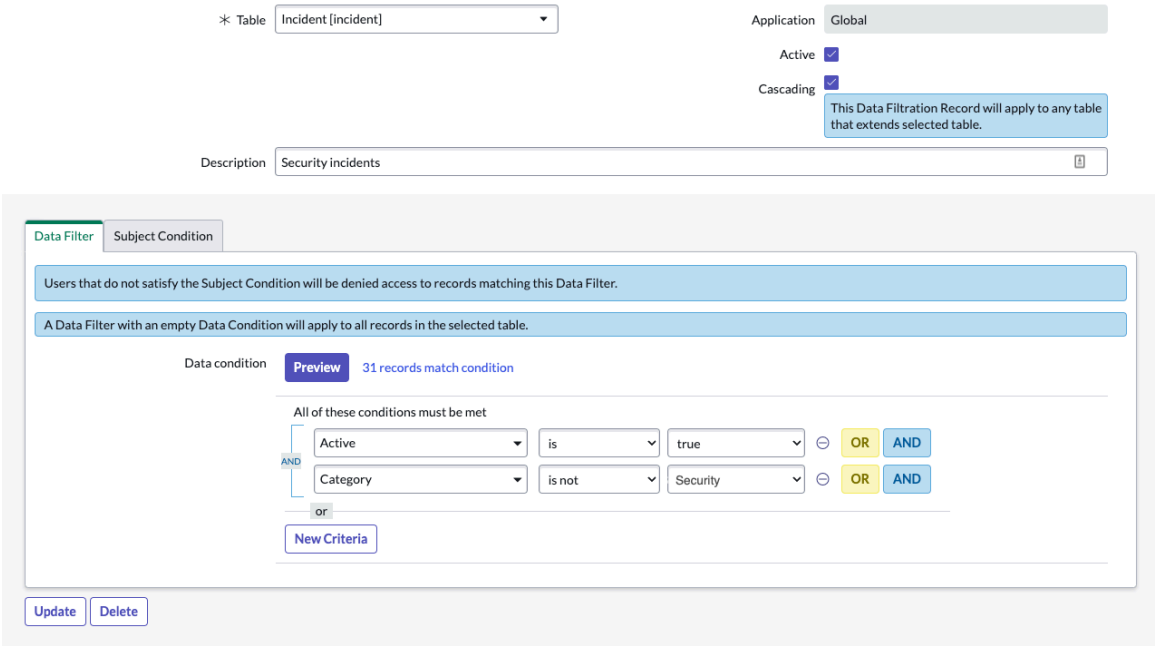


5. Selecione **Salvar**.

Example:

Este exemplo mostra uma regra de filtragem de dados para a tabela Incidente[incident]. O filtro de dados é definido para selecionar todos os registros ativos que não estão na categoria **Segurança**. Com essa regra ativa, os usuários podem ver esses registros. Consulte a seção abaixo para continuar usando critérios fora do conteúdo do registro.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Importante:

A operação **não** em suas condições pode retornar resultados inesperados dependendo do tipo de banco de dados que a instância usa. Por exemplo, considere a seguinte condição:

Para essa condição, o resultado esperado seria que o conjunto de resultados fosse composto por todos os registros em que a empresa não é a `ServiceNow` e todos os registros que não têm um valor no campo da **empresa**. Instâncias que usam bancos de dados diferentes de MySQL e Maria não retornam registros de valores com um campo de **empresa** vazio. Ao usar consultas **não** para essas instâncias, inclua condições para garantir que valores vazios sejam retornados.

Como adicionar atributos de assunto à regra de filtragem de dados

Opcionalmente, use atributos de assunto para restringir o escopo da regra de filtragem de dados com base em atributos como endereço de rede IP, grupos de usuários e funções ou critérios de assunto.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. No registro de filtragem de dados, abra a guia **Critérios de assunto** .
2. Use o Construtor de condições para filtrar os registros da tabela com base em um ou mais dos critérios a seguir.

Opções de critérios de assunto

Opção	Descrição
Critérios de rede	Permite acesso a registros com base no intervalo de IP da rede ou na sub-rede de IP.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
Critérios de assunto	Permite acesso a registros com base em critérios de assunto. Selecione um registro de critérios de assunto para aplicar suas condições à sua regra de filtragem de dados. Para obter detalhes sobre como criar registros de critérios de assunto, consulte Criando critérios de assunto.
Grupo de assuntos	Como permitir o acesso se o usuário for membro de um grupo específico. Selecione um grupo na tabela **Grupos**[sys_user_group].
Função do assunto	Como permitir o acesso se o usuário for membro de um grupo específico. Selecione um grupo na tabela **Funções**[sys_user_role].

Importante: As condições dos critérios de assunto são compatíveis somente com o operador **is**.

3. Depois de adicionar os critérios de assunto, clique em **Salvar**.

Criando critérios de assunto

Crie registros de critérios de assunto para uso em regras de filtragem de dados.

Antes de Iniciar

Função necessária: security_admin

Importante: Para criar ou modificar regras de filtragem de dados, você deve elevar para uma função privilegiada. Para obter detalhes sobre esse processo, consulte Elevar para uma função privilegiada.

Procedimento

1. Navegue até **Todos** > **Filtragem de dados** > **Critérios de assunto**.
2. Na lista **Critérios de assunto**, clique no botão **Novo**.
   Um novo formulário de critérios de assunto é exibido.
3. No formulário, preencha os campos conforme necessário.

Campos de Critérios de assunto

Campo	Descrição
Nome	Nome para os critérios de assunto.
Aplicação	Aplicação com escopo para os critérios do assunto. Este é um campo de apenas leitura e preenchido automaticamente com a aplicação com escopo atual.
Descrição	Descrição dos critérios de assunto

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Clique com o botão direito do mouse no cabeçalho do formulário e clique em **Salvar** no menu de contexto.
   Depois de salvar, os campos **Entradas de critérios** e **Condições de critérios** são exibidos.

Criação de uma entrada de critérios de assunto

Crie uma entrada de critérios de assunto para definir os critérios em que as regras de filtragem de dados filtrarão.

Antes de Iniciar

Função necessária: security_admin

Procedimento

1. No registro de critérios de assunto, abra a guia **Entradas de critérios**.
2. Na lista **Entradas de critérios**, clique em **Novo**.
3. Selecione a entrada de política para os critérios que você deseja criar.

Entradas de política

Entrada de política	Descrição
Critério de filtro de IP	Criação de uma entrada de política com base no endereço IP
Critérios de filtro por função	Criação de uma entrada de política com base na função de uso
Critérios de filtro por grupo	Criação de uma entrada de política com base no grupo de usuário

   Um formulário de **Critérios de filtro de IP**, **Critérios de filtro de função** ou **Critérios de filtro de grupo** é exibido, dependendo da sua seleção nesta etapa.
4. No formulário Critérios de filtro, preencha os campos conforme necessário.

Campos de Critérios de filtro

Campo	Descrição
Nome	Nome para os critérios de filtro
Aplicação	Aplicação com escopo para os critérios do assunto. Este é um campo de apenas leitura e preenchido automaticamente com a aplicação com escopo atual.
Descrição	Descrição dos critérios de filtro

5. Abaixo dos campos de formulário, estão as guias usadas para definir os endereços IP, grupos ou funções das entradas dos critérios de filtro.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Como filtrar campos de critérios para tipos de entrada específicos

Tipo de entrada de política	Descrição	Criação
Critério de filtro de IP	Critérios de filtro de IP do usuário para criar um intervalo ou sub-rede de endereços IP. Os critérios de assunto podem ser comparados ao endereço IP do usuário em relação a este intervalo ou sub-rede.	Use o **Intervalo de IP** ou **Sub-rede (CIDR)** para definir endereços IP para a entrada. Intervalo de IP Na lista **Intervalos de IP**, clique duas vezes em **Inserir uma nova linha** e insira um endereço IP inicial em **IP Inicial**. Em seguida, pressione a tecla Tab e insira um endereço IP final no campo **IP final**. Por fim, pressione Enter para salvar a entrada da lista. Sub-rede (CIDR) Na lista **Sub- redes**, clique duas vezes em **Inserir uma nova linha**e insira um IP de rede no campo **IP de rede**. Em seguida, pressione a tecla Tab e insira uma máscara de rede no campo **Máscara de rede**. Por fim, pressione Enter para salvar a entrada da lista. **Nota:** Os trabalhos agendados que estão sendo acionados por um programador não devem ter dados filtrados usando critérios de rede, já que eles não têm o contexto do IP do cliente solicitante. Um tipo de filtragem mais apropriado pode ser a condição de assunto Função/Grupo.
Critérios de filtro por função	Use os critérios de filtro de função para criar uma seleção de funções. Os critérios de assunto podem ser comparados às funções atribuídas ao usuário em relação a esta seleção.	Use o Construtor de condições no **Campo de condição** para selecionar funções para a entrada.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tipo de entrada de política	Descrição	Criação
Critérios de filtro por grupo	Use os critérios de filtro de grupo para criar uma seleção de grupos de usuário. Os critérios de assunto podem ser comparados aos grupos atribuídos ao usuário em relação a esta seleção.	Na tabela **Grupos para critérios**, clique duas vezes em **Inserir uma nova linha** e selecione um grupo de usuário. Pressione Enter ou clique no ícone de marca de seleção verde para salvar o grupo. Clique no texto **Inserir uma nova linha** abaixo da primeira entrada para criar entradas adicionais.

6. Depois de definir a entrada, clique em **Enviar**.

Nota: Além de criar entradas para seus critérios de assunto, você também pode adicionar as existentes. Clique em **Editar** na guia **Entradas de critérios** e selecione a partir de qualquer entrada existente.

Criação de uma condição de critérios de assunto

Crie uma condição para comparar as informações de um usuário com a entrada de critérios de assunto existentes.

Antes de Iniciar

Função necessária: security_admin

As condições de critério comparam os atributos do usuário às entradas de critérios existentes para determinar se o acesso aos registros deve ser permitido. Para criar uma condição de critérios, você precisa criar critérios de assunto. Para obter detalhes sobre esse processo, consulte Criação de uma entrada de critérios de assunto.

Procedimento

1. No registro de critérios de assunto, abra a guia **Condições de critérios**.
2. Na lista **Condições de critérios**, clique em **Novo**.
3. No formulário **Condição de critérios de assunto**, preencha os campos conforme necessário.

Formulário Condição de critérios de assunto

Campo	Descrição
Rótulo	Um rótulo descritivo para sua condição
Aplicação	Aplicação com escopo para os critérios do assunto. Este é um campo de apenas leitura e preenchido automaticamente com a aplicação com escopo atual.

4. Selecione uma das opções de condição a seguir para criar uma condição para a condição de critérios de assunto usando o Construtor de condições.
Essas opções de condição incluem todas as entradas de critérios de assunto que você criou.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Opcional: Crie mais condições clicando nos botões **Adicionar condição de filtro** ou **Adicionar cláusula "OR"**.

   Nota: A menos que as condições sejam separadas por uma cláusula **ou**, todas as condições deverão ser avaliadas como verdadeiras para que a condição dos critérios do assunto seja avaliada como verdadeira.

6. Clique em **Enviar** para salvar a condição dos critérios do assunto.

O que Fazer Depois

Use critérios de assunto nas regras de filtragem de dados para limitar o acesso a tabelas e registros. Para obter detalhes sobre como usar critérios de assunto em regras de filtragem de dados, consulte Criando critérios de assunto.

Depuração de filtragem de dados

Use o log da sessão para ver como a filtragem de dados afeta seus registros e depurar problemas de acesso do usuário.

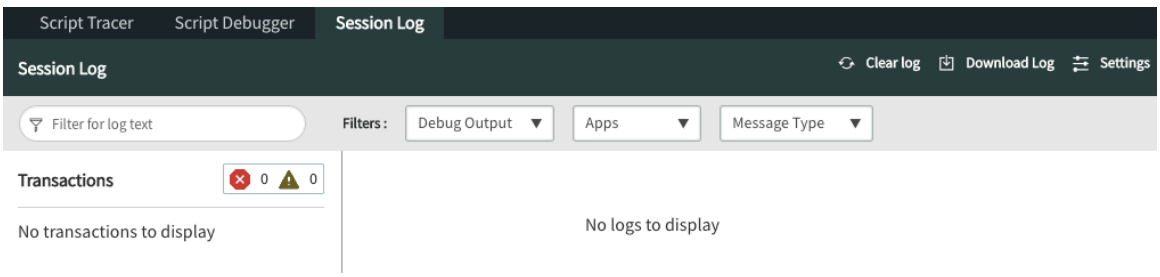
Antes de Iniciar

Função necessária: administrador

As informações de saída aparecem nos logs de sessão quando os usuários acessam os registros. Você pode usar essas informações de registro em log com a representação para saber por que os usuários veem ou não os registros. Você pode usar essas informações para ajustar suas regras de filtragem de dados e garantir que os usuários vejam somente o que você pretende.

Procedimento

1. Navegue até **Todos** > **Segurança do sistema** > **Depuração** > **Depurar toda a segurança**.
   O **Depurador de script** é aberto em uma nova guia ou janela do navegador.



2. Na janela do **Depurador de script**, selecione a guia **Log de sessão**.
3. Em outra guia ou janela do navegador, represente um usuário para solucionar problemas de acesso desse usuário.

   Nota: A representação permite que um administrador veja uma instância com configurações e acesso de outros usuários. Para obter detalhes sobre representação, consulte Representar um usuário.

4. Ao representar um usuário, acesse uma lista ou registro em que você vê um comportamento inesperado.
   Esse comportamento pode ser um registro que o usuário vê, mas não deve ver, ou uma lista de registros que não estão aparecendo conforme o esperado para um usuário.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Depois de acessar registros com o usuário representado, você deve começar a ver a saída no depurador de sessão.

5. Procure informações de filtragem de dados no depurador de sessão.

Este exemplo mostra duas mensagens de log em que um filtro de dados negou acesso aos registros. As entradas de log aparecem como texto em vermelho e incluem o motivo pelo qual o filtro de dados negou acesso, bem como o sys_id do filtro de dados. Você pode clicar nesse sys_id para abrir o registro de filtragem de dados.

Este exemplo mostra uma mensagem de log em que um filtro de dados permitiu acesso a um registro. Essas entradas de log aparecem como texto verde. Assim como na primeira mensagem, você pode clicar nesse sys_id para abrir o registro de filtragem de dados.

6. Use essas informações para fazer ajustes nas regras de filtragem de dados. Repita essas etapas para refinar as regras e dar aos usuários o acesso de que precisam.

Funções de segurança

Funções de segurança fornecem segurança extra, de forma que cada usuário deve ter pelo menos uma função para que a instância possa distinguir entre usuários internos e externos.

Explorar funções explícitas

Aprenda os principais recursos e o valor comercial das Funções explícitas.

Explorar privilégio elevado

Saiba como a função de privilégio elevado habilita privilégios baseados em sessão.

Funções explícitas

Você pode conceder acesso à sua instância a usuários internos e externos. No entanto, talvez você não queira que os dois tipos de usuários tenham o mesmo nível de acesso. Para fornecer segurança adicional, cada usuário deve ter pelo menos uma função para que a instância possa distinguir entre usuários internos e externos.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A partir da versão Paris, nenhum usuário pode ter ambas as funções explícitas (snc_internal e snc_external). Os grupos e a contenção de função não podem incluir as duas funções, já que isso faria com que qualquer membro do grupo ou usuário atribuído a esse grupo ou função tenha automaticamente as ambas as funções. O Now Platform cancela qualquer operação que crie esse cenário.

Usuários externos devem obter, no mínimo, a função snc_external. A função snc_external indica que o usuário é externo à organização. Eles não devem ter nenhum acesso aos recursos, a não ser os permitidos explicitamente por meio de ACLs para a função snc_external ou funções adicionais que herdam a função snc_external. Por padrão, os usuários com a função snc_external não podem acessar:

- Recursos Scripted REST APIs que não estejam marcados como externos.
- Tabelas sem a função que herda a função snc_external ou a função pública.
- Recursos do tipo sem registro, como processadores e páginas de IU sem ter acesso à função snc_external ou uma função que herde a função snc_external.
- Painéis Análise da plataforma.

Não marque a função snc_internal como elevada. Caso contrário, os usuários internos não poderão acessar a instância.

Plug-in Explicit Roles

Quando o plug-in Explicit Roles é ativado:

- Todos os usuários devem ter a função snc_internal para acessar recursos internos ou a função snc_external para acessar recursos externos. Usuários sem nenhuma função explícita podem acessar somente recursos públicos.
- Todos os usuários existentes são atribuídos automaticamente à função snc_internal. Esta função não muda os níveis de acesso existentes ou o comportamento do sistema. Em vez disso, ela fornece uma categoria para diferenciar usuários internos de usuários externos. Todos os usuários internos mantêm o mesmo nível de acesso de antes da ativação do plug-in.

  Dica: Para impedir a mudança da funcionalidade existente para os usuários, a ativação do plug-in Explicit Roles atribui a função do usuário snc_internal a todos os usuários existentes na instância. Isso inclui todos os usuários externos adicionados antes da ativação do plug-in Explicit Roles. Depois que o plug-in Explicit Roles for ativado, faça o seguinte para todos os usuários externos adicionados antes da ativação do plug-in Explicit Roles:

  - Remova a função snc_internal.
  - Adicione a função snc_external.

  Fazer isso garante que os usuários externos adicionados antes de ativar o plug-in Explicit Roles não tenham acesso a recursos internos que devem estar disponíveis somente para usuários internos.

- Usuários recém-criados são atribuídos automaticamente à função snc_internal quando eles tentam se conectar à instância pela primeira vez, a menos que a função snc_external seja explicitamente atribuída a eles. Você pode adicionar a função snc_external a um novo usuário antes de ele se conectar à instância para fornecer direitos de usuário externo.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Importante:

Ative este plug-in durante uma janela de manutenção ou quando poucos usuários estiverem conectados. Os usuários conectados no momento em que o plug-in for ativado não serão atribuídos dinamicamente à função snc_internal. Em vez disso, os usuários devem sair e conectar-se novamente para serem atribuídos à função snc_internal. Quando o plug-in estiver ativado, você pode adicionar ou remover as funções snc_internal e snc_external a qualquer momento para alterar os direitos do usuário.

Depois que o plug-in é ativado, sempre que um usuário se conecta, ele recebe a função snc_internal se a conta ainda não tiver essa função, ou a função snc_external. Isso inclui usuários conectados por meio de representação.

- Todas as ACLs existentes que não tenham um requisito de função são atribuídas automaticamente à função snc_internal. Como as ACLs e os usuários existentes foram atribuídos à função snc_internal, os níveis de acesso existentes não mudam.
- As ACLs recém-criadas que não tenham um requisito de função são atribuídas automaticamente à função snc_internal. Esta atribuição de função não se aplica a uma ACL recém-criada com uma função atribuída.
- Para todos os registros de Processador [sys_processor] existentes ou registros de Processador [sys_processor] recém-criados com **Type=script**, a função snc_internal será adicionada automaticamente ao campo **Funções** se este estiver vazio.
- Para restringir o acesso a páginas de IU a usuários internos, o plug-in atribui automaticamente a função snc_internal à ***** ACL com um **Tipo** de **ui_page**.
- Para restringir o acesso a processadores a usuários internos, o plug-in atribui automaticamente a função snc_internal à ***** ACL com um **Tipo** de **processador**.
- Usuários externos devem obter, no mínimo, a função snc_external para acessar a instância. Esta função deve ser concedida manualmente a usuários externos. O acesso aos registros é concedido por meio de ACLs.

Não mova Conjuntos de atualizações do sistema entre instâncias com e sem o plug-in Explicit Roles habilitado. Para obter mais informações, consulte Conjuntos de atualizações do sistema.

Nota: Este plug-in também requer o plug-in Contextual Security Manager.

Comportamento de glide.security.explicit_roles.do_not_fix

A partir da versão Xanadu, `glide.security.explicit_roles.do_not_fix` passou por ajustes e mudou para snc_internal. Agora, a função snc_internal é a mesma na memória e em sys_user_has_role. O novo comportamento de `glide.security.explicit_roles.do_not_fix` é:

Novo comportamento de glide.security.explicit_roles.do_not_fix

Valor	Resultado
Falso	Adicionar a função snc_internal à memória e a sys_user_has_role
Verdadeiro	Não adicionar a função snc_internal à memória nem a sys_user_has_role

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para excluir a função snc_internal de determinados usuários, use a propriedade `glide.security.explicit_roles.ignore.snc_internal.exclude_role_list`.

Dica: Para reverter para o comportamento anterior de `glide.security.explicit_roles.do_not_fix`, use a propriedade `glide.security.explicit_roles.do_not_fix_in_memory`.

Fornecendo acesso a tabelas para usuários externos

Você pode fornecer a usuários externos acesso a uma tabela adicionando uma função à tabela que herda a função snc_external. Para obter mais informações, consulte Forneça aos usuários externos acesso a uma tabela.

O método hasRoles()

O método `hasRoles()` ainda está disponível, mas será descontinuado na versão Geneva. Em vez disso, use o método `hasRole(nome da função)`.

Se você usar o método `hasRoles()`, observe estas mudanças:

- Este método exclui automaticamente a função snc_internal ao verificar as funções. Isso significa que se um usuário tiver apenas a função snc_internal, o método `hasRoles()` ainda retornará **falso**.
- Se o usuário tiver a função snc_external, o método retornará **falso** porque a instância considera que os usuários externos não têm uma função.

Exclusão mútua: snc_external versus snc_internal

Now Platform impede que os usuários tenham as funções snc_external e snc_internal. Now Platform aplica esta exclusão mútua em todos os lugares do sistema e grava mensagens de erro nos logs de cada conflito.

Nota: As ACLs podem ter ambas as funções se os recursos de ACL devem ser acessíveis a todos os usuários.

Exemplo: adicionar as duas funções explícitas a um usuário (colisão direta):

1. Atribua ao usuário Abel Tuter a função snc_internal.
2. Atribua ao usuário Abel Tuter a função snc_external.

Resultado: a adição da função snc_external falhará porque Abel Tuter tem a função snc_internal.

Exemplo: adicionar as duas funções explícitas a um grupo (colisão direta):

1. Considere um grupo chamado Grupo de Teste que atualmente não tem funções explícitas atribuídas a ele.
2. Adicione Abel Tuter ao Grupo de Teste.
3. Adicione a função snc_external ao Grupo de Teste.

Resultado: a adição da função snc_external falhará porque Abel Tuter já tem a função snc_internal e não pode ter as duas funções.

Exemplo: adicionar uma função explícita a um grupo em que um membro do grupo tem a função explícita conflitante (colisão indireta):

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

1. Atribua ao usuário Abel Tuter a função snc_internal.
2. Considere um grupo chamado Grupo de Teste que atualmente não tem funções explícitas atribuídas a ele.
3. Adicione Abel Tuter ao grupo de teste.
4. Adicione a função snc_external ao Grupo de Teste.

Resultado: a adição da função snc_external ao grupo falhará porque Abel Tuter herdaria a função snc_external por sua associação ao grupo. As duas funções explícitas seriam atribuídas ao mesmo usuário, o que não é permitido.

Para outros exemplos, consulte a tabela a seguir:

Função	Tentativa de ação	Resultado
Colisão direta		
O usuário tem a função snc_internal.	Adicione a função snc_external.	A ação é anulada.
O usuário tem a função snc_external.	Adicione a função snc_internal.	A ação é anulada.
O usuário não tem função explícita.	Adicione a função snc_internal ou snc_external.	A função é adicionada.
O usuário tem ambas as funções explícitas (colisão existente).	Adicione o usuário a um grupo sem funções.	A ação é anulada.
Uma função não associada a nenhum usuário contém a função snc_internal.	Adicione a função snc_external.	A ação é anulada.
Uma função não associada a nenhum usuário contém a função snc_external.	Adicione a função snc_internal.	A ação é anulada.
Uma função tem ambas as funções explícitas (colisão existente).	Adicione a função a um usuário, função ou grupo.	A ação é anulada.
Um grupo sem membros tem a função snc_internal.	Adicione a função snc_external.	A ação é anulada.
Um grupo sem membros tem a função snc_external.	Adicione a função snc_internal.	A ação é anulada.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Função	Tentativa de ação	Resultado
Um grupo sem membros não tem funções.	Adicione a função snc_internal ou snc_external.	A função é adicionada.
Colisão indireta		
Contenção de função com colisão	**1.** Conceda uma função chamada Função de Teste a um usuário com a função snc_internal. **2.** Adicione a função snc_external à Função de Teste.	A ação é anulada.
Contenção de função sem colisão	**1.** Conceda uma função chamada Função de Teste a um usuário sem funções. **2.** Adicione a função snc_external à Função de Teste.	A função é adicionada ao usuário e à Função de Teste.
Contenção de grupo com colisão	**1.** Adicione um usuário que tenha a função snc_internal a um grupo chamado Grupo de Teste 2 (secundário do Grupo de Teste 1). **2.** Adicione a função snc_external ao Grupo de Teste 2. **3.** Adicione a função snc_external a um grupo primário chamado Grupo de teste 1 (primário do Grupo de Teste 2).	A ação é anulada.
Contenção de grupo sem colisão	**1.** Adicione um usuário sem funções a um grupo chamado Grupo de Teste 2 (secundário do Grupo de Teste 1). **2.** Adicione a função snc_external ou snc_internal ao Grupo de Teste 1 (primário do Grupo de Teste 2).	A função é adicionada ao grupo primário, ao grupo secundário e ao usuário.
Contenção de grupo com colisão mais contenção de função com colisão	Adicione contains_external ao Grupo de Teste 1, o primário do Grupo de Teste 2.	O Grupo de Teste 1 e o Grupo de Teste 2 obtêm contains_external, mas não obtêm explicitamente a função snc_external.
	Adicione a função snc_internal ao Grupo de Teste 2, o secundário do Grupo de Teste 1.	A ação é anulada.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Função	Tentativa de ação	Resultado
Mudança de grupo primário mais contenção de grupo	**1.** Remova o Grupo de Teste 1 como primário do Grupo de Teste 2. **2.** Adicione a função snc_internal ao Grupo de Teste 1. **3.** Adicione a função snc_external ao Grupo de Teste 2. **4.** No Grupo de Teste 2, defina o Grupo de Teste 1 como o grupo primário e salve.	A ação é anulada. Repita para grupos já aninhados, com a mesma expectativa.

A causa de uma ação anulada aparece na mensagem de erro e deve ser resolvida antes que outra tentativa seja bem-sucedida.

Para casos diretos, como adicionar uma função explícita a um usuário individual, verifique qual função explícita o usuário deve ter. Se o usuário tiver a função explícita incorreta, ele deverá ser removido primeiro e, em seguida, a função explícita correta deverá ser adicionada.

Para casos indiretos, como adicionar uma função explícita a um grupo (para que um membro do grupo receba as duas funções explícitas), avalie se esse usuário deve estar no grupo. Além disso, determine se o grupo deve receber a função explícita, incluindo qualquer herança por meio da hierarquia de grupo e contenção de função.

Observe que o Now Platform relata somente a primeira colisão possível encontrada. Se as tentativas repetidas continuarem a falhar após a correção, com uma causa raiz diferente a cada vez, reavalie a interdependência de usuário / grupo / função relevante de forma mais ampla. Talvez seja necessário repensar como os grupos e as contenções de função estão estruturados.

Como solicitar Funções explícitas

Ative Funções explícitas solicitando o plug-in "Explicit Roles" (com.glide.explicit_roles) por meio do Now Support Catálogo de serviços.

Antes de Iniciar

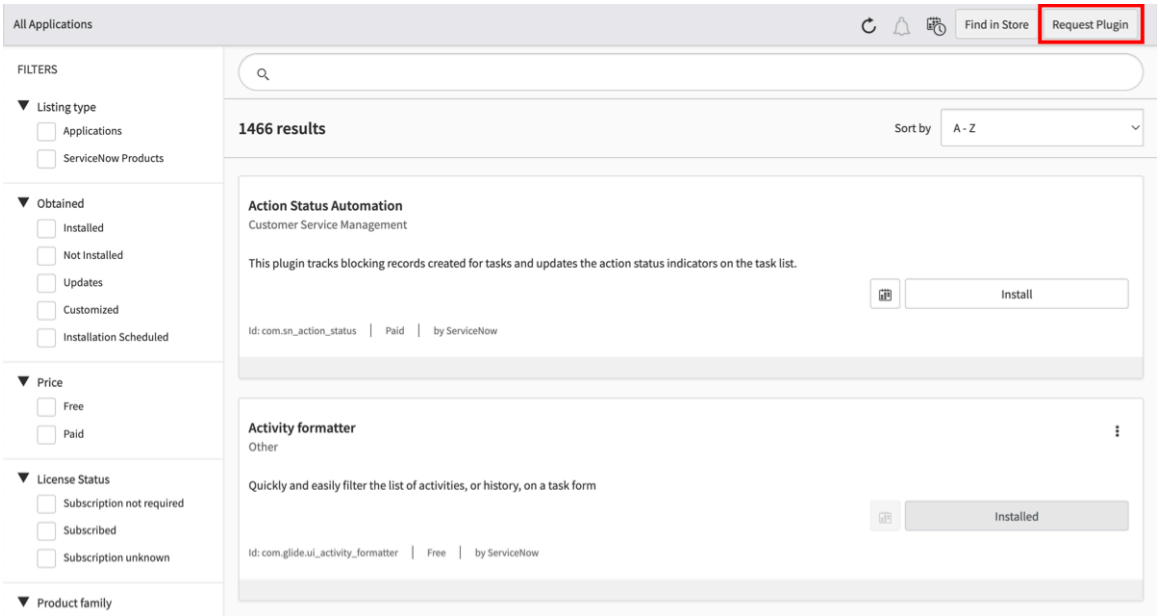
Função necessária: administrador

Importante: Ative este plug-in durante uma janela de manutenção ou quando poucos usuários estiverem conectados. Os usuários conectados no momento em que o plug-in for ativado não serão atribuídos dinamicamente à função snc_internal. Em vez disso, os usuários devem sair e conectar-se novamente para serem atribuídos à função snc_internal. Quando o plug-in estiver ativado, você pode adicionar ou remover as funções snc_internal e snc_external a qualquer momento para alterar os direitos do usuário.

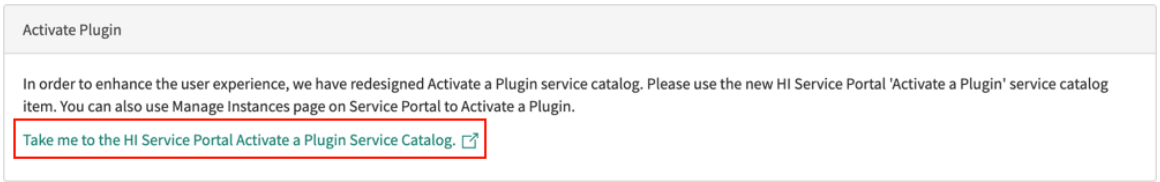
Procedimento

1. Navegue até **Todas** > **Aplicações do sistema** > **Todas os aplicações disponíveis** > **Todas**.
2. Na página Todas as Aplicações, selecione **Solicitar plug-in** para abrir o formulário **Ativar plug-in** em Now Support.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. No Now Support, selecione o link para acessar o Now Support Portal de serviços Catálogo de serviços.



4. Selecione sua instância.
5. Selecione **Ações > Ativar plug-in**.
6. No formulário **Ativar plug-in**, forneça as seguintes informações.

Formulário Ativar plug-in

Campo	Descrição
Qual é a sua instância de destino	Instância na qual o plug-in será ativado.
Qual plug-in você deseja ativar	Nome do plug-in a ser ativado. **Nota:** Se o sistema não listar o plug-in desejado ou se você estiver ativando o plug-in em uma instância do OEM ou no local, marque a caixa de seleção O **plug-in que estou procurando não está listado** e insira o nome do plug-in.
Selecionar data e hora de manutenção	A data e a hora para ativar o plug-in.

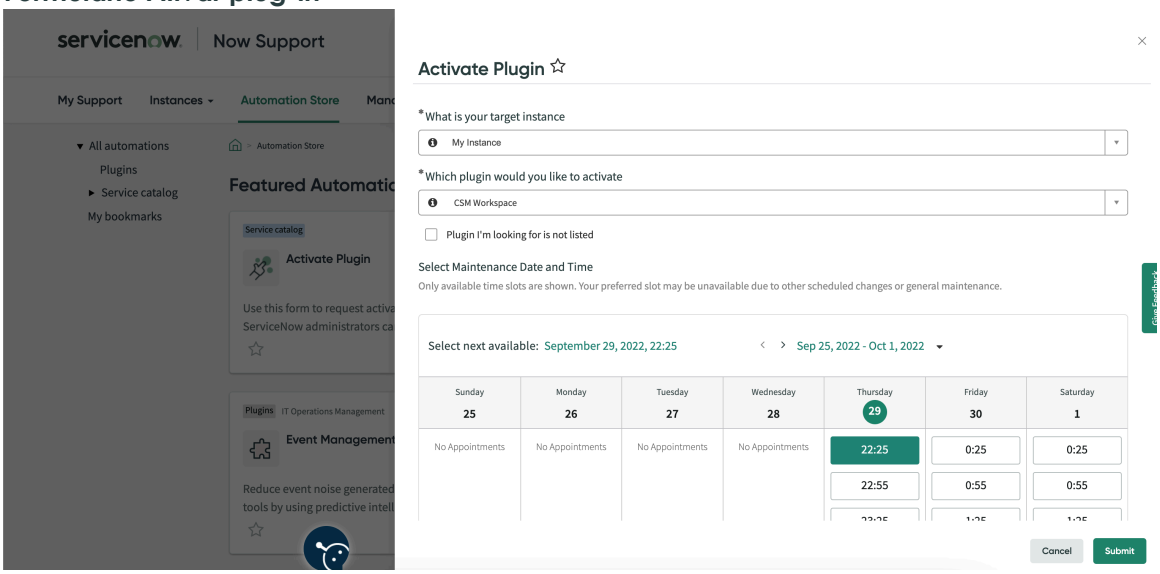
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: Os plug-ins são ativados em dois lotes, uma pela manhã e outra à noite, em todos os dias úteis no fuso horário do Pacífico dos EUA. Se o plug-in deve ser ativado em um momento específico, insira a solicitação no campo **Motivo/ Comentários**.

Example

Por exemplo, consulte o formulário a seguir para ativar o plug-in Espaço de trabalho CSM em uma instância chamada Minha instância.

Formulário Ativar plug-in



7. Selecione **Enviar**.
   Para obter detalhes adicionais sobre como solicitar um plug-in, consulte Solicitar um plug-in no artigo do Catálogo de serviços [KB0751715] em Now Support Base de conhecimento.

Funções de privilégio elevado

Funções de privilégio elevado exigem que você aceite manualmente a responsabilidade de usar a função antes de acessar os recursos da função.

Por padrão, você não tem funções de privilégio elevado ao fazer login. Você deve elevar manualmente o privilégio da função. Uma função de privilégio elevado dura apenas o tempo de duração da sessão do usuário. O tempo limite ou logout da sessão remove a função.

Você pode designar qualquer função como uma função de privilégio elevado e atribuir essa função a um ou mais usuários. Faça isso quando quiser impedir que os usuários tenham acesso aos direitos que a função fornece imediatamente após o login. Você pode designar a função de privilégio no formulário Função. Consulte Criar uma função para obter instruções.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para usar uma função elevada, você deve atender a estas condições:

- A função elevada deve ser atribuída a você.
- Você deve elevar manualmente para uma função elevada específica para obter seus privilégios, mesmo se você já estiver elevado a uma segunda função elevada que contém a primeira função elevada.

  Por exemplo, se a função elevada A contiver a função elevada B, mesmo se você elevar para a função A, ainda deverá elevar para a função B para obter seus privilégios.

Função de administrador

Para conceder a função de administrador a um usuário, o usuário que fez a concessão também deve ter a função de administrador. Por exemplo, um usuário com apenas a função user_admin não pode conceder a função de administrador a outros usuários.

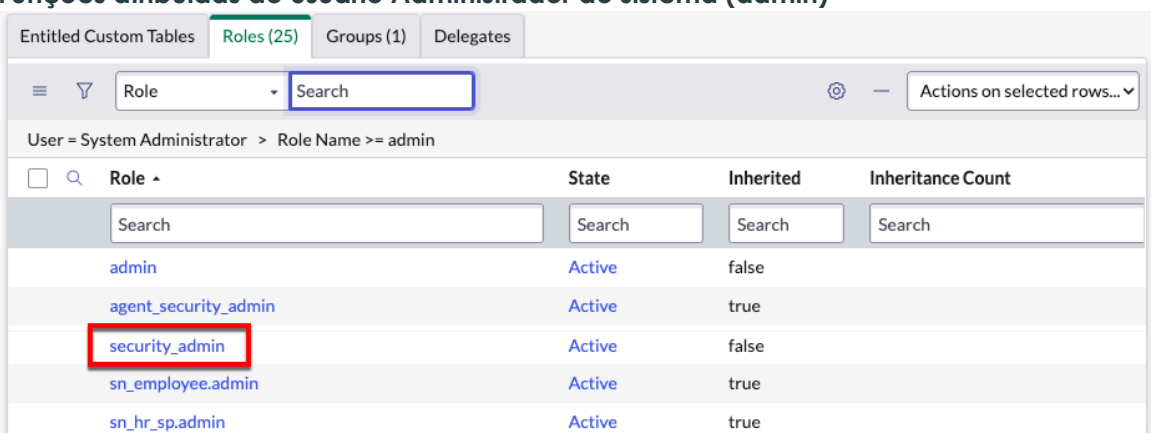
- Usuários não administradores não podem adicionar um usuário a um grupo que contém a função de administrador.
- Para conceder a função security_admin a um usuário, o usuário que concedeu também deve ter a função de administrador e deve ser elevado à função security_admin antes de conceder a função security_admin a outros usuários. Um usuário com apenas a função de administrador não pode conceder a função security_admin a outros usuários.
- Um usuário sem a função security_admin não pode adicionar um usuário a um grupo que contém a função security_admin.

Aviso: O uso de privilégios elevados na função de administrador não é compatível e pode causar um comportamento inesperado. Para exigir que os administradores elevem manualmente, consulte Como forçar os administradores a elevar manualmente.

A função security_admin.

No sistema de base, a função security_admin é a única função que tem privilégios elevados. Essa função é atribuída automaticamente ao usuário Administrador do sistema (admin) padrão. Ela fornece acesso a ACLs e Configurações de alta segurança.

Funções atribuídas ao usuário Administrador do sistema (admin)



Nota: Para ver essa função, você deve elevar para a função security_admin primeiro. Se você estiver conectado como usuário Administrador do sistema (admin), não poderá ver o registro security_admin na lista de funções.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Função security_admin.

A função security_admin é uma função de privilégio elevado fornecida com Configurações de Alta Segurança que permite aos usuários criar e alterar controles de acesso e mudar as Configurações de alta segurança.

No sistema de base, somente o usuário administrador do sistema (admin) padrão tem a função security_admin. Como isso requer a elevação de privilégios, o usuário administrador não tem essa função no login. Depois de elevar os privilégios, o usuário administrador tem a função security_admin pela duração da sessão do usuário. Para obter mais informações, consulte Elevação para uma função privilegiada.

Para manter a segurança alta, a função security_admin requer privilégios elevados. Limite os usuários e grupos aos quais você atribui essa função.

Elevação para uma função privilegiada

O administrador do sistema de base pode elevar a uma função privilegiada para ter acesso aos recursos das configurações de alta segurança.

Antes de Iniciar

Função necessária: administrador

Nota: Se você conceder a usuários adicionais a função de administrador, eles não poderão ser elevados a uma função privilegiada. Somente o administrador do sistema de base pode elevar.

Procedimento

1. Na faixa superior, clique em sua imagem ou clique em suas iniciais se você não tiver uma imagem carregada.
2. Selecione **Elevar funções**.
   Uma caixa de diálogo é exibida contendo as funções disponíveis para elevação.
3. Selecione as funções elevadas a serem atribuídas e clique em **OK**.
   Esta função concede ao usuário privilégios elevados para todos os recursos controlados pela função para o restante da sessão. Quando o usuário faz logout, os privilégios elevados são encerrados com a sessão, mas podem ser restabelecidos no próximo login.
4. Encerre a elevação de função retornando à caixa de diálogo na etapa 2 e desmarcando a função.

Como forçar os administradores a elevar manualmente

Uma propriedade está disponível para forçar todos os usuários com a função de administrador a selecionar manualmente a função para a qual desejam elevar.

Antes de Iniciar

Função necessária: security_admin

Procedimento

1. Faça login como administrador.
2. Eleve sua função para security_admin.
3. Navegue até **sys_properties.list**.
4. Pesquise e selecione a propriedade *glide.security.strict_elevate_privilege*.
5. Defina o campo Valor como **verdadeiro** e clique em **Enviar**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resultados
Quando o usuário faz login, é apresentada uma janela de diálogo para selecionar a função para a qual ele pode elevar.

Conexões e credenciais

As credenciais e as informações de conexão são necessárias para obter acesso a um computador ou dispositivo de rede para Descoberta, Mapeamento de Serviços e Gestão de nuvem ou para executar o trabalho usando Orquestração. Ao adicionar conteúdo ao compartilhamento ou à AppStore, você pode configurar conexões e credenciais relevantes ao seu ambiente sem modificar o conteúdo criado.

Explorar Saiba mais sobre credenciais.	Configurar Configurar credenciais.
Referência Veja os detalhes sobre credenciais.	Solução de problemas Saiba como solucionar problemas em conexões e credenciais.

Explorando credenciais, conexões e aliases

Todas as integrações de aplicação no Now Platform usam conexões, credenciais e aliases para permitir que as aplicações acessem os recursos.

Antes de poder executar uma integração de aplicação no Now Platform, você deve criar e configurar informações de conexão, credenciais correspondentes e adicionar um alias. Para entender como ServiceNow define estes termos:

Conexão

Uma conexão é uma integração com um sistema, como um endereço IP ou endpoint com protocolos. Ele contém detalhes específicos, como detalhes de banco de dados, ao integrar a um banco de dados.

Credencial

Uma credencial são dados de autenticação necessários para estabelecer a conexão, como um ID e senha.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Alias

Um alias é uma convenção de nomenclatura, ou tag, que se vincula a um conjunto de conexões ou credenciais em sua instância. Um alias contém as informações de credencial e conexão necessárias para fazer uma integração de aplicação. Em vez de inserir essas informações sempre que integrar, é possível usar um alias. Por exemplo, é possível designar um alias para hospedar suas credenciais de CQ, desenvolvimento e produção para a mesma integração de aplicação. O alias resolve a integração da aplicação para cada ambiente.

O Now Platform distingue diferentes tipos de aliases:

Alias de credencial

Este alias se associa apenas aos dados de credencial e é resolvido durante o tempo de execução.

Alias de credencial e conexão

Este alias se associa às informações de conexão e aos dados de credencial necessários para concluir a integração e é resolvido durante o tempo de execução.

Nos aliases de conexão e credencial, também é possível criar aliases adicionais chamados de aliases secundários. Os aliases secundários permitem que você crie várias conexões na mesma integração de aplicação. Ao criar um alias secundário, o alias sob o qual você o criou se torna um alias primário. Enquanto os aliases secundários herdam as propriedades de seus alias primários, os aliases secundários carregam suas próprias informações de conexão e credencial.

Benefícios de usar as Conexões, Credenciais e Aliases

- Local central para armazenar e gerenciar credenciais para um serviço externo
- Defina uma vez e reutilize para vários recursos da plataforma
- Minimize a configuração de outros recursos da plataforma
- Permita que não administradores usem conexões e credenciais predefinidas
- Maior segurança

Recursos que usam Conexões, Credenciais e Aliases

Os seguintes recursos usam conexões, credenciais e aliases:

- Flow Designer
- IntegrationHub
- Gestão de nuvem
- Descoberta
- Orquestração
- Mapeamento de serviços

É possível configurar os aliases no Now Platform de uma de duas maneiras:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Usando o módulo Conexões e credenciais. Consulte Crie um alias de Conexão e Credenciais.
- No painel de conexões de Integration Hub. Consulte Adicionar uma conexão.

Nota: Integration Hub requer uma assinatura separada. Para obter mais informações, consulte SolicitaçãoIntegration Hub.

Sincronização de credenciais em MID Servers

Cada MID Server em sua rede sincronizado com a instância mantém uma cópia de cada credencial que você cria. O (MID) Server Gestão, Instrumentação e Descoberta é um aplicativo Java que habilita a comunicação e o movimento dos dados entre uma instância ServiceNow e aplicativos externos, fontes de dados e serviços. Esta sincronização acelera a leitura de credenciais quando aplicações como Descoberta ou Mapeamento de serviços precisarem acessar vários dispositivos na rede. Os MID Servers são sincronizados quando encontram um trabalho *credentials_reload* na Fila do ECC. O trabalho de recarregamento instrui o MID Server a fazer uma chamada SOAP para a instância para obter a lista inteira de credenciais na tabela Credenciais [discovery_credentials], incluindo todos os valores de campos. Para saber mais, consulte MID Server.

A resposta SOAP que sua instância envia para cada MID Server também inclui campos personalizados que você adicionou a qualquer formulário de credencial que tenha personalizado. Se você adicionou campos de referência, os dados na tabela referenciada também serão enviados como parte da resposta SOAP. Isso pode levar a problemas de desempenho quando ocorre a sincronização de credenciais com vários MID Servers. Para controlar isso, adicione manualmente essas propriedades à tabela Propriedades do sistema [sys_properties]:

Nota: Para alterar os valores nessas propriedades, adicione-os à tabela Propriedades do sistema [sys_properties]. Se você não adicioná-los, o sistema usará o valor padrão.

Propriedade	Descrição
`com.snc.credentials_user_fields`	Inclui todos os campos personalizados na sincronização de credenciais. Defina esta propriedade como falsa se não deseja incluir os campos que você adicionou aos formulários de credencial. • **Tipo**: verdadeiro | falso • **Valor padrão**: verdadeiro
`com.snc.credentials_recursion_depth`	Define o número de tabelas a serem percorridas quando o mecanismo de sincronização de credenciais coletar os campos das tabelas de referência. Reduza este número se você estiver com problemas de desempenho e tiver personalizado formulários de credencial que incluem campos de referência para tabelas que também têm campos de referência. • **Tipo**: inteiro • **Valor padrão**: 3

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Proteções de escopo para credenciais e conexões

Você pode classificar determinados tipos de registros de Conexão e Credencial como pertencentes a um escopo e estender as proteções de escopo a eles. Essas políticas de escopo protegem os registros criados em uma tabela e evitam interações com registros privados para outro escopo.

Um campo **Aplicação** fica disponível nas tabelas Conexão [sys_connection] e Credenciais do Descoberta [discovery_credentials] para associar esses tipos de registros a escopos específicos. Ele não fica visível em formulários de IU no Xanadu, mas é possível adicioná-lo facilmente a eles. Para saber mais sobre esses tipos de registro e como adicionar o campo aos formulários de IU, consulte:

- Introdução às conexões
- Introdução às credenciais
- Aliases de credencial da Descoberta
- Configuração do layout do formulário

Restringir o uso de um registro de conexão e credenciais a um escopo específico é importante para gerenciar aplicações que exigem segurança imposta. Esses aplicações incluem Prestação de serviços de RH ou Operações de segurança Os registros de conexão e credenciais criados em aplicações administradas com escopo não ficam visíveis para os usuários administradores. Associar um registro de Conexão e Credenciais a um escopo da aplicação específico oferece as seguintes proteções:

- Aplica regras de ACLs (lista de controle de acesso) a escopos restritos. Para saber mais sobre as ACLs em escopo, consulte Regras da lista de controle de acesso.

  Nota: Algumas aplicações que usam administração de escopo e segurança aplicada podem exigir configuração adicional. Para saber mais, consulte Gerenciar funções de RH

- Protege registros quando consultados usando um script. Se você fizer uma consulta do escopo Global e o registro de Conexão e Credencial estiver em um escopo protegido, ele não aparecerá na consulta, a menos que seja concedido acesso a ele.

É possível personalizar e conceder acesso a registros de consulta restrita usando o Acesso restrito de chamador. Para saber mais, consulte Configurações do privilégio de acesso do chamador restrito. As restrições de escopo também se aplicam a todas as tabelas secundárias das tabelas Conexão [sys_connection] e Credenciais do Descoberta [discovery_credentials]. Campos vazios e outros escopos não são restritos.

Nota: As proteções de escopo são habilitadas apenas para escopos protegidos específicos para evitar confusão ao configurar novos registros. Se alguém fizer uma conexão no escopo da aplicação com escopo, não haverá restrição de escopo automática.

Separação de domínio e credenciais e conexões

A separação de domínio é suportada em Credenciais e conexões. O Domain Separation permite separar dados, processos e tarefas administrativas em agrupamentos lógicos chamados de domínios. Você pode controlar vários aspectos dessa separação, incluindo quais usuários podem ver e acessar os dados.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nível de suporte: Padrão

- Inclui nível de suporte **Básico**.
- Lógica de negócios: o provedor de serviço (SP) cria ou modifica processos por cliente. Os casos de uso refletem o uso adequado do aplicativo por vários clientes de SP em uma única instância.
- O proprietário da instância deve configurar a lógica de negócios do produto minimamente viável (MVP) e os parâmetros de dados por locatário conforme esperado para o aplicativo específico.

Exemplo de caso de uso: um administrador deve ser capaz de fazer os comentários necessários quando um registro é encerrado para um locatário, mas não para outro.

Para obter mais informações sobre os níveis de suporte, consulte Suporte de aplicação para separação de domínio.

Visão geral

As credenciais estão vinculadas a vários recursos ServiceNow que acessam sistemas fora da instância. As credenciais seguem a separação de domínio vinculada ao recurso que usa as credenciais.

Conexões são informações específicas do protocolo que fazem referência a um host de destino fora da instância. Uma conexão pode especificar o domínio para executar uma atividade.

Como funciona a separação de domínio em Credenciais e conexões

As credenciais acessam os recursos fora da instância e são usadas pelas aplicações Descoberta, Orquestração, Mapeamento de serviços e Cloud Provisioning and Governance. Essas credenciais não estão vinculadas a um domínio específico. Em vez disso, elas podem ser vinculadas a uma aplicação e depois seguir a separação de domínio que o aplicativo usa. As credenciais também podem ser atribuídas a um MID Server e então seguir a separação de domínio especificada pela configuração MID Server.

As conexões acessam um host de destino usando uma conexão JMS, JDBC ou HTTP(s). É possível especificar um domínio global ou específico ao qual a conexão pertence.

Informações relacionadas

Domain Separation para provedores de serviço

Modelos de configuração de Conexão e credencial

Permita que usuários com as funções admin e flow_designer configurem integrações de spoke com sistemas de terceiros usando um formulário único e personalizável.

Por exemplo, é possível configurar uma integração OAuth, que registra um provedor OAuth, gera um token e cria registros de conexão e de credencial. Um designer de ação ou desenvolvedor pode usar um modelo de configuração para configurar o spoke em um lugar e o sistema cria os registros associados.

Benefícios

Os modelos de configuração habilitam:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Administradores ou designers de fluxo a configurar integrações complexas usando um único formulário.
- Desenvolvedores a definir valores estáticos em uma integração, simplificando o processo de configuração para administradores e designers de fluxo.

Tipos de credenciais suportados

É possível criar modelos de configuração para integrações com estes tipos de credencial:

- Autorização básica
- Chave de API
- Tipo de concessão do portador OAuth JWT
- Tipo de concessão do Código de autorização OAuth
- Autenticação personalizada

Componentes do modelo de configuração

Modelo de Dados Padrão

Define informações estáticas que se aplicam a todas as integrações. Por exemplo, é possível definir a API e o URL do token se o valor se aplicar a cada integração.

Modelo de dados dinâmico

Define as informações que o usuário deve preencher para configurar a integração. Por exemplo, você pode adicionar pares de chave-valor de nome de usuário e senha para coletar valores definidos pelo usuário.

Script de pós-processamento

Cria registros adicionais necessários para a integração. Por exemplo, se o seu spoke incluir tabelas personalizadas, você poderá criar registros nessas tabelas com base na entrada do usuário no modelo de configuração. Este script é executado depois que os registros de conexão e de credencial são criados.

Script de pré-edição

Preenche previamente os campos personalizados na seção **Informações adicionais** ao editar uma conexão existente. O preenchimento prévio dos campos personalizados permite que você exiba o valor atual associado ao campo personalizado.

Dados de demonstração

A tabela Modelos de conexão e credencial [sys_alias_templates] inclui modelos de exemplo para demonstrar como configurar modelos para tipos de autenticação comuns. Use estes exemplos como um guia ao criar o seu próprio.

Configure um modelo para o tipo de concessão do Portador OAuth JWT

Este modelo de configuração de exemplo define registros de Credencial e conexão usando o tipo de concessão de Portador JWT para autenticar solicitações para Docusign.

Modelo de dados padrão

Cada item de nível superior no modelo de dados padrão cria um registro associado. O modelo inclui estas seções:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- `Credencial`: cria um registro na tabela Credenciais.
- `Conexão`: cria um registro na tabela Conexões [sys_connection] e qualquer registro de conexão associado.
- `Adicional`: cria opcionalmente registros em uma tabela personalizada. O script de pós-processamento informa ao sistema o que fazer com esses registros.

O exemplo a seguir cria os registros necessários para autenticação do tipo de concessão do Portador OAuth JWT.

```
{
  "credential": {
    "oauth_entity": {
      "oauth_entity_profile": [
        {
          "grant_type": "urn:ietf:params:oauth:grant-type:jwt-bearer",
          "name": "Docusign Profile",
          "default": true,
          "oauth_entity_profile_scope": [
            "users:read.email"
          ]
        }
      ],
      "code_challenge_method": "S256",
      "type": "consumer",
      "oauth_entity_scope": [
        {
          "oauth_entity_scope": "users:read.email",
          "name": "email"
        }
      ],
      "client_id": "<provider-client-id>",
      "use_mutual_auth": false,
      "revoke_token_url":
 "https://<provider-domain-name>.com/oauth2/revoke",
      "default_grant_type":
 "urn:ietf:params:oauth:grant-type:jwt-bearer",
      "public_client": false,
      "oauth_api_script": "3e3a3a11c333210016194ffe5bba8f70",
      "name": "Docusign Spoke OAuth",
      "client_secret": "<provider-client-secret>",
      "auth_url": "https://<provider-domain-name>.com/oauth2/auth",
      "token_url": "https://<provider-domain-name>.com/oauth2/token",
      "redirect_url":
 "https://<instance-name>.service-now.com/oauth_redirect.do"
    },
    "jwt_provider": {
      "jwt_keystore_aliases": {
        "kid": "<provider-key-id>",
        "name": "Docusign Spoke JWT Key",
        "signing_keystore": "<signing-keystore-sys-id>",
        "signing_algorithm": "rsa_256",
        "signing_key_password": "password"
      },
      "jwt_claim_validation" : [ {
        "name" : "iss",
```

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

```
        "is_standard" : true,
        "data_type" : "string",
        "value":"<docusign-iss-claim>"
      }, {
        "name" : "sub",
        "is_standard" : true,
        "data_type" : "string",
        "value":"<docusign-sub-claim>"
      }, {
        "name" : "aud",
        "is_standard" : true,
        "data_type" : "string",
        "value":"<docusign-aud-claim>"
      }, {
        "name" : "scope",
        "is_standard" : false,
        "data_type" : "string",
        "value" : "signature impersonation"
      } ],
      "name": "Docusign Spoke JWT Provider",
      "jwt_api_script": "9ef6af86ff10330001d3cd6bd53bf144"
    },
    "name": "Docusign Spoke Credential",
    "table": "oauth_2_0_credentials"
  },
  "connection": {
    "use_mid": false,
    "connection_url": "https://<provider-domain-name>.com",
    "name": "Docusign Spoke Connection",
    "table": "http_connection"
  },
"additional":{
    "docusign_account_name": "<docusign-account-name>",
    "docusign_account_email": "<docusign-account-email>"
}
}
```

Esquema de dados dinâmicos

O esquema de dados dinâmicos define o que o usuário vê quando cria um alias de Conexão e credencial e coleta sua entrada. Use a sintaxe de referência com pontos para mapear a entrada do usuário para campos criados no modelo de dados padrão. Por exemplo, o `connection_fields` mapeia a entrada de usuário para o campo `connection_url` no objeto `connection` criado pelo modelo de dados padrão.

```
{
  "connection_fields": [
    {
      "name": "connection.connection_url",
      "label": "Connection URL",
      "type": "text",
      "defaultValue": "https://demo.docusign.net",
      "hint": "Connection URL for Docusign"
    }],
"additional_fields":[
    {
      "name": "additional.docusign_account_id",
```

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

```
      "label": "Docusign Account Number",
      "type": "text",
      "hint": "Docusign Account Number"
    },
    {
      "name": "additional.docusign_account_name",
      "label": "Docusign Account Name",
      "type": "text",
      "hint": "Name to identify the Docusign account"
    },
    {
      "name": "additional.docusign_account_email",
      "label": "Docusign Account Email",
      "type": "text",
      "hint": "Docusign Account Email"
    }
 ],
 "credential_fields": [
    {
      "name": "credential.oauth_entity.client_id",
      "label": "OAuth Client ID",
      "type": "text",
      "hint": "Client ID for Docusign"
    },
    {
      "name": "credential.oauth_entity.redirect_url",
      "label": "OAuth Redirect URL",
      "type": "text",
      "defaultValue":
"https://<instance-name>.service-now.com/oauth_redirect.do",
      "hint": "Callback URL for Docusign"
    },
{
      "name": "credential.jwt_provider.jwt_claim_validation[0].value",
      "label": "Issuer (iss) Claim value",
      "type": "text",
      "hint": "The integrator key (also known as client ID) of the
application"
    },
{
      "name": "credential.jwt_provider.jwt_claim_validation[1].value",
      "label": "Subject (sub) Claim value",
      "type": "text",
      "hint": "The user ID of the user to be impersonated"
    },
{
      "name": "credential.jwt_provider.jwt_claim_validation[2].value",
      "label": "Audience (aud) Claim value",
      "type": "text",
      "defaultValue": "account-d.docusign.com",
      "hint": "The URI of the authentication service instance to be used
e.g. account.docusign.com"
    },
    {
      "name": "credential.jwt_provider.jwt_keystore_aliases.kid",
      "label": "Key ID (kid)",
      "type": "text",
```

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

```
      "hint": "Indicates which key was used to secure the JWS"
    },
    {
      "name":
 "credential.jwt_provider.jwt_keystore_aliases.signing_keystore",
      "label": "Key Store",
      "type": "file"
    }
  ]
}
```

Script de pós-processamento

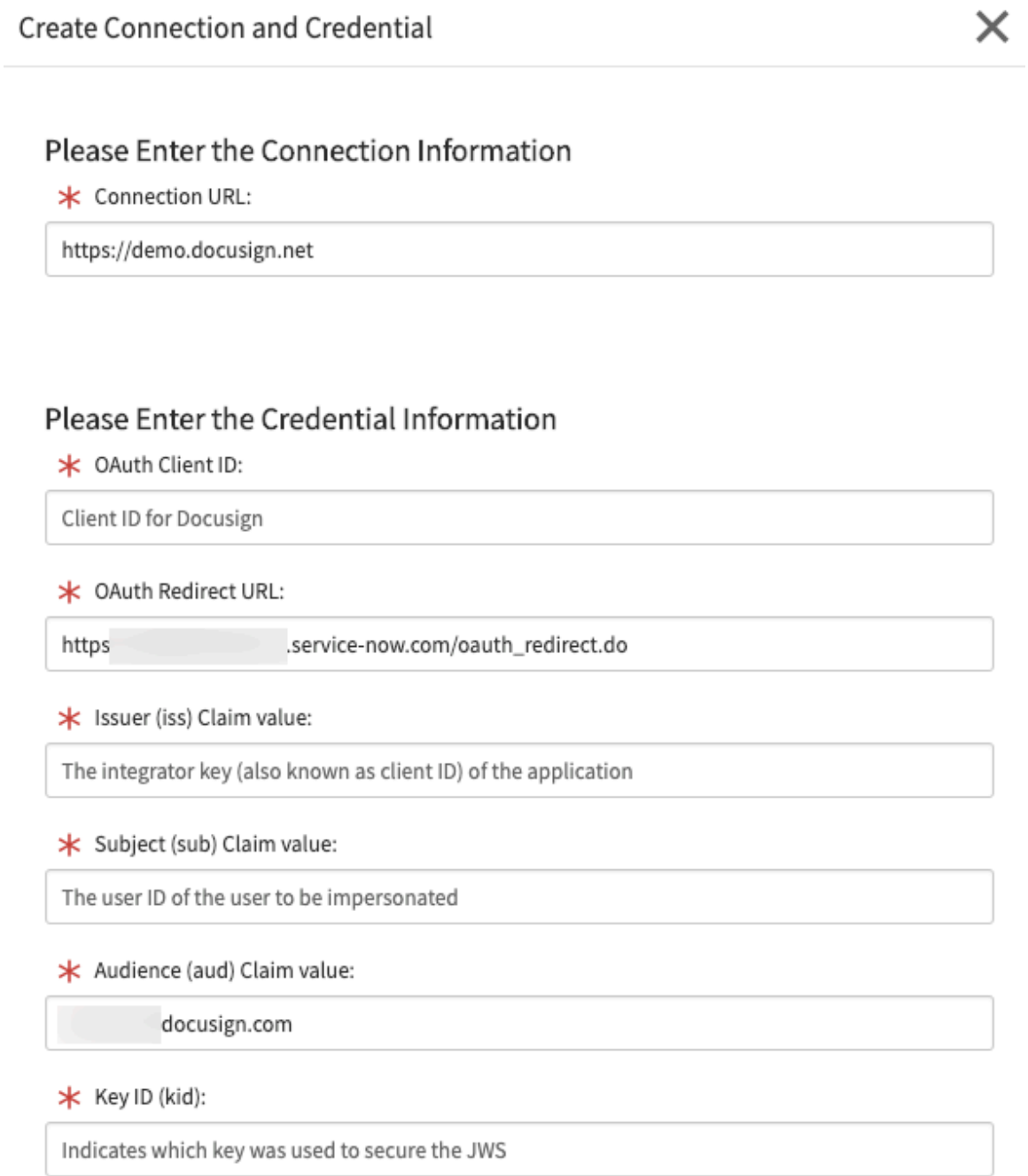
O script de pós-processamento a seguir mapeia a entrada do usuário para campos na tabela sn_docusign_spoke_accounts.

```
(function execute(aliasId, connectionSysId, jsonDefaultData,
 jsonDynamicData) {
 var jsonDynamicDataP = JSON.parse(jsonDynamicData);
 var accountGR = new GlideRecord("sn_docusign_spoke_accounts");
    accountGR.setValue("account_name",
 jsonDynamicDataP["additional.docusign_account_name"]);
    accountGR.setValue("alias", aliasId);
    accountGR.setValue("email",
 jsonDynamicDataP["additional.docusign_account_email"]);
    accountGR.setValue("id",
 jsonDynamicDataP["additional.docusign_account_id"]);
    accountGR.insert();
})(aliasId, connectionSysId, jsonDefaultData, jsonDynamicData);
```

Formulário resultante de configuração de conexão e credencial Docusign

Quando o usuário navegar até o Alias de conexão e credencial Docusign associado e selecionar **Criar nova conexão e credencial**, aparecerá o seguinte diálogo.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Crie um modelo de configuração

Crie um modelo que define as entradas necessárias para configurar um spoke. Defina pares de chave-valor estáticos para criar registros e defina valores que se aplicam a cada integração. Defina pares de chave-valor dinâmicos para coletar entrada do usuário e defina valores de campos que podem variar. Usando este modelo, os administradores e designers de fluxo podem configurar o spoke a partir de um único formulário.

Antes de Iniciar
Função necessária: administrador

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegue até **Todos** > **IntegrationHub** > **Conexões e credenciais** > **Modelos de configuração**.
2. Selecione **Novo**.
3. Selecione o tipo de modelo de configuração que deseja criar.

Tipo de configuração	Descrição
Conexão HTTP com tipo de concessão de Código de Autorização OAuth	Cria um modelo para registrar o sistema de terceiros como um provedor OAuth usando um código de autorização.
Conexão HTTP com tipo de concessão de Portador JWT OAuth	Cria um modelo para registrar o sistema de terceiros como um provedor OAuth usando um token da web JSON.
OAuth via HTTP com tipo de concessão de Credenciais do cliente	Cria um modelo para integração a uma aplicação de terceiros por meio da autenticação OAuth 2.0 que usa o tipo de concessão de credenciais do cliente.
Conexão HTTP com tipo de concessão de Credenciais de cliente OAuth (armazenamento externo)	Cria um modelo que permite o envio de solicitações de tokens OAuth que compreendem credenciais do cliente armazenadas por um armazenamento externo para um servidor OAuth por meio do MID Server.
Conexão HTTP com Credencial de Autenticação Básica	Cria um modelo para integração com o sistema de terceiros usando autenticação básica.
Conexão HTTP com Credencial de Chave de API	Cria um modelo para integração com o sistema de terceiros usando uma chave de API.
Outra Configuração	Cria um modelo em branco, permitindo que você configure um modelo para autenticação personalizada.

4. No campo **Nome**, adicione um nome para identificar o modelo.
5. No campo **Modelo de dados padrão**, faça as mudanças necessárias.

   Este campo define informações estáticas que se aplicam a todas as integrações. Por exemplo, é possível definir a API e o URL do token se o valor se aplicar a cada integração.

   Estes objetos no modelo de dados padrão são necessários:

   - `credencial`: cria um registro de credencial com os campos obrigatórios.
   - `conexão`: cria um registro de conexão com os campos obrigatórios. Acesse os atributos de conexão que usam o objeto secundário `extended_attributes`. Por exemplo:

```
"connection": {
            "extended_attributes": {
                "api_version": "v1"

             },
```

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

```
        "connection_url": "https://<provider-domain-name>.com",
        "name": "Spoke Connection",
        "table": "http_connection"
    }
```

É possível usar o objeto `additional` para configurar os dados para uma tabela personalizada e usar o script de pós-processamento para inserir os dados na tabela.

Nota: No modelo de dados padrão para o tipo de concessão do Código de autorização OAuth, os valores para o `oauth_entity_profile_scope` e as chave `oauth_entity_scope` devem corresponder. No exemplo a seguir, ambas as chaves possuem o valor `Ler e-mail do usuário`.

```
"oauth_entity_profile": [
        {
          "grant_type": "authorization_code",
          "name": "<provider-name> Profile",
          "default": true,
          "oauth_entity_profile_scope": [
            "Read user's email"
          ]
        }
      ],
      "code_challenge_method": "S256",
      "type": "consumer",
      "oauth_entity_scope": [
        {
          "oauth_entity_scope": "Read user's email",
          "name": "email"
        }
      ],
```

6. No campo **Esquema de dados dinâmicos**, faça quaisquer mudanças necessárias.

   Este campo Define as informações que o usuário deve preencher para configurar a integração. Por exemplo, você pode adicionar pares de chave-valor de nome de usuário e senha para coletar valores definidos pelo usuário.

   Os campos no esquema de dados dinâmicos incluem estas propriedades:

   - `nome`: o campo para o qual mapeia a entrada do usuário. Por exemplo, para mapear a entrada do usuário para o campo URL de Conexão no registro Conexão, insira `connection.connection_url`.
   - `rótulo`: o rótulo do campo que o usuário vê ao preencher o modelo.
   - `tipo`: o tipo de campo. Certifique-se de que este tipo de dados corresponda ao tipo de dados do campo para o qual você está mapeando o valor.
   - `defaultValue`: opcional. O valor padrão do campo. Se nenhum padrão for fornecido, será exibida a dica.
   - `dica`: opcional. Texto de dica a ser exibido quando não há valor padrão.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Se estiver configurando um modelo para a autenticação do tipo de concessão do Portador OAuth JWT, talvez queira a entrada do usuário para um único par chave-valor na matriz `jwt_claim_validation`. É possível se referir a um único par chave-valor no esquema de dados dinâmicos, consultando seu índice na matriz. Por exemplo, seu modelo de dados padrão pode incluir este snippet.

```
"jwt_claim_validation" : [ {
        "name" : "iss",
        "is_standard" : true,
        "data_type" : "string",
        "value":"<docusign-iss-claim>"
      }, {
        "name" : "sub",
        "is_standard" : true,
        "data_type" : "string",
        "value":"<docusign-sub-claim>"
      }, {
        "name" : "aud",
        "is_standard" : true,
        "data_type" : "string",
        "value":"<docusign-aud-claim>"
      }, {
        "name" : "scope",
        "is_standard" : false,
        "data_type" : "string",
        "value" : "signature impersonation"
      } ],
```

Consulte o par chave-valor `iss` usando o índice baseado em zero do item: `credential.jwt_provider.jwt_claim_validation[0].value`.

7. Opcional: No campo **Script de pós-processamento**, adicione um script que c Cria registros adicionais necessários para a integração. Por exemplo, se o seu spoke incluir tabelas personalizadas, você poderá criar registros nessas tabelas com base na entrada do usuário no modelo de configuração. Este script é executado depois que os registros de conexão e de credencial são criados.
   O script de pós-processamento tem acesso a esses objetos globais.

Objeto global	Descrição
aliasId	Sys_id do registro de alias da tabela Alias de conexão e credencial [sys_alias].
connectionSysId	Sys_id do registro de conexão criado pelo modelo.
jsonDefaultData	Conteúdo JSON do campo **Modelo de dados padrão** no formato de Cadeia de caracteres.
jsonDynamicData	Conteúdo JSON do campo **Modelo de dados dinâmicos** no formato de Cadeia de caracteres.

8. No campo **Pré-editar Script**, adicione um script que preenche previamente os campos adicionais ao editar uma conexão.

   Este script retorna uma matriz de objetos. Cada objeto tem um par de nome-valor para preencher os campos adicionais. Por exemplo, se a conexão precisar de campos

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

que estão na tabela personalizada, será possível mapear esses campos para a tabela personalizada.

O **Pré-editar script** tem acesso aos seguintes objetos globais:

Objeto global	Descrição
aliasId	Sys_id do registro de alias da tabela Alias de conexão e credencial [sys_alias].
connectionSysId	Sys_id do registro de conexão criado pelo modelo.
jsonDefaultData	Conteúdo JSON do campo **Modelo de dados padrão** no formato de Cadeia de caracteres.
jsonDynamicData	Conteúdo JSON do campo **Modelo de dados dinâmicos** no formato de Cadeia de caracteres.

Cada objeto no script tem as seguintes propriedades:

- `nome`: nome do campo personalizado para especificar o valor na conexão.
- `valor`: valor que você deseja mapear para preencher o campo personalizado. É possível mapear o campo usando uma função, variável ou o codificando.

Os seguintes tipos de dados são suportados para os campos:

Tipos de dados suportados para os campos

Tipo	Descrição
Texto	Valor da cadeia de caracteres.
Booleano	Caixa de seleção. A seleção indica o valor verdadeiro e a desmarcação indica o valor falso.
Número	Valor numérico.
Data	Valor de data no formato aaaa-mm-dd. Também é possível usar o objeto GlideDate.
Opção	Lista de opções válidas definidas no campo **Esquema de dados dinâmicos**.
Referência	GlideRecord válido.
Grupo de botões de rádio	Grupos que contêm um conjunto diferente de campos. Esses grupos estão disponíveis como uma opção em uma lista suspensa quando você editar uma conexão. Os campos em cada grupo aparecem quando você seleciona o grupo necessário na lista suspensa. Por exemplo, considere a seguinte estrutura do grupo de rádios definido no campo **Esquema de dados dinâmicos**: `{ "name": "radio_groups", "label": "Radio Groups", "type": "radio", "groups": [{ "name": "radio_group1", "label": "Radio Group 1", "fields": [{`

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tipo	Descrição

	<pre>"name": "radio_field1",
	"label": "Radio Field 1",
	"type": "text",
	"defaultValue": "efgh",
	"mandatory": true
	}]
	}, {
	"name": "radio_group2",
	"label": "Radio Group 2",
	"fields": [{
	"name": "radio_field2",
	"label": "Radio Field 2",
	"type": "text",
	"defaultValue": "abcd",
	"mandatory": true
	}],
	"default_group": true
	}</pre> Para este exemplo, é possível usar o seguinte snippet de código para entender como os grupos de rádios são usados no script usando a referência com pontos: <pre>{
	name:
	"radio_field.first_radio_group.radio_field1",
	value: "radio field 1"
	}, {
	name:
	"radio_field.second_radio_group.radio_field 2",
	value: "radio field 2"
	}, {
	name: “radio_groups”,
	value:
	gr.getValue(‘radio_groups’)
	}</pre> Para obter mais informações sobre como usar a referência com pontos, consulte Referência com pontos.

Dica: Se os valores preenchidos previamente não estiverem aparecendo nos campos ao editar uma conexão, navegue até **Diagnóstico do sistema** > **Depuração da sessão** > **Log de depuração** para diagnosticar o problema.

9. Adicione o modelo a um alias de conexão e credencial.

a. Navegue até **IntegrationHub** > **Conexões e credenciais** > **Aliases de conexão e credenciais**.

b. Abra o registro de alias do spoke.

c. No campo **Modelo de configuração**, clique no ícone de pesquisa.

d. Selecione o modelo que você criou na lista.

e. Clique em **Atualizar**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resultados
Quando o usuário navegar até o alias associado de Conexão e credenciais e selecionar **Criar nova conexão e credencial**, aparecerá um diálogo para coletar sua entrada. Se você criou um modelo para o tipo de concessão do Código de autorização OAuth, também é possível recuperar um token OAuth a partir deste diálogo.

O que Fazer Depois
Teste o modelo navegando até o alias associado de Conexão e credencial e selecionando **Criar nova conexão e credencial**. Verifique se a caixa de diálogo coleta os dados esperados e cria os registros necessários no sistema.

Introdução às conexões

Use a tabela de conexões para configurar uma conexão Basic, JMS, JDBC ou HTTP(s) a um host de destino.

Tabela de Conexão

A tabela de conexão (sys_connection) é a tabela base para todas as tabelas de conexão. É possível configurar conexões para os seguintes protocolos:

- Conexão Básica para PowerShell e SSH
- JDBC
- JMS
- HTTP(s)

A tabela de conexão faz referência à tabela de alias de conexão, que acopla o alias de conexão às informações de conexão. Cada conexão registra as seguintes informações:

Propriedades de conexão base

Campo	Descrição
Nome	Nome da conexão. Este campo deve ser exclusivo na tabela.
Credencial	Especifique a credencial a ser usada com esta conexão. Isso é opcional.
Alias de conexão	O alias de conexão resolve sua conexão e credenciais no tempo de execução. Somente uma conexão está ativa por alias de conexão de cada vez.
Ativo	Marque para tornar a conexão atual ativa.
Domínio	Domínio ao qual a conexão pertence.

A credencial é exclusiva nas conexões ativas, se não estiver vazia.

Upgrade de informações de conexão

- As tabelas de conexão JDBC [jdbc_connection] e conexão JMS [orch_jms_ds] são tabelas de conexão Orquestração existentes que agora se estendem da tabela de Conexão [sys_connection]. As tabelas originalmente estendidas de sys_metadata. Os dados relacionados a sys_metadata são removidos.
- As tabelas se movem do plug-in do tempo de execução Orquestração [com.snc.runbook_automation.runtime] para o plug-in Credenciais e conexões.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- O processo de upgrade obtém informações de conexão JDBC e JMS e cria aliases de conexão correspondentes e atribui o alias à sua conexão correspondente.
- Mudanças no nome do campo JDBC:
  - O servidor JDBC foi renomeado para host
  - A porta do banco de dados foi renomeada para porta
  - Os dados do servidor JDBC e do banco de dados migram para o host e a porta durante o upgrade

Crie uma conexão básica para PowerShell e SSH

Configure as informações de conexão a serem usadas com uma atividade personalizada ou ação que use o protocolo PowerShell ou Secure Shell (SSH).

Antes de Iniciar

Função necessária: administrador ou connection_admin

Procedimento

1. Navegue até **Todos** > **Credenciais e conexões** > **Conexões**.
2. Clique em **Nova**.
3. Selecione **Conexão básica para PowerShell e SSH**.
4. Preencha o formulário.

Campo	Descrição
Nome	Nome exclusivo do registro de conexão.
Credencial	Selecione o registro de credencial usado para autorizar a conexão.
Alias de conexão	Selecione o registro de alias a ser associado a esta conexão. Usar um alias permite que você atualize o registro de conexão sem precisar reconfigurar nenhuma ação ou atividade que use o alias.
Host	Nome de domínio totalmente qualificado do host de destino em que o sistema executa a atividade ou ação. Por exemplo, host.domain.com.
Ativo	Selecione para tornar esta conexão ativa.
Domínio	Determina o domínio em que a atividade é executada. O Flow Designer não suporta a separação de domínio e ignora este campo.
Substituir porta padrão	Porta de destino usada pela conexão. Se você deixar este campo em branco, o sistema usará o valor de porta padrão.
Usar MID Server	Selecione para se conectar ao host de destino por meio de um MID Server. Se selecionado, defina os campos na seção Configuração avançada do MID Server. **Nota:** O PowerShell requer um MID Server.
Seleção de MID	Opção para selecionar o MID Server ou Cluster do MID específico.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	◦ **Seleção automática do MID Server**: seleciona o MID Server automaticamente. ◦ **MID Server específico**: usa o MID Server selecionado. ◦ **Cluster do MID específico**: usa o Cluster do MID selecionado. Este campo fica disponível quando **Usar MID Server** está marcado. **Nota:** Certifique-se de que o registro de conexão Integration Hub seja referenciado, não um registro de conexão Orquestração.
Recursos	Os recursos que MID Server deve oferecer suporte para serem qualificados para seleção. O sistema executa a ação ou atividade de um MID Server que oferece suporte aos recursos selecionados. Exibido somente se **Usar MID Server** estiver selecionado. Os recursos necessários determinam qual MID Server é selecionado no tempo de execução. Para saber mais sobre como um MID Server é selecionado durante o tempo de execução, consulte Seleção do MID Server. Este campo fica visível apenas quando **Seleção automática do MID Server** estiver selecionada na lista de Seleção MID.
Aplicação MID	A aplicação que MID Server deve oferecer suporte para ser qualificado para seleção. O sistema executa a ação de um(a) MID Server que oferece suporte à aplicação selecionada. Exibido somente se **Usar MID Server** estiver selecionado. Para saber mais sobre como um(a) MID Server é selecionado durante o tempo de execução, consulte Seleção do MID Server.
MID Server	MID Server específico no qual a etapa é executada. Este campo fica visível apenas quando **MID Server específico** for selecionado da lista de Seleção MID.
Cluster do MID	O Cluster do MID específico que você deseja usar. Este campo fica disponível quando **Usar Mid Server** está marcado e **Cluster de MID específico** estiver selecionado na lista Seleção de MID.

5. Clique em **Enviar**.

Criar uma conexão HTTP(s)

A conexão HTTP(s) fornece as informações que as atividades ou ações HTTP(s) personalizadas usam para se conectar.

Antes de Iniciar

Função necessária: connection_admin

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Credenciais e conexões** > **Conexões**, clique em **Nova** e selecione **Conexão HTTP(s)**.
2. Adicione as seguintes informações de conexão e clique em **Enviar**:

Campo	Descrição
Nome	Nome exclusivo desta conexão HTTP(s).
Credencial	Selecione o registro de credencial usado para autorizar a conexão.
Alias de conexão	Selecione o registro de alias a ser associado a esta conexão. Usar um alias permite que você atualize o registro de conexão sem precisar reconfigurar nenhuma ação ou atividade que use o alias.
Construtor de URL	Insira manualmente o URL de conexão ou use o sistema para construir o URL baseado em entradas. O padrão é desmarcado. Se verificado, o URL de conexão é calculado dos seguintes campos: ◦ Autenticação mútua — Marque a caixa, se a autenticação mútua for usada. ◦ Protocolo — se a autenticação mútua não for usada, insira o protocolo. O padrão é HTTPs. ◦ Perfil de protocolo — Se a autenticação mútua for usada, insira o perfil de protocolo de sys_protocol_profile. ◦ Host ◦ Porta ◦ Caminho base — Caminho da cadeia de caracteres de conexão. **Nota:** Se a autenticação mútua estiver marcada, o URL de conexão será criado: Protocolo + :// + host:port +URL. Se a autenticação mútua estiver desmarcada, a URL de conexão será criada desta forma: Perfil do protocolo + :// + host:porta +URL
URL de conexão	Se o construtor de URL estiver desmarcado, insira o URL de conexão neste campo. **Nota:** Se a autenticação mútua estiver marcada, o URL de conexão será criado: Protocolo + :// + host:port +URL. Se a autenticação mútua estiver desmarcada, o URL de conexão será criado: Perfil do protocolo + :// + host:port +URL
Ativo	Marque a caixa para tornar esta conexão ativa.
Domínio	Determine o domínio no qual a ação ou a atividade é executada.
Usar MID Server	Marque para usar um MID Server para esta ação ou atividade. Se selecionado, defina os campos na seção Configuração avançada do MID Server.
Seleção de MID	Opção para selecionar o MID Server ou Cluster do MID específico.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	◦ **Seleção automática do MID Server**: seleciona o MID Server automaticamente. ◦ **MID Server específico**: usa o MID Server selecionado. ◦ **Cluster do MID específico**: usa o Cluster do MID selecionado. Este campo fica disponível quando **Usar MID Server** está marcado. **Nota:** Certifique-se de que o registro de conexão Integration Hub seja referenciado, não um registro de conexão Orquestração.
Recursos	Os recursos que MID Server deve oferecer suporte para serem qualificados para seleção. O sistema executa a ação ou atividade de um MID Server que oferece suporte aos recursos selecionados. Exibido somente se **Usar MID Server** estiver selecionado. Os recursos necessários determinam qual MID Server é selecionado no tempo de execução. Para saber mais sobre como um MID Server é selecionado durante o tempo de execução, consulte Seleção do MID Server. Este campo fica visível apenas quando **Seleção automática do MID Server** estiver selecionada na lista de Seleção MID.
Aplicação MID	A aplicação que MID Server deve oferecer suporte para ser qualificado para seleção. O sistema executa a ação de um(a) MID Server que oferece suporte à aplicação selecionada. Exibido somente se **Usar MID Server** estiver selecionado. Para saber mais sobre como um(a) MID Server é selecionado durante o tempo de execução, consulte Seleção do MID Server.
MID Server	MID Server específico no qual a etapa é executada. Este campo fica visível apenas quando **MID Server específico** for selecionado da lista de Seleção MID.
Cluster do MID	O Cluster do MID específico que você deseja usar. Este campo fica disponível quando **Usar Mid Server** está marcado e **Cluster de MID específico** estiver selecionado na lista Seleção de MID.
Tempo limite de conexão	Número de milissegundos que o sistema espera por uma conexão de host bem-sucedida. Se uma conexão bem-sucedida não ocorrer durante esse tempo, a solicitação de conexão expirará. Deixe este campo em branco para usar o valor de tempo limite de conexão padrão do sistema.

3. Clique em **Enviar**.
   Você está pronto para criar uma atividade ou ação personalizada HTTP(s).

Criar uma conexão JDBC

A Conexão JDBC fornece as informações que as atividades ou ações personalizadas JDBC usam para se conectarem a vários bancos de dados de destino.

Antes de Iniciar

Você deve ter um arquivo JAR apropriado, seja ele fornecido com a instância ou um arquivo JAR personalizado.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: A instância ServiceNow fornece arquivos `mysql-connector-java-5.1.21.jar`, `sql-server-jdbc-4.0.jar`e `ojdbc6.jar` como parte da versão atual, que suporta bancos de dados MySQL, SQLServer e Oracle. Outros bancos de dados, como Sybase ou DB2 Universal, devem usar um arquivo JAR personalizado que deve ser carregado para a instância antes de definir a conexão JDBC.

Função necessária: connection_admin

Por Que e Quando Desempenhar Esta Tarefa

As credenciais JDBC são recuperadas separadamente pelo modelo de designer de atividades e suportam o armazenamento externo de credenciais, tal como CyberArk.

Procedimento

1. Navegue até **Todos** > **Credenciais e conexões** > **Conexões**, clique em **Nova** e selecione **Conexão JDBC**.
2. Preencha o formulário usando os campos da tabela.
   A seleção do banco de dados no campo **Formato** determina quais campos estão disponíveis.

Campos de conexão JDBC

Campo	Formato do banco de dados	Descrição
Nome	Todos	Nome exclusivo desta conexão JDBC. Por exemplo, você pode inserir **JDBC MySQLProd**.
Credencial	Todos	Adicione credenciais para o provedor JDBC.
Alias de conexão	Todos	Selecione o registro de alias a ser associado a esta conexão. Usar um alias permite que você atualize o registro de conexão sem precisar reconfigurar nenhuma ação ou atividade que use o alias.
Tempo limite da consulta	Todos	Tempo máximo decorrido em que a consulta JDBC pode ser executada sem uma resposta.
Tempo limite de conexão	Todos	Número de segundos que o sistema espera por uma conexão de JDBC bem-sucedida. Se uma conexão bem-sucedida não ocorrer durante esse tempo, a solicitação de conexão expirará. Deixe este campo em branco para usar o valor de tempo limite de conexão padrão do sistema.
Ativo	Todos	Marque a caixa para tornar esta uma conexão ativa.
Domínio	Todos	Domínio desta tabela. Por padrão, a tabela Conexão JDBC [jdbc_connection] é executada no domínio **global**.
Formato	Todos	Tipo de banco de dados para esta conexão. As opções padrão são: ◦ **MySQL** ◦ **Oracle** ◦ **SQLServer** ◦ **Nenhum(a)**

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Formato do banco de dados	Descrição
		É possível adicionar **Sybase** ou **DB2 Universal** à lista de seleção carregando o arquivo JAR do driver JDBC apropriado na instância. O Orquestração reconhece automaticamente esses drivers quando são carregados no sistema e os adiciona a esta lista.
Host	Oracle, MySQL, SQLServer	Nome do host ou endereço IP do servidor do banco de dados.
Oracle sid	Oracle	O identificador do site do banco de dados Oracle. O valor padrão é **orcl**.
Porta Oracle	Oracle	Porta que o banco de dados Oracle está usando. O valor padrão é **1521**.
Nome do banco de dados	MySQL, SQLServer	Nome do banco de dados.
Porta	My SQL, SQLServer	Porta que o banco de dados selecionado está usando.
Nome da instância	SQLServer	Nome da instância do SQLServer selecionado
URL de Conexão	Todos	URL que o MID Server usa para se conectar ao banco de dados especificado. O URL é criado automaticamente quando você salva o formulário e é somente leitura para os bancos de dados padrão. **Nota:** Se o formato selecionado não for um dos bancos de dados padrão, você deve criar o URL de conexão manualmente para que o MID Server saiba como criar a conexão.
Driver JDBC	Nenhum, DB2 Universal, Sybase	O driver JDBC a ser usado para esta conexão quando não for um banco de dados padrão. **Nota:** Se você adicionar um banco de dados Sybase ou DB2 Universal, deve inserir o nome do driver neste campo e carregar o arquivo do driver JAR para a instância.
Usar MID Server	Todos	Marque para usar um MID Server para esta ação ou atividade. Se selecionado, defina os campos na seção Configuração avançada do MID Server.
Seleção de MID	Todos	Opção para selecionar o MID Server ou Cluster do MID específico. ◦ **Seleção automática do MID Server**: seleciona o MID Server automaticamente. ◦ **MID Server específico**: usa o MID Server selecionado. ◦ **Cluster do MID específico**: usa o Cluster do MID selecionado.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Formato do banco de dados	Descrição
		Este campo fica disponível quando **Usar MID Server** está marcado. **Nota:** Certifique-se de que o registro de conexão Integration Hub seja referenciado, não um registro de conexão Orquestração.
Recursos	Todos	Os recursos que MID Server deve oferecer suporte para serem qualificados para seleção. O sistema executa a ação ou atividade de um MID Server que oferece suporte aos recursos selecionados. Exibido somente se **Usar MID Server** estiver selecionado. Os recursos necessários determinam qual MID Server é selecionado no tempo de execução. Para saber mais sobre como um MID Server é selecionado durante o tempo de execução, consulte Seleção do MID Server. Este campo fica visível apenas quando **Seleção automática do MID Server** estiver selecionada na lista de Seleção MID.
Aplicação MID	Todos	A aplicação que MID Server deve oferecer suporte para ser qualificado para seleção. O sistema executa a ação de um(a) MID Server que oferece suporte à aplicação selecionada. Exibido somente se **Usar MID Server** estiver selecionado. Para saber mais sobre como um(a) MID Server é selecionado durante o tempo de execução, consulte Seleção do MID Server.
MID Server	Todos	MID Server específico no qual a etapa é executada. Este campo fica visível apenas quando **MID Server específico** for selecionado da lista de Seleção MID.
Cluster do MID	Todos	O Cluster do MID específico que você deseja usar. Este campo fica disponível quando **Usar Mid Server** está marcado e **Cluster de MID específico** estiver selecionado na lista Seleção de MID.

3. Clique em **Enviar**.

Informações relacionadas

Credenciais JDBC

Crie uma conexão JMS

Configure seu sistema para usar JMS (Java Messaging Service) com uma ação ou atividade JMS personalizada.

Antes de Iniciar

Função necessária: connection_admin

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

O MID Server deve ter connection factories JMS corretos para a sua organização. Configure esses valores na propriedade *mid.property.jms.command.allowed_factory_names*, encontrada em **MID Server** > **Propriedades**. Os valores padrão para esta propriedade podem ser alterados para qualquer valor ou lista de valores separada por vírgula divulgada pelo provedor JMS de terceiros.

Procedimento

1. Navegue até **Credenciais e conexões** > **Conexões**.
2. Clique em **Novo**, selecione **Conexão JMS**, preencha o formulário e, em seguida, clique em **Enviar**.

Opção	Descrição
Nome	Nome exclusivo desta connection factory.
Credencial	Adicione credenciais para o provedor JMS.
Alias de conexão	Selecione o registro de alias a ser associado a esta conexão. Usar um alias permite que você atualize o registro de conexão sem precisar reconfigurar nenhuma ação ou atividade que use o alias.
Context Factory inicial	Nome da classe JNDI que é usada para criar o InitialContext. **Nota:** Por exemplo, para conectar-se ao ActiveMQ V5.10 (JMS Provider), o valor é `org.apache.activemq.jndi.ActiveMQInitialContextFactory`.
URL do Provedor	Local da instalação do provedor JMS em execução. **Nota:** Por exemplo, para conectar-se ao ActiveMQ V5.1: `tcp://ipAddressOrHostName:61616`.
Ativo	Marque a caixa para tornar esta uma conexão ativa.
Domínio	Determine o domínio no qual a ação ou a atividade é executada.
Usar MID Server	Marque para usar um MID Server para esta ação ou atividade. Se selecionado, defina os campos na seção Configuração avançada do MID Server.
Seleção de MID	Opção para selecionar o MID Server ou Cluster do MID específico.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	◦ **Seleção automática do MID Server**: seleciona o MID Server automaticamente. ◦ **MID Server específico**: usa o MID Server selecionado. ◦ **Cluster do MID específico**: usa o Cluster do MID selecionado. Este campo fica disponível quando **Usar MID Server** está marcado.
Cluster do MID	O Cluster do MID específico que você deseja usar. Este campo fica disponível quando **Usar Mid Server** está marcado e **Cluster de MID específico** estiver selecionado na lista Seleção de MID.
Recursos	Os recursos que MID Server deve oferecer suporte para serem qualificados para seleção. O sistema executa a ação ou atividade de um MID Server que oferece suporte aos recursos selecionados. Exibido somente se **Usar MID Server** estiver selecionado. Para saber mais sobre como um(a) MID Server é selecionado durante o tempo de exe-
Aplicação MID	A aplicação que MID Server deve oferecer suporte para ser qualificado para seleção. O sistema executa a ação de um(a) MID Server que oferece suporte à aplicação selecionada. Exibido somente se **Usar MID Server** estiver selecionado. Para saber mais sobre como um(a) MID Server é selecionado durante o tempo de exe-

3. Navegue até **Conexões e credenciais** > **Credenciais**.
4. Clique em **Nova**, selecione **Credenciais JMS** e, em seguida, forneça o nome do usuário e a senha que o MID deve usar para se comunicar com o provedor JMS.
   Para obter mais informações, consulte Credenciais JMS.
5. Clique em **Enviar**.
   Você está pronto para criar uma atividade ou ação JMS personalizada.

Crie atributos de conexão para IntegrationHub

Defina variáveis específicas de conexão que você pode usar em Integration Hub etapas de integração.

Antes de Iniciar

Função necessária:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- A função de administrador é necessária para criar atributos de conexão.
- A função de administrador ou connection_admin é necessária para atribuir os valores de atributo.
- A função de administrador ou action_designer é necessária para usar atributos em uma ação personalizada.

Os atributos de conexão são usados apenas por etapas de integração, que precisam de uma assinatura para Integration Hub. Para obter mais informações sobre a ativação de Integration Hub, consulte Solicitar um plug-in Integration Hub.

Por Que e Quando Desempenhar Esta Tarefa

Ao usar uma etapa de integração, você deve estabelecer uma conexão com um sistema externo. Use um alias de conexão e credencial em vez de definir a conexão em linha. Um alias permite que você atualize os detalhes da conexão uma vez sem precisar reconfigurar todas as ações. Qualquer etapa de ação que usa um alias herda os atributos associados a ele. Flow Designer exibe atributos como cápsulas de dados que você pode arrastar para sua etapa de ação. Por exemplo, você pode criar um atributo de tamanho de página que se torna um parâmetro de consulta da etapa REST.

Para obter mais informações sobre como construir ações personalizadas Flow Designer, consulte Designer de ações.

Procedimento

1. Navegue até **Todos** > **Credenciais e conexões** > **Aliases de conexão e credencial**.
2. Crie ou selecione um registro de alias.
3. Na lista relacionada Atributos de conexão, clique em **Nova**.
4. Defina o rótulo do atributo e o tipo de campo.
   Para obter uma lista de tipos de campo, consulte tipos de campo.
5. Clique no link relacionado à exibição Avançada para definir as preferências do dicionário avançado para o atributo.
   Por exemplo, para criar um atributo com um valor dinamicamente calculado. Consulte Formulário de entrada de dicionário.
6. Clique em **Enviar**.
7. Defina os valores de atributo no registro de conexão.

   a. Navegue até **Credenciais e conexões** > **Conexões**.

   b. Crie ou selecione um registro de conexão com o mesmo tipo de conexão que o alias.

   c. No **Alias de conexão**, selecione o alias com atributos de conexão.

   d. Salve o registro.
   A guia Atributos é preenchida com os atributos de conexão definidos no registro do alias.

   e. Defina valores para os atributos.
   Se o alias tiver **Suportar várias conexões ativas** habilitado, será possível associar mais de um registro de conexão a um alias e definir os valores de atributo em cada registro de conexão. Se houver vários registros de conexão com valores de atributo para o mesmo alias, a conexão usada quando o fluxo é executado determina os valores de atributo.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por exemplo, suponha que você tenha uma ação que usa um alias com dois endpoints de conexão ativos: produção e teste. O atributo é resolvido para o valor definido pela conexão usada em tempo de execução.

8. Adicione o alias a uma etapa de integração em Designer de ações.
   a. Navegue até Flow Designer e crie ou selecione uma ação.
   b. Adicione uma etapa de integração à ação.
   c. Em Detalhes da conexão, adicione o alias para os quais você criou atributos.

   Os atributos de conexão associados ao alias são exibidos como cápsulas de dados no painel Dados.

   Nota: O sistema não rastreia mudanças em rótulos de atributo de conexão e tipos de dados depois de associar o alias a uma etapa. Para atualizar o rótulo do atributo de conexão ou o tipo de dados, exclua o alias da etapa e adicione-o novamente.

Introdução às credenciais

O MID Server usa as credenciais que você cria na tabela Credentials [discovery_credentials] para acessar os recursos da Descoberta, Orquestração, Mapeamento de serviços e Gestão de nuvem.

Como os MID Servers usam credenciais

Por padrão, os MID Servers do Windows usam as credenciais de login do serviço do MID Server na máquina do host para descobrir dispositivos Windows na rede. Você deve Configurar as credenciais de serviço Windows MID Server para que tenham pelo menos privilégios de administrador local. Para máquinas Linux e UNIX e dispositivos de rede, o MID Server usa as credenciais SSH e SNMP configuradas na instância em **Descoberta** > **Credenciais**.

MID Servers aos quais o Orquestração deve ter acesso para que as credenciais necessárias executem comandos nos computadores na rede, conforme especificado pelas Atividades do fluxo de trabalho. a Orquestração pode usar as mesmas credenciais de SSH e SNMP que Descoberta, mas possui duas credenciais adicionais projetadas para atividades do fluxo de trabalho específicas: Windows (para atividades do PowerShell) e VMware.

Criptografia e descriptografia

A plataforma armazena credenciais em um campo criptografado na tabela Credenciais [discovery_credentials]. Depois de inseridas, elas não podem ser exibidas.

Quando o MID Server solicita credenciais, o Now Platform descriptografa as credenciais usando o seguinte processo:

1. As credenciais são descriptografadas na instância com a chave fixa password2.
2. As credenciais são criptografadas novamente na instância com a chave pública do MID Server.
3. As credenciais são criptografadas no balanceador de carga com SSL.
4. As credenciais são descriptografadas no MID Server com SSL.
5. As credenciais são descriptografadas no MID Server com a chave privada do MID Server.

Nota: A plataforma não tem chaves de criptografia separadas para instâncias de vários locatários.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Pedido de credenciais

As credenciais podem ser atribuídas a um valor de pedido no Formulário de credenciais, que força a aplicação a tentar todas as credenciais à sua disposição em uma certa sequência. Se você não especificar um valor de pedido, a aplicação tentará as credenciais na tabela Credenciais [discovery_credential] aleatoriamente, até que encontre uma que funcione. Por exemplo, quando:

- a Orquestração tenta executar um comando em um servidor SSH, como uma máquina Linux ou UNIX.
- O Descoberta tenta consultar um dispositivo SNMP, tal como uma impressora, roteador ou no-break.

Depois de identificar as credenciais para um dispositivo, o Descoberta e a Orquestração criam uma afinidade entre as credenciais e o dispositivo que usa a tabela Afinidade de credencial `[dscy_credentials_affinity]`. Todas as descobertas subsequentes ou atividades da Orquestração tentam corresponder as credenciais nesta tabela a um dispositivo para o qual existe uma afinidade. Se as credenciais de um dispositivo forem alteradas, o Descoberta e a Orquestração tentarão todas as credenciais disponíveis novamente até criarem uma nova afinidade.

Nota: Se a Orquestração e o Descoberta estiverem instalados e o alias de credencial estiver habilitado, poderão existir várias afinidades. Nesse caso, a plataforma pesquisa as credenciais de cada afinidade e insere a credencial da afinidade com a ordem mais baixa no probe.

Solicitar credenciais é útil nas seguintes situações:

- A tabela de credenciais contém muitas credenciais, sendo algumas usadas com mais frequência do que outras. Por exemplo, a tabela contém 150 credenciais SSH e cinco delas são usadas para fazer login em 90% dos dispositivos. É uma prática recomendada configurar essas cinco credenciais com números de ordem baixa, o que as coloca no topo da lista de execução. Descoberta e a Orquestração funcionam mais rápido quando tentam essas credenciais comuns pela primeira vez. Após a primeira conexão bem-sucedida, o Now Platform sabe quais credenciais usar na próxima vez para cada dispositivo.
- O Now Platform tem segurança de login intensa. Por exemplo, configure as credenciais do banco de dados com um valor de ordem baixa se os servidores de banco de dados Solaris na rede fornecerem apenas três tentativas de login com falha antes de bloquear o MID Server.

Aliases de credencial

Os aliases de credencial ficam disponíveis para Descoberta e Orquestração.

Os aliases para Descoberta habilitam um administrador para:

- Empregue um comportamento de filtragem de credenciais com níveis configuráveis de conformidade.
- Atribua vários aliases de credencial a uma programação da Descoberta.
- Impede a criação de afinidades de credencial que usam credenciais confidenciais ou inadequadas. Para saber mais, consulte Afinidades de credenciais.

Os aliases para Orquestração permitem que os criadores de fluxo de trabalho:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Atribuam credenciais individuais a qualquer atividade em um fluxo de trabalho da Orquestração
- Atribuam credenciais individuais a qualquer ação no Flow Designer
- Atribuam credenciais diferentes para cada ocorrência do mesmo tipo de atividade em um fluxo de trabalho da Orquestração.
- Atribuam credenciais diferentes a cada ocorrência da mesma ação no fluxo do designer.

Armazenamentos de credenciais externas

Se não quiser que as credenciais sejam armazenadas em sua instância, use repositórios de credenciais externas. Os armazenamentos de credenciais externas salvam as credenciais em um site externo que sua instância pode acessar. CyberArk é o único armazenamento externo de credenciais suportado. No entanto, outros armazenamentos externos podem ser configurados usando a API da ServiceNow.

Crie um alias de Conexão e Credenciais

Defina um alias para rotular uma credencial ou registro de conexão.

Antes de Iniciar

Função necessária:

- A função de administrador é necessária para criar um alias.
- As funções credential_admin e connection_admin têm acesso de leitura ao registro do alias.

Por Que e Quando Desempenhar Esta Tarefa

O alias Conexão e credencial define um alias que rotula um registro de conexão ou credencial. O alias contém esses campos.

Procedimento

1. Navegue até **Todos** > **Conexões e credenciais** > **Aliases de conexão e credencial**.
2. Clique em **Nova**.
3. Preencha os campos no formulário.

Aliases de conexão e credencial

Campo	Descrição
Nome	Nome do alias. Um alias só pode conter caracteres alfa, número e sublinhado. Durante um upgrade, o marcador no registro de credencial migra para um alias de credencial e conexão. Se o marcador de credencial contiver caracteres especiais diferentes de alfabetos, números e sublinhados, isso preserva o nome do marcador após um upgrade. Ainda é possível usar este alias migrado, mas não é possível atualizar o alias até que mude o nome para atender a restrições de nomenclatura.
ID	Identificador exclusivo para o alias de conexões e credenciais, com base no formato `scope_name.alias_name`.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	◦ Se o escopo for Global, o ID será o nome do alias. Por exemplo, se você criar um alias do Workday no escopo global, ele definirá o ID para `workday`. ◦ Se você criar um alias workday no escopo da aplicação de RH, ele definirá o ID para `x_hr_app.workday`.
Tipo	Selecione **Credencial** ou **Conexão e credencial**. O padrão é Conexão e credencial.
Aplicação	Escopo da aplicação em relação ao qual o alias de conexão e credenciais é atribuído. O escopo da sessão atual selecionado pela última vez no seletor de aplicações é exibido. ◦ Por exemplo, **Global** aparece se for o escopo atual desta sessão. ◦ É possível mudar o escopo no seletor de aplicação antes de criar um alias. Para saber mais sobre escopos de aplicação e como selecioná-los, consulte: ▪ Escopo da aplicação ▪ Selecione uma aplicação no seletor de aplicações
Tipo de conexão	Nome do tipo de conexão, seja Basic, HTTP, JDBC, JMS ou Kafka. O padrão é HTTP.
Suporte a várias conexões ativas	Designador que indica se o alias suporta várias conexões ativas. Adicione conexões usando a tabela Conexões e as associe ao alias usando a lista relacionada às Conexões.
Política de nova tentativa padrão	Tente novamente a política para o alias. Para obter mais informações, consulte Política de nova tentativa.
Modelo de configuração	Modelo de configuração a ser usado para criar um registro de credencial e de conexão.

4. Clique em **Salvar**.
   Aparece a lista relacionada a Conexões e Atributos de conexão.

Lista relacionada	Descrição
Conexões	Registros de conexão relacionados associados a este alias. Depois de criar o alias, é possível definir registros de conexão e associá-los ao alias. Se **Suportar múltiplas conexões ativas** estiver selecionado, será possível associar mais de uma conexão a um alias.
Atributos da conexão	Atributos para conexão. Defina dados específicos a uma conexão e use-os em uma etapa de integração Integration Hub. Para obter mais informações, consulte Crie atributos de conexão para IntegrationHub.
Aliases secundários	Aliases secundários associados ao alias primário. Depois de criar um alias de credencial e de conexão, é possível criar o alias secundário para configurar múltiplas conexões para a mesma integração de aplicação.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Lista relacionada	Descrição
Conexões	Registros de conexão relacionados associados a este alias. Depois de criar o alias, é possível definir registros de conexão e associá-los ao alias. Se **Suportar múltiplas conexões ativas** estiver selecionado, será possível associar mais de uma conexão a um alias.
Atributos da conexão	Atributos para conexão. Defina dados específicos a uma conexão e use-os em uma etapa de integração Integration Hub. Para obter mais informações, consulte Crie atributos de conexão para IntegrationHub.

5. Opcional: Se deseja criar uma nova credencial e conexão associadas ao seu alias de credencial, em *Related Links*, clique em **Criar nova conexão e credencial**.
   A conexão resultante e os registros de credencial são baseados em um modelo de configuração predefinido. Consulte modelos de configuração de credencial e conexão.
6. Opcional: Se deseja criar um alias secundário para seu alias de credencial e conexão, na lista relacionada**Aliases secundários**, selecione **Novo**.

   a. Insira um nome para o alias secundário e selecione **Enviar**.
      O alias secundário herda as propriedades do alias primário. Em seguida, é possível configurar um alias secundário para conter seu próprio conjunto de informações de conexão e credencial.

O que Fazer Depois

Crie um ou mais registros de conexão para associar aos aliases secundários ou ao alias. Para obter mais informações sobre a criação das conexões, consulte Introdução às conexões. Adicione atributos de conexão ao alias para disponibilizar metadados de conexão para fluxos em Flow Designer.

Como configurar a integração do OAuth por meio do MID Server

Crie um registro de conexão que permita o envio de uma solicitação de token OAuth a um servidor de terceiros por meio de um MID Server.

Antes de Iniciar

Confirme se você assinou o ServiceNow IntegrationHub Standard Pack Installer. Para obter mais informações, consulte https://www.servicenow.com/content/dam/servicenow-assets/public/en-us/doc-type/legal/snc-addendum-integrationhub.pdf.

Função necessária: administrador

Procedimento

Configure a conexão com um modelo de configuração.

a. Navegue até **Todos** > **IntegrationHub** > **Modelos de configuração**.

b. Selecione **Novo**.

c. Selecione **Conexão HTTP com tipo de concessão de Credenciais de cliente OAuth**.

d. Atualize o formulário conforme necessário.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por exemplo, é possível informar o escopo nos campos `oauth_entity_profile_scope` e `oauth_entity_scope` da seção "Modelo de dados padrão". Para aprender a criar um modelo de configuração, consulte Crie um modelo de configuração.

e. Selecione **Enviar**.
Você criou o modelo de configuração.

f. Navegue até **Todos** > **IntegrationHub** > **Aliases de conexão e credencial**.

g. Atualize o formulário.

Alias de conexão e credencial

Campo	Descrição
Nome	Nome do alias. Um alias só pode conter caracteres alfa, número e sublinhado. Durante um upgrade, o marcador no registro de credencial migra para um alias de credencial e conexão. Se o marcador de credencial contiver caracteres especiais diferentes de alfabetos, números e sublinhados, isso preserva o nome do marcador após um upgrade. Ainda é possível usar esse alias migrado, mas não é possível atualizá-lo até que você mude o nome para atender às restrições de nomenclatura.
Aplicação	Identificador exclusivo do alias de conexão e credencial, com base no formato `scope_name.alias_name`. ◦ Se o escopo for Global, o ID será o nome do alias. Por exemplo, se você criar um alias do Workday no escopo global, ele definirá o ID para `workday`. ◦ Se você criar um alias do workday no escopo do app de RH, ele definirá o ID como `x_hr_app.workday`.
Alias primário	Opção para selecionar o alias sob o qual você está criando esse alias de conexão e credencial. O alias de conexão e credencial que você está criando é um alias secundário. Um alias secundário é listado na guia **Aliases secundários**, na página do alias primário de conexão e credencial.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Tipo	Opção para indicar o tipo de alias que você está criando. Escolha dentre as seguintes opções. ◦ Credencial: alias que contém um registro de credencial. ◦ Conexão e credencial: alias que contém um registro de conexão e credencial. Essa opção é selecionada por padrão. Confirme se a opção "Conexão e credencial" está selecionada.
Suporte a várias conexões ativas	Designador que indica se o alias suporta várias conexões ativas. Adicione conexões usando a tabela Conexões e as associe ao alias usando a lista relacionada às Conexões.
Política de nova tentativa padrão	Tente novamente a política para o alias. Para obter mais informações, consulte Política de nova tentativa.
Modelo de configuração	Opção para selecionar o modelo de configuração com base no qual você está criando o alias de conexão e credencial. Selecione o modelo do tipo **Conexão HTTP com tipo de concessão de Credenciais de Cliente OAuth** que você criou.

h. Selecione **Enviar**.
Você criou o registro de alias de conexão e credencial.

i. Navegue até **Todos** > **IntegrationHub** > **Painel de conexões**.

j. No campo "Pesquisar todas as conexões", digite o nome do registro de alias de conexão e credencial que você criou.

k. No registro, selecione **Exibir detalhes**.

l. Selecione **Configurar**.

m. Preencha o formulário.

Registro de conexão

Campo	Descrição
Nome da conexão	Nome do registro de conexão. Não é possível atualizar o nome.
URL de Conexão	Opção para informar a URL que se conecta ao servidor de terceiros.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Usar MID	Opção para especificar que você deseja enviar solicitações de token OAuth por meio de um MID Server. **Importante:** Confirme se a opção está selecionada.
Seleção de MID	Opção para especificar se você deseja usar um MID Server específico, habilitar a seleção automática do MID Server ou usar um Cluster do MID. Escolha uma das opções a seguir. ◦ Selecionar automaticamente o MID Server ◦ MID Server específico ◦ Cluster do MID específico
MID Server	Opção para selecionar um MID Server. **Nota:** Essa opção aparecerá se você selecionar **MID Server específico** no campo "Seleção de MID".
Cluster do MID	Opção para selecionar um Cluster do MID. **Nota:** Essa opção aparecerá se você selecionar **Cluster do MID específico** no campo "Seleção de MID".
ID do cliente OAuth	Opção para especificar o ID do cliente.
Segredo do cliente OAuth	Opção para especificar o segredo do cliente.
Conectar-se ao servidor Auth via MID Server	Opção para especificar que a conexão entre a instância da ServiceNow e o servidor de autenticação ocorre por meio do MID Server. **Importante:** Confirme se a opção está selecionada.
URL do token Oauth	Opção para especificar a URL do token OAuth usada para solicitar tokens OAuth.

n. Selecione **Configurar e obter token do OAuth**.
O registro de conexão e credencial é criado.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Aliases de credencial da Descoberta

Os aliases de credencial para Descoberta permitem que um administrador use credenciais específicas nas agendas de Descoberta. É possível configurar comportamentos para seus aliases que determinam o quão estritamente o sistema impõe seu uso.

Sem aliases de credencial, as agendas de Descoberta podem acessar todas as credenciais definidas na instância. Este comportamento pode não ser desejável em algumas circunstâncias, especialmente para credenciais com privilégios elevados. Os aliases de credencial fornecem mais controle sobre quais credenciais uma programação da Descoberta tem permissão para usar e impede a exposição desnecessária de credenciais com privilégios elevados.

Como os aliases de credencial funcionam

Uma regra de negócio chamada *Inserir aliases de afinidade descoberta e cred* (anteriormente denominada *Inserir afinidade descoberta*) é executada quando um registro é inserido na fila do ECC. A regra de negócio anexa os aliases de credencial definidos na programação de Descoberta ao probe, de modo que o MID Server possa realizar a filtragem de credencial. A primeira tarefa do MID Server é criar a lista de credenciais a serem pesquisadas. Ela filtra as credenciais por afinidade e então por marcadores, se existir algum. As afinidades vão para a parte superior da lista e os marcadores correspondentes vão para a parte inferior da lista. O MID Server itera na lista até encontrar uma credencial que funcione. O MID Server cria uma afinidade para esta credencial.

Nota: As credenciais devem corresponder a todos os marcadores de credencial.

Se a regra de negócio determinar que existe uma afinidade para o dispositivo, a regra identificará o *credential_id* adequado a ser usado. Este é o *sys_id* do registro na tabela Credenciais `[discovery_credentials]`. Quando a plataforma encontrar uma afinidade com um valor de alias de credencial, definido como *credential_alias* na regra de negócio, a regra de negócio determinará se, ou não, a credencial referenciada pela afinidade possui o alias especificado. Em caso afirmativo, a regra de negócio seleciona o *credential_id* do alias e passa esse valor para o MID Server. Se a credencial não tiver o alias de credencial especificado, todas as outras afinidades existentes para o sistema de destino serão verificadas.

Crie um alias de credenciais da Descoberta

Crie o alias e adicione esse alias a uma credencial no registro de credencial. É possível adicionar uma credencial a vários aliases e adicionar várias credenciais a um único alias.

Antes de Iniciar

Função necessária: administrador, credential_admin (apenas acesso de leitura), connection_admin (apenas acesso de leitura)

Por Que e Quando Desempenhar Esta Tarefa

Uma programação da Descoberta usa apenas credenciais que estão contidas nos aliases definidos para essa programação.

Nota: Se um alias de credencial for definido para uma programação, ele ignorará qualquer afinidade de credencial anteriormente existente entre a credencial e o destino que é descoberto em uma programação que é configurada para usar esse alias de credencial.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

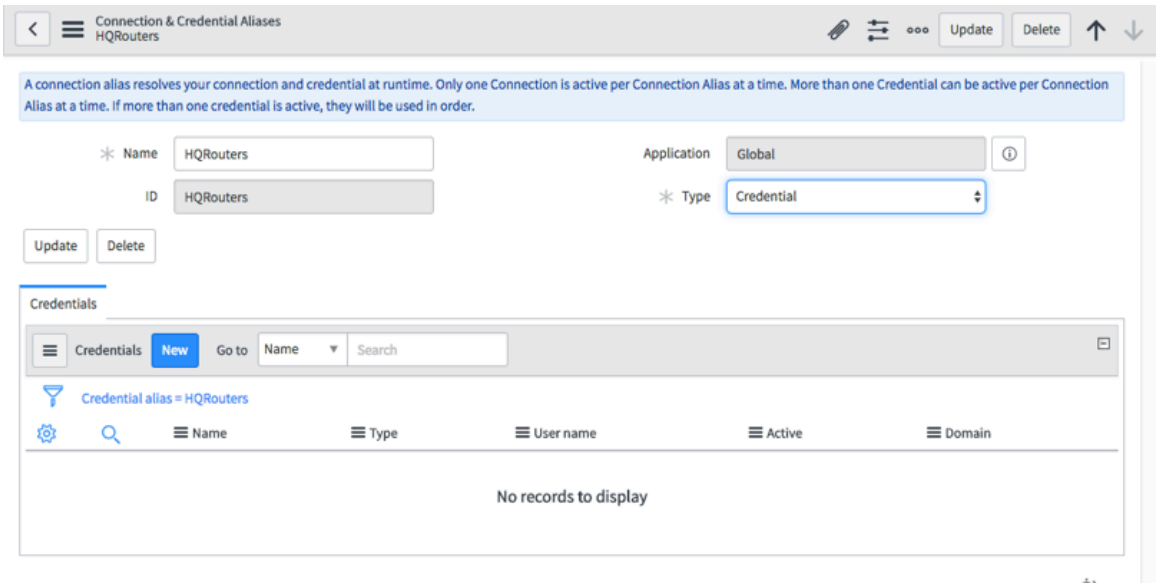
1. Crie um alias.

a. Navegue até **Conexões e credenciais** > **Aliases de conexão e credencial**.

b. Clique em **Novo**.

c. Insira um nome exclusivo para o alias e selecione **Credencial** para o **Tipo** de alias.

d. Clique em **Enviar**.
Aparece a lista relacionada de **Credenciais**. É possível adicionar novas credenciais para este alias nesta lista, mas não credenciais existentes.



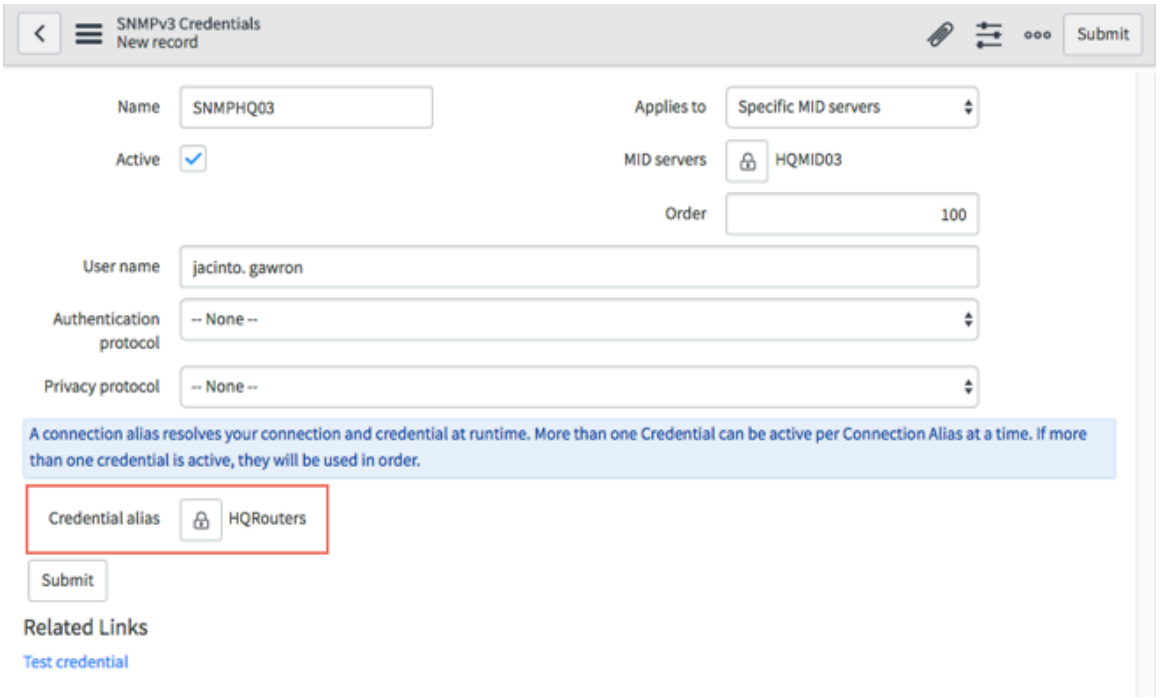
2. Configure uma credencial para o novo alias.

a. Navegue até **Conexões e credenciais** > **Credenciais**.

b. Selecione uma credencial existente da lista ou clique em **Novo** para criar uma nova credencial.

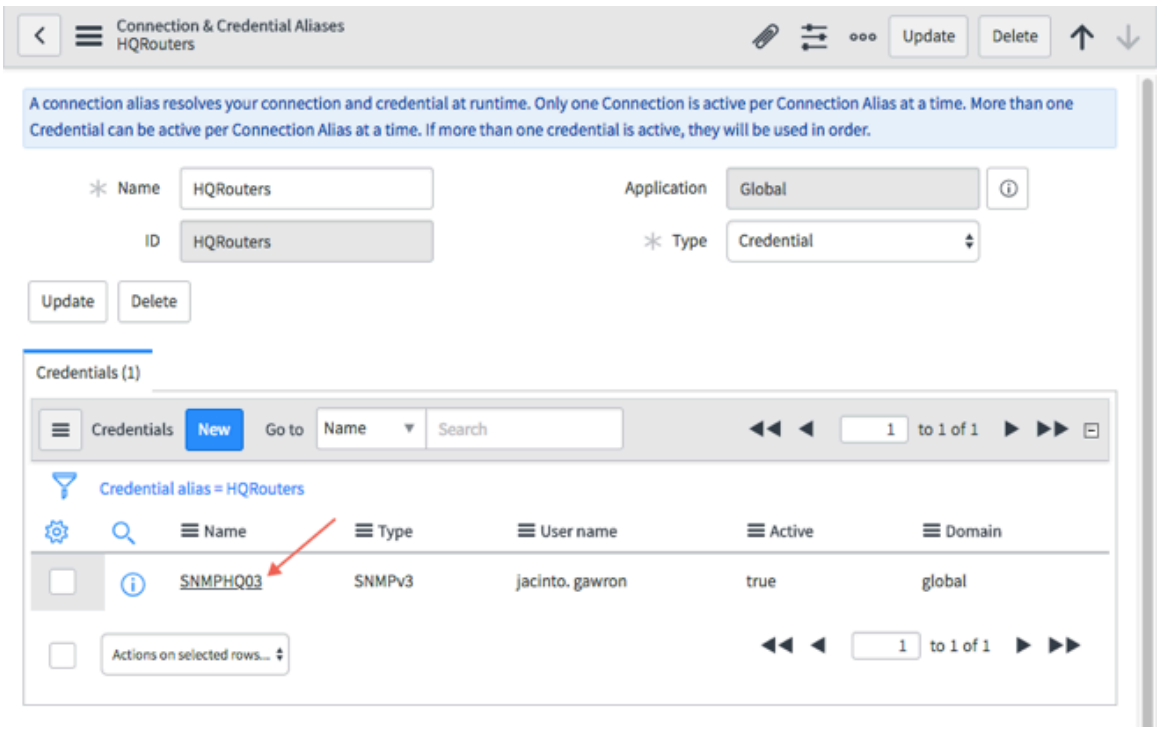
c. No registro de credencial, destrave o campo **Alias de credencial** e selecione o alias que você criou.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



d. Salve ou envie o registro.

3. Volte para **Conexões e credenciais** > **Aliases de conexão e credencial** e abra seu novo alias.
   A credencial que você anexou ao alias agora aparece na lista relacionada.



4. Para criar uma credencial adicional para este alias, clique em **Novo** na lista relacionada e selecione um tipo de credencial.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O nome do alias é preenchido previamente no campo **Alias de credencial** do registro de credencial.

5. Preencha os campos do formulário e envie o registro.

Aliases de credencial para atividades da Orquestração

O alias de credencial fornece ao administrador mais controle sobre as credenciais usadas nas atividades da Orquestração.

Isso é útil quando uma atividade requer credenciais específicas para executar uma tarefa. É possível usar um marcador de credencial para designar credenciais individuais a qualquer atividade em um fluxo de trabalho da Orquestração ou atribuir credenciais diferentes para cada ocorrência do mesmo tipo de atividade em um fluxo de trabalho da Orquestração.

O alias de credencial interage com a afinidade de credencial para determinar quais credenciais devem ser usadas para uma atividade da Orquestração.

Como funcionam os aliases de credencial

Uma regra de negócio denominada *Inserir afinidade Descoberta* (renomeada a partir de Inserir afinidade de credencial na versão Geneva) é executada quando um registro é inserido na Fila do ECC. Esta regra determina se existe uma afinidade de credencial para o dispositivo e identifica o *credential_id* apropriado (o *sys_id* do registro n tabela Credenciais `[discovery_credentials]`) a ser usado. Quando a plataforma encontra uma afinidade com um valor de alias de credencial definido (*credential_alias* na regra de negócio), a regra de negócio determina se a credencial referenciada pela afinidade possui o alias especificado. Em caso afirmativo, a regra de negócio seleciona o *credential_id* do alias de credencial e passa esse valor para o MID Server. Se a credencial não tiver o alias de credencial especificado, todas as outras afinidades existentes para o sistema de destino serão verificadas. Se nenhuma afinidade fizer referência a uma credencial marcada corretamente, o MID Server vai iterar por meio da tabela Credenciais *[discovery_credentials]* e seleciona a credencial com o marcador apropriado. O MID Server então cria uma nova afinidade para esta credencial.

Criar e testar suas credenciais

Crie e teste as credenciais que a Descoberta, o Mapeamento de serviços, Gestão de nuvem e Orquestração precisam para acessar o hardware e o software em sua rede.

Antes de Iniciar

Função necessária: administrador
Analise sua política de segurança e as opções com a equipe de segurança da sua organização.

Por Que e Quando Desempenhar Esta Tarefa

Esta tarefa contém procedimentos gerais para criar credenciais. Consulte a documentação do seu tipo de credencial para obter detalhes sobre campos e requisitos específicos.

Tipos de credenciais suportados

Credenciais de aplicativo	Credenciais de autenticação básica	Credenciais do servidor Chef
Credenciais CIM	Credenciais de acesso à nuvem	Credenciais de Infoblox
Credenciais JDBC	Credenciais JMS	Credenciais OAuth 2.0

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tipos de credenciais suportados

Credenciais do SAP	Credenciais de SNMP	Credenciais SSH
Credenciais do VMware	Credenciais do Windows	Credenciais do repositório de imagens do contêiner

Nota: Para melhorar a segurança, limite o escopo de credenciais a um MID Server específico ou programação para evitar credenciais desnecessárias.

Procedimento

1. Navegue até um destes módulos:
   - **Descoberta** > **Credenciais**
   - **Mapeamento de serviços** > **Credenciais**
   - **Orquestração** > **Credenciais**
2. Clique em **Nova**.
3. Na página Credenciais, clique em um link para o tipo de credencial e preencha o formulário.

   Consulte a documentação do tipo de credencial selecionado para obter detalhes.

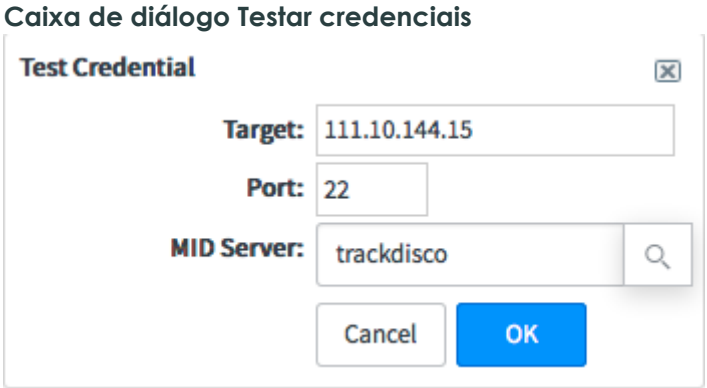
   É possível enviar um registro de credencial primeiro e, em seguida, testá-lo posteriormente ou testar a credencial imediatamente antes de salvá-lo.

   O teste de credencial é suportado para estes tipos de credencial:
   - Chaves privadas de SSH
   - Windows
   - SNMP v3
   - VMware
   - JDBC
   - JMS
4. Em **Links relacionados**, clique em **Testar credencial**.

   Nota: As credenciais são criptografadas em todos os momentos durante o teste.

5. Preencha os campos na caixa de diálogo Testar credencial.

Caixa de diálogo Testar credenciais



© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campos de teste de credencial

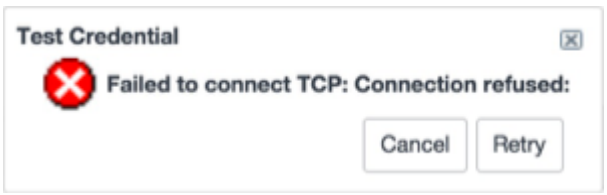
Campo	Descrição	Tipo de credencial
Destino	Host de destino no qual essas credenciais são executadas. Este valor deve ser um endereço IP para todos os tipos de credenciais, exceto VMware, que pode ser a URL do host. Não é possível direcionar nenhum MID Server. **Nota:** Para JMS, este é o URL do provedor. As informações neste URL informam ao JNDI como encontrar e acessar o Provedor JMS. Um valor de exemplo para conectar ao ActiveMQ V5.1, is `tcp://ipAddressOrHostName:61616`.	Todos
Porta	Porta no destino a ser usada para este teste. O sistema preenche previamente este campo com a porta padrão para o tipo de credencial selecionado.	Todos
MID Server	MID Server a ser usado para este teste. Você deve usar um Windows MID Server para testar as credenciais do Windows. Apenas MID Servers **Ativos** e **Validados** estão disponíveis.	Todos
Tipo DB	Tipo de banco de dados no qual essas credenciais serão testadas.	JDBC
Nome de BD	Nome do banco de dados no qual essas credenciais são testadas.	JDBC
Fábrica de Contexto Inicial	Nome da classe JNDI que é usada para criar o InitialContext. Usando esta **Fábrica de contexto inicial**, diversos objetos JMS, como JMS Connection, são criados. Por exemplo, para conectar-se ao ActiveMQ	JMS

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição	Tipo de credencial
	V5.10, (JMS Provider), o valor neste campo seria `org.apache.activemq.jndi.ActiveMQInitialContextFactory`	

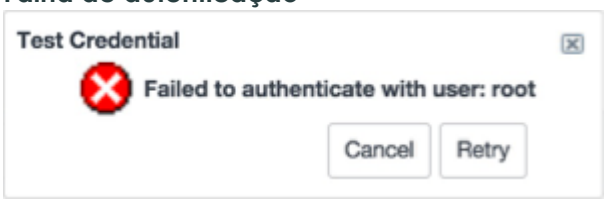
6. Clique em **OK** para iniciar o teste.
   Aparece um indicador, mostrando que o sistema está tentando entrar em contato com o destino usando as credenciais que você forneceu. Quando a instância se conecta ao destino, ela exibe uma mensagem de sucesso. Se a instância encontrar um problema com as entradas de teste fornecidas, ela exibirá a mensagem de erro apropriada. A seguir estão algumas mensagens de erro comuns.
   - Número de porta ou destino incorreto:

     Falha de conexão TCP

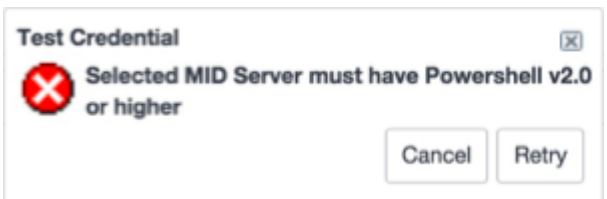
   - Nome de usuário ou senha incorretos:

     Falha de autenticação

   - MID Server incorreto para credenciais do Windows:

     Erro do MID Server

7. Clique em **Repetir** para abrir a caixa de diálogo Credencial de teste e corrija o erro de entrada.
8. Quando seu teste de credenciais for bem-sucedido, clique em **Enviar** para salvar o registro.

> **Importante:** O teste de credenciais não garante que as credenciais tenham os privilégios necessários para as tarefas de fluxo de trabalho pretendidas Descoberta ou Orquestração.

Credenciais Ansible Tower

As credenciais Ansible Tower são necessárias para acessar sua conta de gestão de configuração Ansible. Use essas credenciais para gerenciar os recursos Ansible através da aplicação Gestão de nuvem.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para integrar Cloud Provisioning and Governance com a conta de gestão de configuração do Ansible, você deve configurar o nome de usuário e a senha da conta do administrador no Ansible.

Campos de formulário e credenciais do Ansible Tower

Campo	Descrição
Nome	Forneça um nome descritivo.
Nome de usuário/senha	Insira as credenciais de autenticação do usuário do Ansible Tower com direitos de administrador.

Nota: Não é necessário configurar os outros campos.

Credenciais de chave de API

Uma chave de API é um código exclusivo que é passado para uma API para identificar a aplicação ou usuário de chamada.

Credenciais de chave de API

Campos de formulário de credenciais de chave de API

Campo	Valor de entrada
Nome	Insira um nome exclusivo e descritivo para esta credencial.
Ativo	Habilite ou desabilite essas credenciais para uso.
Chave de API	Insira a chave de API.
Alias de credencial	Permite que os criadores de fluxo e de fluxo de trabalho atribuam credenciais individuais para qualquer atividade em um fluxo ou fluxo de trabalho ou atribua diferentes credenciais a cada ocorrência do mesmo tipo de atividade em um fluxo ou fluxo de trabalho.
Aplica-se a	Selecione se deseja aplicar essas credenciais a **Todos os MID Servers** em sua rede, ou a um ou mais **MID Servers específicos**. Especifique os MID Servers que devem usar essas credenciais no campo **MID Servers**.
Ordem	A ordem (sequência) na qual o Descoberta testa esta credencial ao tentar fazer login nos dispositivos. Quanto menor o número, mais alta será a exibição dessa credencial na lista. Estabeleça a ordem de credenciais ao usar um grande número de credenciais ou quando a segurança bloquear usuários após três tentativas de login com falha. Se todas as credenciais tiverem o mesmo número na ordem (ou número nenhum), a instância vai tentar usar as credenciais em uma ordem aleatória.

Credenciais de aplicativo

Algumas aplicações requerem credenciais além das credenciais que a máquina host precisa. Credenciais necessárias para acessar estas aplicações são chamadas de credenciais de aplicação.

Uma credencial típica contém um nome de usuário e uma senha para fazer login em um dispositivo ou aplicação. Embora a maioria das aplicações exija apenas uma credencial

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

para acessá-las, às vezes, os hosts e as aplicações têm credenciais separadas para segurança extra. Por exemplo, o ABAP SAP Central Services (ASCS) requer credenciais de aplicativo além das credenciais de host SSH ou Windows para o servidor que hospeda o ASCS.

Nota: ServiceNow se referem a dispositivos e aplicativos que compõem um serviço de aplicativos, como ICs (Configuration items, itens de configuração).

Assim como com credenciais de host, você atribui credenciais de aplicativo a MID Servers.

Você cria credenciais de aplicativo por tipo de IC, por exemplo, o tipo de IC para ASCS é a aplicação SAP ASCS [cmdb_ci_appl_sap_ascs]. O padrão pré-configurado para descobrir ICs pertencentes a este tipo de IC contém comandos que exigem um MID Server para usar a credencial do aplicativo para este tipo de IC. Se houver mais de uma credencial configurada para este tipo de IC, o MID Server tentará usar essas credenciais na ordem que você definir até encontrar a credencial adequada.

Verifique as informações de requisitos do Descoberta na documentação da ServiceNow para determinar se você precisa configurar credenciais de aplicação para ICs de aplicação específicos. Não haverá necessidade de configurar credenciais de aplicativo se os pré-requisitos do Descoberta não mencionarem isso.

Campos de formulário de credenciais do aplicativo

Campo	Descrição
Nome	Nome da credencial. Use um nome descritivo como Oracle DB ou London Oracle DB (para um banco de dados Oracle). Não use espaços ou caracteres especiais para o nome da credencial.
Ativo	Marque a caixa de seleção para usar a credencial.
Nome de usuário	Insira o nome de usuário real da credencial do aplicativo.
Senha	Insira a senha real da credencial do aplicativo. Não use espaços ou caracteres especiais para o nome da credencial.
Tipo de IC	Selecione um tipo de IC ao qual o IC pertence.
Alias de credencial	Crie um alias para atribuir credenciais específicas para agendas de descoberta específicos. Ao atribuir um alias, você deve identificar o nome da tabela para o tipo de IC cujas credenciais de aplicação a aplicação usa. As aplicações podem usar credenciais de aplicação de um tipo de IC diferente do seu próprio. Para uma aplicação específica, consulte a lista da tabela apropriada: • ABAP SAP Central Services (ASCS): cmdb_ci_appl_sap_ascs • Dispositivo IBM Security Access Manager: cmdb_ci_app_server_webseal • Instância Central do SAP: cmdb_ci_appl_sap_ascs • SAP Central Services (SCS): cmdb_ci_appl_sap_ascs • Liquidação de recebimento avaliada do SAP (ERS): cmdb_ci_appl_sap_ascs • Cluster SAP Java: cmdb_ci_appl_sap_ascs • Instância de diálogo do SAP NetWeaver: cmdb_ci_appl_sap_ascs • Caixa de correio do Microsoft Exchange (para Microsoft Exchange): cmdb_ci_exchange_mailbox

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campos de formulário de credenciais do aplicativo

Campo	Descrição
	• Banco de dados Microsoft SQL: cmdb_ci_db_mssql_instance • Servidor MySQL: cmdb_ci_db_mysql_instance • Fila da Oracle Advanced: cmdb_ci_db_ora_instance • Banco de dados Oracle: cmdb_ci_db_ora_instance • Conjunto do E-Business Oracle: cmdb_ci_db_ora_instance • Módulo Oracle WebLogic: cmdb_ci_app_server_weblogic • Enterprise Message Service (EMS) de Tibco: cmdb_ci_appl_tibco_message
Aplica-se a	Selecione se deseja aplicar essas credenciais a **Todos os MID Servers** em sua rede, ou a um ou mais **MID Servers específicos**. Especifique os MID Servers que devem usar essas credenciais no campo **MID Servers**.
Ordem	A ordem (sequência) na qual o Descoberta testa esta credencial ao tentar fazer login nos dispositivos. Quanto menor o número, mais alta será a exibição dessa credencial na lista. Estabeleça a ordem de credenciais ao usar um grande número de credenciais ou quando a segurança bloquear usuários após três tentativas de login com falha. Se todas as credenciais tiverem o mesmo número na ordem (ou número nenhum), a instância vai tentar usar as credenciais em uma ordem aleatória.

Credenciais de autenticação básica

O tipo de credencial de autenticação básica gerencia o acesso para armazenar credenciais de autenticação básica.

Esses campos estão disponíveis no formulário de Credenciais para autenticação básica.

Formulário de credenciais de Autenticação básica

Campo	Valor de entrada
Nome	Insira um nome exclusivo e descritivo para esta credencial. Por exemplo, você pode chamá-la **de Autenticação básica**.
Nome de usuário	Insira o nome de usuário.
Senha	Insira a senha.
ID da Credencial	Insira a chave exclusiva configurada para essas credenciais no sistema de armazenamento externo de credenciais da CyberArk. O ID de credencial pode ser usado como uma substituição de seguro quando vários cofres estão em uso. Por padrão, a sintaxe no campo **ID de credencial** é: *<safe name>:<Credential ID>*. Se o nome seguro for omitido, deve haver um nome seguro definido no arquivo `config.xml`. Para mudar o caractere separador dos dois pontos padrão para outro caractere, substitua o valor pelo parâmetro opcional *ext.cred.safe_name*. O campo **ID de credencial** tem um limite de 40 caracteres.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formulário de credenciais de Autenticação básica

Campo	Valor de entrada
	Este campo só fica visível quando a caixa de seleção **Armazenamento externo** está marcada.
Armazenamento de credenciais externas	Marque esta caixa de seleção para usar um sistema de armazenamento externo de credenciais externas. Quando você seleciona esta opção, os campos **Nome de usuário** e **Senha** são substituídos pelo campo **ID de credencial**. Atualmente, o único sistema de armazenamento externo compatível é o CyberArk.
Ordem	A ordem (sequência) na qual o Descoberta testa esta credencial ao tentar fazer login nos dispositivos. Quanto menor o número, mais alta será a exibição dessa credencial na lista. Estabeleça a ordem de credenciais ao usar um grande número de credenciais ou quando a segurança bloquear usuários após três tentativas de login com falha. Se todas as credenciais tiverem o mesmo número na ordem (ou número nenhum), a instância vai tentar usar as credenciais em uma ordem aleatória.

Credenciais do servidor Chef

As credenciais do servidor Chef acessam as integrações do Chef com a instância.

Esses campos estão disponíveis no formulário Credenciais para credenciais de tipo de servidor Chef. Essas informações vêm das configurações que você definiu ao executar a Instalação do servidor Chef.

Campo	Descrição
Nome	Insira um nome exclusivo e descritivo para esta credencial.
Ativo	Habilite ou desabilite essas credenciais para uso.
Nome do Administrador	Forneça o nome do administrador que você criou durante a instalação do servidor Chef.
Chave de Administrador	Insira a chave privada RSA que o servidor Chef gerou quando você criou o administrador.
Nome do validador	Insira o validador.
Chave de Validador	Insira a chave privada RSA que o servidor Chef gerou quando você criou uma organização.
Nome do Cert.	Insira o nome da certificação.
Chave de Certificado	Insira a chave de certificação.

Credenciais CIM

O tipo de credencial CIM gerencia o acesso a um servidor CIM (também chamado de CIMOM – Common Information Model Object Manager) para obter informações sobre servidores VMware ESX. Este tipo de credencial está disponível para a Descoberta.

Esses campos ficam disponíveis no formulário Credenciais para CIM.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Nome	Insira um nome exclusivo e descritivo para esta credencial.
Ativo	Habilite ou desabilite essas credenciais para uso.
Nome de usuário	Insira o nome de usuário a ser criado na tabela Credenciais. Evite espaços iniciais ou finais em nomes de usuário. Um aviso vai ser exibido se a plataforma detectar espaços iniciais ou finais no nome de usuário. Para a descoberta CIM, o usuário deve ter a função de administrador.
Senha	Insira a senha.
ID da Credencial	Insira a chave exclusiva configurada para credenciais externas no arquivo JAR carregado no MID Server para um sistema de credenciais externas. O campo **ID de credencial** tem um limite de 40 caracteres. Este campo só estará visível quando a caixa de seleção **Armazenamento de credenciais externas** estiver marcada.
Alias de credencial	Permita que os criadores do fluxo de trabalho atribuam credenciais individuais a qualquer atividade em um fluxo de trabalho do Orquestração ou atribuam credenciais diferentes a cada ocorrência do mesmo tipo de atividade em um fluxo de trabalho do Orquestração. Para usar a credencial para descobrir ICs que não pertencem a este tipo de IC usando o Mapeamento de serviços e os Padrões de descoberta, insira o nome da tabela para o tipo de IC ao qual o IC pertence, por exemplo, cmdb_ci_apache_web_server.
Armazenamento externo de credenciais	Marque esta caixa de seleção para usar um sistema de armazenamento externo de credenciais externas. Quando você seleciona esta opção, os campos **Nome de usuário** e **Senha** são substituídos pelo campo **ID de credencial**. O armazenamento externo de credenciais só está disponível quando o plug-in Armazenamento externo de credenciais está ativado. **Nota:** Atualmente, o único sistema de armazenamento externo compatível é o CyberArk.
Aplica-se a	Selecione se deseja aplicar essas credenciais a **Todos os MID Servers** em sua rede, ou a um ou mais **MID Servers específicos**. Especifique os MID Servers que devem usar essas credenciais no campo **MID Servers**.
MID servers	Selecione um ou mais MID Servers na lista de MID Servers disponíveis. As credenciais configuradas neste registro estão disponíveis para os MID Servers nesta lista. Este campo está disponível somente quando você seleciona **MID Servers específicos** no campo **Aplica-se a**. **Nota:** Selecionar **MID Servers específicos** não afeta a seleção do MID Server. Ele é usado somente para decidir quais MID Servers devem ter visibilidade para a credencial. **MID Servers específicos** não são compatíveis com atividades do Orquestração.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Ordem	A ordem (sequência) na qual o Descoberta testa esta credencial ao tentar fazer login nos dispositivos. Quanto menor o número, mais alta será a exibição dessa credencial na lista. Estabeleça a ordem de credenciais ao usar um grande número de credenciais ou quando a segurança bloquear usuários após três tentativas de login com falha. Se todas as credenciais tiverem o mesmo número na ordem (ou número nenhum), a instância vai tentar usar as credenciais em uma ordem aleatória.
Conta de serviço Windows MID Server	Quando ativa, a credencial definida representa a conta de serviço do MID Server.

Configure dispositivos de armazenamento NetApp para credenciais CIM

Os dispositivos de armazenamento NetApp exigem configuração adicional para que o Descoberta possa explorá-los.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Instale o agente SMI-S no host do dispositivo de armazenamento.

   Consulte Guia de Instalação e Configuração do Data ONTAP SMI-S Agent 5.2 para obter instruções e requisitos.

   Nota:

   A ServiceNow não mantém a documentação neste site. Este documento pode mudar sem aviso prévio.

2. Crie uma conta de usuário e uma senha para o agente SMI-S.
3. Crie um registro de credencial para as credenciais do agente SMI-S.
   Defina o tipo de credencial como **CIM**.

Credenciais de acesso à nuvem

Os tipos de credencial em nuvem gerenciam o acesso a aplicações baseadas em nuvem, incluindo Amazon Web Services e a nuvem do Microsoft Azure.

Funções IAM (Identity and Access Management) AWS

Se você tiver um MID Server instalado no Amazon EC2 em uma nuvem AWS e se o MID Server estiver configurado para descobrir os recursos na nuvem, é possível usar as credenciais de segurança fornecidas pelas funções IAM (Identity and Access Management) AWS em vez das credenciais gerenciadas em sua instância. Essas credenciais AWS concedem permissões na nuvem através de um perfil de instância, com base em funções. Essas credenciais são temporárias e giram automaticamente em um intervalo configurável. Quando uma função de IAM é definida no MID Server. Para obter detalhes, consulte Configurar o MID Server para funções de IAM da AWS.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A Descoberta ignora quaisquer credenciais armazenadas na instância em favor das credenciais concedidas pela função no perfil da instância. Para obter mais informações sobre os perfis de instância AWS, consulte Funções IAM para Amazon EC2.

Credenciais AWS

Campos de formulário de credenciais da AWS

Campo	Valor de entrada
Nome	Nome exclusivo e descritivo das credenciais de AWS.
Ativo	Opção para usar a credencial.
ID da chave de acesso	O **ID da chave de acesso** que você gerou no Console de gestão da AWS, como: APIAIOSFODNN7EXAMPLE.
Chave secreta de acesso	A **Chave secreta de acesso** que você gerou no Console de gestão da AWS, como: wPalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY.

Campos de formulário da credencial Azure Service Principal

Campo	Valor
Nome	Insira o nome da entidade de serviço a ser registrada na instância.
ID de locatário e	Cole o valor da **ID do diretório** do Azure do portal do Azure no campo Gestão de nuvem **ID do locatário**.
ID de cliente	Cole o valor de **ID da aplicação** do Azure que você registrou no campo Gestão de nuvem **ID do cliente**.
Método de Autenticação	Selecione **Segredo do cliente**. **Nota:** Não há suporte para **Asserção do cliente**.
Chave secreta	Cole a chave secreta que foi gerada ao criar a entidade de serviço do Azure. Este campo aparece quando o **Método de autenticação** é **Segredo do cliente**.

Credenciais de Contrato do Azure Enterprise

As credenciais do Contrato do Azure Enterprise são necessárias para a funcionalidade de faturamento fornecida pela aplicação Gestão de nuvem.

Campos de formulário das credenciais do Contrato do Azure Enterprise

Campo	Descrição
Nome	Insira um nome descritivo.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campos de formulário das credenciais do Contrato do Azure Enterprise

Campo	Descrição
Número de inscrição	Insira o número de inscrição do Azure.
Chave de acesso	Cole a chave de acesso que o Azure fornece.

Credenciais da Gestão de nuvem

Este tipo de credencial está disponível para Orquestração.

Campos de formulário das credenciais da Gestão de nuvem

Campo	Valor de entrada
Nome	Insira um nome exclusivo e descritivo para esta credencial. Por exemplo, você pode chamá-lo de **Cloud Atlanta**.
Ativo	Habilite ou desabilite essas credenciais para uso.
Tipo	Especifique o **AWS**.
Nome de usuário	Insira o nome do usuário CIM para criar na tabela Credenciais. Evite os espaços iniciais ou finais nos nomes de usuário. Um aviso vai ser exibido se a plataforma detectar espaços iniciais ou finais no nome de usuário.
Senha	Insira a senha CIM.
Senha SSH	Insira uma frase memorável para geração de chave. Por exemplo, é possível inserir **Sexta-feira é um bom dia**.
Chave privada SSH	Insira a chave privada SSH.
Protocolo de autenticação	Selecione o protocolo de autenticação **MD5**ou **SHA** que foi usado para gerar a **Chave de autenticação**.
Chave de Autenticação	Insira uma chave de autenticação gerada por SSH.
Protocolo de privacidade	Insira um dos seguintes protocolos de privacidade que descreva a criptografia para a **Chave de privacidade**: • **3DES** para Triple DES (Data Encryption Standard) • **AES128** para AES (Advanced Encryption Standard) com criptografia de 128 bits • **AES192** para AES com criptografia de 192 bits • **AES256** para AES com criptografia de 256 bits • **DES** para criptografia DES legada
Insira uma chave de privacidade adicional.	
Alias de credencial	Permita que os criadores do fluxo de trabalho atribuam credenciais individuais a qualquer atividade em um fluxo de trabalho da Orquestração ou atribuam credenciais diferentes a cada ocorrência do mesmo tipo de atividade em um fluxo de trabalho da Orquestração.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campos de formulário das credenciais da Gestão de nuvem

Campo	Valor de entrada
Armazenamento externo de credenciais	Marque esta caixa de seleção para usar um sistema de armazenamento externo de credenciais externas. Quando você seleciona esta opção, os campos **Nome de usuário** e **Senha** são substituídos pelo campo **ID de credencial**. Atualmente, o único sistema de armazenamento externo suportado é CyberArk.
Aplica-se a	Selecione se deseja aplicar essas credenciais a **Todos os MID Servers** em sua rede, ou a um ou mais **MID Servers específicos**. Especifique os MID Servers que devem usar essas credenciais no campo **MID Servers**.
Classificação	Insira a Classificação de Aplicação para descoberta de CI.
Ordem	A ordem (sequência) na qual o Descoberta testa esta credencial ao tentar fazer login nos dispositivos. Quanto menor o número, mais alta será a exibição dessa credencial na lista. Estabeleça a ordem de credenciais ao usar um grande número de credenciais ou quando a segurança bloquear usuários após três tentativas de login com falha. Se todas as credenciais tiverem o mesmo número na ordem (ou número nenhum), a instância vai tentar usar as credenciais em uma ordem aleatória.

Credenciais de nó da Gestão de nuvem (CMP)

As credenciais de nó da Gestão de nuvem (CMP) associam as credenciais para um servidor virtual que a Gestão de nuvem provisiona. A aplicação Gestão de nuvem cria automaticamente essas credenciais.

Nota: Talvez seja necessário desativar essas credenciais, se você não quiser mais usá-las, mudar a precedência da ordem ou selecionar um MID Server com permissão para acessá-las. Caso contrário, não será necessário criar ou modificar manualmente este tipo de credencial.

Campos de formulário de credenciais de nó CMP

Campo	Descrição
Nome	O nome gerado automaticamente com base no datacenter em que a máquina virtual está localizada.
Ativo	Se as credenciais estiverem ativas.
Aplica-se a	Escolha se esta credencial está disponível para um MID Server específico ou todos os MID Servers.
Ordem	A ordem (sequência) na qual o Descoberta testa esta credencial ao tentar fazer login nos dispositivos. Quanto menor o número, mais alta será a exibição dessa credencial na lista. Estabeleça a ordem de credenciais ao usar um grande número de credenciais ou quando a segurança bloquear usuários após três tentativas de login com falha. Se todas as credenciais tiverem o mesmo número na ordem (ou número nenhum), a instância vai tentar usar as credenciais em uma ordem aleatória.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campos de formulário de credenciais de nó CMP

Campo	Descrição
Nome de usuário e senha.	O nome de usuário e a senha do servidor virtual.
Senha SSH e chave privada SSH	A chave privada e a senha que protegem a chave se o servidor virtual precisar dela.
Protocolo de autenticação e chave de autenticação	A chave privada e a senha que protegem a chave se o servidor virtual precisar dela.
Protocolo de privacidade e chave de privacidade	O protocolo de criptografia usado com o servidor virtual e insira a chave de privacidade.
Alias de credencial	Permita que os criadores do fluxo de trabalho atribuam credenciais individuais a qualquer atividade em um fluxo de trabalho do Orquestração ou atribuam credenciais diferentes a cada ocorrência do mesmo tipo de atividade em um fluxo de trabalho do Orquestração.

Credenciais do par de chaves SSH da Gestão de nuvem (CMP)

Os pares de chave SSH da Gestão de nuvem (CMP) armazenam as chaves que a aplicação Gestão de nuvem gera automaticamente quando os usuários provisionam os recursos da pilha.

Nota: Talvez seja necessário desativar essas credenciais, se não desejar mais usá-las. Caso contrário, não será necessário criar ou modificar manualmente este tipo de credencial.

Campos de formulário de credenciais de par de chaves SSH CMP

Campo	Descrição
Nome	O nome gerado automaticamente.
Ativo	Se as credenciais estiverem ativas.
Chave pública SSH	A chave pública.
Chave privada SSH	Uma chave privada segura que pode ser usada em vez de uma senha para logins SSH.

Credenciais de Infoblox

As credenciais Infoblox são necessárias para configurar pools IP (IPAM) na aplicação Gestão de nuvem.

Esses campos estão disponíveis no formulário Credenciais para credenciais de tipo Infoblox.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Nome	Insira um nome exclusivo e descritivo para esta credencial.
Ativo	Habilite ou desabilite essas credenciais para uso.
Aplica-se a	Escolha se esta credencial está disponível para um MID Server específico ou todos os MID Servers.
Ordem	A ordem (sequência) na qual o Descoberta testa esta credencial ao tentar fazer login nos dispositivos. Quanto menor o número, mais alta será a exibição dessa credencial na lista. Estabeleça a ordem de credenciais ao usar um grande número de credenciais ou quando a segurança bloquear usuários após três tentativas de login com falha. Se todas as credenciais tiverem o mesmo número na ordem (ou número nenhum), a instância vai tentar usar as credenciais em uma ordem aleatória. A ordem (sequência) na qual o Descoberta testa esta credencial ao tentar fazer login nos dispositivos. Quanto menor o número, mais alta será a exibição dessa credencial na lista. Estabeleça a ordem de credenciais ao usar um grande número de credenciais ou quando a segurança bloquear usuários após três tentativas de login com falha. Se todas as credenciais tiverem o mesmo número na ordem (ou número nenhum), a instância vai tentar usar as credenciais em uma ordem aleatória.
Versão de wAPI	Insira a versão de wAPI que você está usando.
Nome de usuário e senha.	Insira o nome de usuário InfoBlox e a senha.

Credenciais JDBC

O tipo de credencial JDBC gerencia o acesso a uma conexão JDBC (Java Database Connectivity). Este tipo de credencial está disponível para Descoberta e Orquestração.

Esses campos estão disponíveis no formulário Credenciais para credenciais de tipo JDBC.

Campo	Descrição
Nome	Insira um nome exclusivo e descritivo para esta credencial.
Ativo	Habilite ou desabilite essas credenciais para uso.
Nome de usuário	Insira o nome de usuário a ser criado na tabela Credenciais. Evite espaços iniciais ou finais em nomes de usuário. Um aviso vai ser exibido se a plataforma detectar espaços iniciais ou finais no nome de usuário. Para a descoberta CIM, o usuário deve ter a função de administrador.
Senha	Insira a senha.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
ID da Credencial	Insira a chave exclusiva configurada para credenciais externas no arquivo JAR carregado no MID Server para um sistema de credenciais externas. O campo **ID de credencial** tem um limite de 40 caracteres. Este campo só estará visível quando a caixa de seleção **Armazenamento de credenciais externas** estiver marcada.
Alias de credencial	Permita que os criadores do fluxo de trabalho atribuam credenciais individuais a qualquer atividade em um fluxo de trabalho do Orquestração ou atribuam credenciais diferentes a cada ocorrência do mesmo tipo de atividade em um fluxo de trabalho do Orquestração. Para usar a credencial para descobrir ICs que não pertencem a este tipo de IC usando o Mapeamento de serviços e os Padrões de descoberta, insira o nome da tabela para o tipo de IC ao qual o IC pertence, por exemplo, cmdb_ci_apache_web_server.
Armazenamento externo de credenciais	Marque esta caixa de seleção para usar um sistema de armazenamento externo de credenciais externas. Quando você seleciona esta opção, os campos **Nome de usuário** e **Senha** são substituídos pelo campo **ID de credencial**. O armazenamento externo de credenciais só está disponível quando o plug-in Armazenamento externo de credenciais está ativado. **Nota:** Atualmente, o único sistema de armazenamento externo compatível é o CyberArk.
Aplica-se a	Selecione se deseja aplicar essas credenciais a **Todos os MID Servers** em sua rede, ou a um ou mais **MID Servers específicos**. Especifique os MID Servers que devem usar essas credenciais no campo **MID Servers**.
MID servers	Selecione um ou mais MID Servers na lista de MID Servers disponíveis. As credenciais configuradas neste registro estão disponíveis para os MID Servers nesta lista. Este campo está disponível somente quando você seleciona **MID Servers específicos** no campo **Aplica-se a**. **Nota:** Selecionar **MID Servers específicos** não afeta a seleção do MID Server. Ele é usado somente para decidir quais MID Servers devem ter visibilidade para a credencial. **MID Servers específicos** não são compatíveis com atividades do Orquestração.
Ordem	A ordem (sequência) na qual o Descoberta testa esta credencial ao tentar fazer login nos dispositivos. Quanto menor o número, mais alta será a exibição dessa credencial na lista. Estabeleça a ordem de credenciais ao usar um grande número de credenciais ou quando a segurança bloquear usuários após três tentativas de login com falha. Se todas as credenciais tiverem o mesmo número na ordem (ou número nenhum), a instância vai tentar usar as credenciais em uma ordem aleatória.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Conta de serviço Windows MID Server	Quando ativa, a credencial definida representa a conta de serviço do MID Server.

Credenciais JMS

O tipo de credenciais JMS gerencia o acesso a um JMS (Java Message Service). Este tipo de credencial está disponível para Descoberta e Orquestração.

Esses campos ficam disponíveis no formulário Credenciais para JMS.

Campo	Descrição
Nome	Insira um nome exclusivo e descritivo para esta credencial.
Ativo	Habilite ou desabilite essas credenciais para uso.
Nome de usuário	Insira o nome de usuário a ser criado na tabela Credenciais. Evite espaços iniciais ou finais em nomes de usuário. Um aviso vai ser exibido se a plataforma detectar espaços iniciais ou finais no nome de usuário. Para a descoberta CIM, o usuário deve ter a função de administrador.
Senha	Insira a senha.
ID da Credencial	Insira a chave exclusiva configurada para credenciais externas no arquivo JAR carregado no MID Server para um sistema de credenciais externas. O campo **ID de credencial** tem um limite de 40 caracteres. Este campo só estará visível quando a caixa de seleção **Armazenamento de credenciais externas** estiver marcada.
Alias de credencial	Permita que os criadores do fluxo de trabalho atribuam credenciais individuais a qualquer atividade em um fluxo de trabalho do Orquestração ou atribuam credenciais diferentes a cada ocorrência do mesmo tipo de atividade em um fluxo de trabalho do Orquestração. Para usar a credencial para descobrir ICs que não pertencem a este tipo de IC usando o Mapeamento de serviços e os Padrões de descoberta, insira o nome da tabela para o tipo de IC ao qual o IC pertence, por exemplo, cmdb_ci_apache_web_server.
Armazenamento externo de credenciais	Marque esta caixa de seleção para usar um sistema de armazenamento externo de credenciais externas. Quando você seleciona esta opção, os campos **Nome de usuário** e **Senha** são substituídos pelo campo **ID de credencial**. O armazenamento externo de credenciais só está disponível quando o plug-in Armazenamento externo de credenciais está ativado. **Nota:** Atualmente, o único sistema de armazenamento externo compatível é o CyberArk.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Aplica-se a	Selecione se deseja aplicar essas credenciais a **Todos os MID Servers** em sua rede, ou a um ou mais **MID Servers específicos**. Especifique os MID Servers que devem usar essas credenciais no campo **MID Servers**.
MID servers	Selecione um ou mais MID Servers na lista de MID Servers disponíveis. As credenciais configuradas neste registro estão disponíveis para os MID Servers nesta lista. Este campo está disponível somente quando você seleciona **MID Servers específicos** no campo **Aplica-se a**. **Nota:** Selecionar **MID Servers específicos** não afeta a seleção do MID Server. Ele é usado somente para decidir quais MID Servers devem ter visibilidade para a credencial. **MID Servers específicos** não são compatíveis com atividades do Orquestração.
Ordem	A ordem (sequência) na qual o Descoberta testa esta credencial ao tentar fazer login nos dispositivos. Quanto menor o número, mais alta será a exibição dessa credencial na lista. Estabeleça a ordem de credenciais ao usar um grande número de credenciais ou quando a segurança bloquear usuários após três tentativas de login com falha. Se todas as credenciais tiverem o mesmo número na ordem (ou número nenhum), a instância vai tentar usar as credenciais em uma ordem aleatória.
Conta de serviço Windows MID Server	Quando ativa, a credencial definida representa a conta de serviço do MID Server.

Credenciais OAuth 2.0

As credenciais do OAuth 2.0 permitem que a ServiceNow obtenha acesso às contas de usuário em um serviço HTTP.

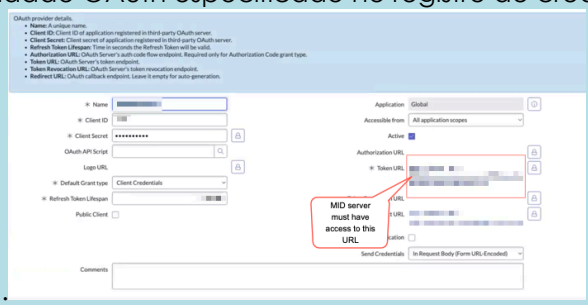
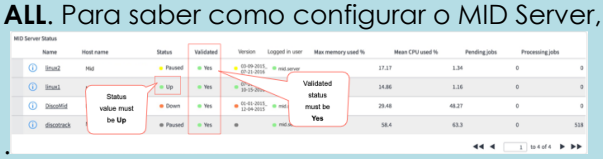
Esses campos ficam disponíveis no formulário Credenciais para OAuth 2.0.

Formulário de credenciais OAuth 2.0

Campo	Valor de entrada
Nome	Insira um nome exclusivo e descritivo para esta credencial. Por exemplo, é possível chamar isso de **Credencial OAuth2**.
Ativo	Especifique se esta credencial está ativa.
Perfil de Entidade OAuth	Um perfil OAuth é uma combinação de um tipo de concessão e pelo menos um escopo.
Conectar-se ao servidor Auth via MID Server	Conecta sua instância ServiceNow a um servidor OAuth no local que reside atrás de um firewall por meio de um MID Server. Ele também pode conectar sua instância ServiceNow a um servidor OAuth baseado na nuvem por meio de um MID Server. Quando esta opção é habilitada, a solicitação de um token de OAuth é enviada por meio do MID Server.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formulário de credenciais OAuth 2.0

Campo	Valor de entrada
	Importante: • A opção aparece quando o valor no campo **Tipo de concessão** no Perfil de entidade OAuth é definido como **Credenciais do cliente**. Para saber como definir um perfil de entidade OAuth para um provedor terceirizado de OAuth, consulte Conectar-se a um provedor OAuth de terceiros. • Se você habilitar a caixa de seleção **Conectar-se ao servidor Auth via MID Server**, deverá identificar o MID Server ou MID Servers necessário na lista **Aplica-se a**.
Aplica-se a	Especifique se o registro da credencial é aplicável a todos os MID Servers ou a um MID Server específico. Se específico, adicione os MID Servers conforme necessário. **Importante:** Lembre-se dessas considerações se tiver marcado a caixa de seleção **Conectar-se ao servidor Auth via MID Server**. • Certifique-se de que todos os MID Servers selecionados em Aplica-se a possam se comunicar com o servidor Auth. Isso é necessário para executar a solicitação de **URL de token** do token mencionado no registro do provedor OAuth (que está vinculado ao perfil da entidade OAuth especificado no registro de credencial do OAuth 2.0).  • Certifique-se de que haja pelo menos um MID Server (no MID Servers selecionado em **Aplica-se a**) com estas configurações: ◦ O valor do campo **Status** é **Ativo**. ◦ O valor do campo **Validado** é **Sim**. ◦ A capacidade de MID Server está definida como **REST** ou **ALL**. Para saber como configurar o MID Server, consulte  . Para saber mais sobre esses status, consulte Painel do MID Server.
Ordem	A ordem (sequência) na qual o Descoberta testa esta credencial ao tentar fazer login nos dispositivos. Quanto menor o número, mais alta será a exibição

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formulário de credenciais OAuth 2.0

Campo	Valor de entrada
	dessa credencial na lista. Estabeleça a ordem de credenciais ao usar um grande número de credenciais ou quando a segurança bloquear usuários após três tentativas de login com falha. Se todas as credenciais tiverem o mesmo número na ordem (ou número nenhum), a instância vai tentar usar as credenciais em uma ordem aleatória.
Alias de credencial	Especifique o alias de credencial que você deseja vincular à credencial do OAuth 2.0.
Tipo de Integração	Indica o tipo de integração para a credencial. Invoque a API de terceiros com a solicitação de Oauth que gera o token de OAuth que seja específico do sistema ou do usuário. A seguir estão os tipos de integração: • **Sistema**: extraia as informações de token com base no perfil do solicitante. • **Pessoal**: extraia as informações de token que sejam específicas do usuário. O usuário que inicia a sessão. Se **Pessoal** for selecionado na página Perfil do solicitante do OAuth, um sinalizador adicional denominado **Pessoal** será exibido. **Nota:** • Quaisquer informações relacionadas a um usuário somente podem ser acessadas com tokens de OAuth específicos do usuário com o Tipo de integração **Pessoal**. • Para usar o token relacionado ao usuário de sessão, você precisa selecionar **Executar como** arquivado nas Propriedades de fluxo como **Usuário que inicia a sessão**.

Credenciais do SAP

O tipo de credencial do SAP gerencia o acesso aos sistemas SAP JCo. Este tipo de credencial está disponível para Descoberta e Orquestração.

Esses campos estão disponíveis no formulário Credenciais para as credenciais do tipo SAP.

Campo	Descrição
Nome	Insira um nome exclusivo e descritivo para esta credencial.
Ativo	Habilite ou desabilite essas credenciais para uso.
Nome de usuário	Insira o nome de usuário a ser criado na tabela Credenciais. Evite espaços iniciais ou finais em nomes de usuário. Um aviso vai ser exibido se a plataforma detectar espaços iniciais ou finais no nome de usuário. Para a descoberta CIM, o usuário deve ter a função de administrador.
Senha	Insira a senha.
ID da Credencial	Insira a chave exclusiva configurada para credenciais externas no arquivo JAR carregado no MID Server para um sistema de credenciais externas. O campo **ID de credencial** tem um limite de 40 caracteres.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Este campo só estará visível quando a caixa de seleção **Armazenamento de credenciais externas** estiver marcada.
Alias de credencial	Permita que os criadores do fluxo de trabalho atribuam credenciais individuais a qualquer atividade em um fluxo de trabalho do Orquestração ou atribuam credenciais diferentes a cada ocorrência do mesmo tipo de atividade em um fluxo de trabalho do Orquestração. Para usar a credencial para descobrir ICs que não pertencem a este tipo de IC usando o Mapeamento de serviços e os Padrões de descoberta, insira o nome da tabela para o tipo de IC ao qual o IC pertence, por exemplo, cmdb_ci_apache_web_server.
Armazenamento externo de credenciais	Marque esta caixa de seleção para usar um sistema de armazenamento externo de credenciais externas. Quando você seleciona esta opção, os campos **Nome de usuário** e **Senha** são substituídos pelo campo **ID de credencial**. O armazenamento externo de credenciais só está disponível quando o plug-in Armazenamento externo de credenciais está ativado. **Nota:** Atualmente, o único sistema de armazenamento externo compatível é o CyberArk.
Aplica-se a	Selecione se deseja aplicar essas credenciais a **Todos os MID Servers** em sua rede, ou a um ou mais **MID Servers específicos**. Especifique os MID Servers que devem usar essas credenciais no campo **MID Servers**.
MID servers	Selecione um ou mais MID Servers na lista de MID Servers disponíveis. As credenciais configuradas neste registro estão disponíveis para os MID Servers nesta lista. Este campo está disponível somente quando você seleciona **MID Servers específicos** no campo **Aplica-se a**. **Nota:** Selecionar **MID Servers específicos** não afeta a seleção do MID Server. Ele é usado somente para decidir quais MID Servers devem ter visibilidade para a credencial. **MID Servers específicos** não são compatíveis com atividades do Orquestração.
Ordem	A ordem (sequência) na qual o Descoberta testa esta credencial ao tentar fazer login nos dispositivos. Quanto menor o número, mais alta será a exibição dessa credencial na lista. Estabeleça a ordem de credenciais ao usar um grande número de credenciais ou quando a segurança bloquear usuários após três tentativas de login com falha. Se todas as credenciais tiverem o mesmo número na ordem (ou número nenhum), a instância vai tentar usar as credenciais em uma ordem aleatória.
Conta de serviço Windows MID Server	Quando ativa, a credencial definida representa a conta de serviço do MID Server.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Credenciais de SNMP

Descoberta explora muitos tipos de dispositivos (comutadores, roteadores, impressoras e assim por diante) usando o protocolo SNMP. As credenciais do SNMP não incluem um nome de usuário, apenas uma senha, chamada de *cadeia de caracteres da comunidade*.

A cadeia de caracteres da comunidade somente leitura padrão para vários dispositivos SNMP é pública e Descoberta tentará isso automaticamente. Insira as credenciais SNMP apropriadas, se forem diferentes da cadeia de caracteres *pública*.

A descoberta do SNMP usa todas as cadeias de caracteres da comunidade configuradas. Este comportamento não se aplica à descoberta do SNMPv3.

A Consulta SNMP de atividade da Orquestração padrão retorna o identificador de objeto (OID) de um dispositivo e requer credenciais SNMP.

Credenciais da comunidade SNMP

O tipo de credencial de Comunidade SNMP gerencia o acesso para descobrir muitos tipos de dispositivos (comutadores, roteadores, impressoras, etc.) usando o protocolo SNMP. Este tipo de credencial está disponível para Descoberta, Mapeamento de serviços e Orquestração.

As credenciais do SNMP não incluem um nome de usuário, apenas uma senha (a cadeia de caracteres da comunidade). A cadeia de caracteres da comunidade somente leitura padrão para vários dispositivos SNMP é pública e o sistema tentará isso automaticamente. Insira as credenciais SNMP apropriadas, se forem diferentes da cadeia de caracteres pública.

Esses campos estão disponíveis no formulário Credenciais para comunidade SNMP.

Campo	Descrição
Nome	Insira um nome exclusivo e descritivo para esta credencial.
Ativo	Habilite ou desabilite essas credenciais para uso.
Nome de usuário	Insira o nome de usuário a ser criado na tabela Credenciais. Evite espaços iniciais ou finais em nomes de usuário. Um aviso vai ser exibido se a plataforma detectar espaços iniciais ou finais no nome de usuário. Para a descoberta CIM, o usuário deve ter a função de administrador.
Senha	Insira a senha.
ID da Credencial	Insira a chave exclusiva configurada para credenciais externas no arquivo JAR carregado no MID Server para um sistema de credenciais externas. O campo **ID de credencial** tem um limite de 40 caracteres. Este campo só estará visível quando a caixa de seleção **Armazenamento de credenciais externas** estiver marcada.
Alias de credencial	Permita que os criadores do fluxo de trabalho atribuam credenciais individuais a qualquer atividade em um fluxo de trabalho do Orquestração ou atribuam credenciais diferentes a cada ocorrência do mesmo tipo de atividade em um fluxo de trabalho do Orquestração. Para usar a credencial para descobrir ICs que não pertencem a este tipo de IC usando o Mapeamento de serviços e os Padrões de

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	descoberta, insira o nome da tabela para o tipo de IC ao qual o IC pertence, por exemplo, cmdb_ci_apache_web_server.
Armazenamento externo de credenciais	Marque esta caixa de seleção para usar um sistema de armazenamento externo de credenciais externas. Quando você seleciona esta opção, os campos **Nome de usuário** e **Senha** são substituídos pelo campo **ID de credencial**. O armazenamento externo de credenciais só está disponível quando o plug-in Armazenamento externo de credenciais está ativado. **Nota:** Atualmente, o único sistema de armazenamento externo compatível é o CyberArk.
Aplica-se a	Selecione se deseja aplicar essas credenciais a **Todos os MID Servers** em sua rede, ou a um ou mais **MID Servers específicos**. Especifique os MID Servers que devem usar essas credenciais no campo **MID Servers**.
MID servers	Selecione um ou mais MID Servers na lista de MID Servers disponíveis. As credenciais configuradas neste registro estão disponíveis para os MID Servers nesta lista. Este campo está disponível somente quando você seleciona **MID Servers específicos** no campo **Aplica-se a**. **Nota:** Selecionar **MID Servers específicos** não afeta a seleção do MID Server. Ele é usado somente para decidir quais MID Servers devem ter visibilidade para a credencial. **MID Servers específicos** não são compatíveis com atividades do Orquestração.
Ordem	A ordem (sequência) na qual o Descoberta testa esta credencial ao tentar fazer login nos dispositivos. Quanto menor o número, mais alta será a exibição dessa credencial na lista. Estabeleça a ordem de credenciais ao usar um grande número de credenciais ou quando a segurança bloquear usuários após três tentativas de login com falha. Se todas as credenciais tiverem o mesmo número na ordem (ou número nenhum), a instância vai tentar usar as credenciais em uma ordem aleatória.
Conta de serviço Windows MID Server	Quando ativa, a credencial definida representa a conta de serviço do MID Server.

Credenciais SNMPv3

As credenciais SNMPv3 aceitam um protocolo de privacidade e uma chave de privacidade adicional e estão disponíveis para Descoberta e Orquestração. Para armazenamento externo no CyberArk, é possível selecionar uma chave de conta de privacidade.

Esses campos ficam disponíveis no formulário Credenciais para SNMPv3.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campos da credencial SNMPv3

Campo	Valor de entrada
Nome	Nome exclusivo e descritivo desta credencial. Por exemplo, você pode chamá-la de **SNMP Community Atlanta**.
Ativo	Habilite ou desabilite essas credenciais para uso.
Aplica-se a	Selecione se deseja aplicar essas credenciais a **Todos os MID Servers** em sua rede, ou a um ou mais **MID Servers específicos**. Especifique os MID Servers que devem usar essas credenciais no campo **MID Servers**.
MID servers	Selecione um ou mais MID Servers na lista de MID Servers disponíveis. As credenciais configuradas neste registro estão disponíveis para os MID Servers nesta lista. Este campo está disponível somente quando você seleciona **MID Servers específicos** no campo **Aplica-se a**.
Ordem	A ordem (sequência) na qual o Descoberta testa esta credencial ao tentar fazer login nos dispositivos. Quanto menor o número, mais alta será a exibição dessa credencial na lista. Estabeleça a ordem de credenciais ao usar um grande número de credenciais ou quando a segurança bloquear usuários após três tentativas de login com falha. Se todas as credenciais tiverem o mesmo número na ordem (ou número nenhum), a instância vai tentar usar as credenciais em uma ordem aleatória.
Nome de usuário	Insira o nome de usuário de SNMP. Evite espaços à esquerda ou à direita em nomes de usuário. Um aviso será exibido se a plataforma detectar espaços à esquerda ou à direita no nome de usuário.
Protocolo de autenticação	Selecione o tipo de autenticação a ser usado para esta credencial. As opções são: • MD5 • SHA-1 • SHA-224 • SHA-256 • SHA-384 • SHA-512
Chave de Autenticação	Insira a chave de autenticação para usar para esta credencial.
Protocolo de privacidade	Selecione o protocolo de criptografia para esta credencial. As opções são: • 3DES • AES128 • AES192

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campos da credencial SNMPv3

Campo	Valor de entrada
	• AES256 • DES
Chave de privacidade	Insira a chave associada ao protocolo de privacidade selecionado.
ID da Credencial	Insira a chave exclusiva configurada para credenciais externas no arquivo JAR carregado no MID Server para um provedor de credenciais externas. O campo **ID de credencial** tem um limite de 40 caracteres. Este campo só está visível quando a caixa de seleção **Armazenamento de credencial externo** está marcada.
ID de credencial de privacidade	Insira a chave de conta de privacidade configurada para credenciais SNMPv3 no CyberArk. Se você estiver usando um protocolo de privacidade no CyberArk, este campo deve ter o mesmo valor que o campo **Nome** da Conta de privacidade SNMPv3 do CyberArk. Este campo fica visível apenas para SNMPv3 quando você selecionar a **CyberArk** do campo **Tipo de armazenamento de credencial**. Se você não estiver usando uma chave de privacidade para CyberArk, deixe este campo em branco.
Alias de credencial	Permita que os criadores do fluxo de trabalho atribuam credenciais individuais a qualquer atividade em um fluxo de trabalho da Orquestração ou atribuam credenciais diferentes a cada ocorrência do mesmo tipo de atividade em um fluxo de trabalho da Orquestração.
Armazenamento externo de credenciais	Marque esta caixa de seleção para usar um sistema de armazenamento externo de credenciais externas. Quando o armazenamento externo está habilitado, aparece o campo **ID de credencial**. O Armazenamento externo de credenciais só está disponível quando o plug-in Armazenamento externo de credenciais está ativado e a exibição do plug-in **Armazenamento externo de credenciais** foi selecionada.
Tipos de armazenamentos de credenciais	Selecione o provedor de armazenamento externo. Selecione **CyberArk** somente se estiver usando uma chave de privacidade CyberArk SNMPv3. O campo **ID de credencial de privacidade** aparece para permitir a entrada da chave.
Usar Contexto	Marque esta caixa de seleção para adicionar um valor de contexto a esta credencial. Este campo está visível na exibição dA Descoberta . Os contextos não são compatíveis no momento com o Armazenamento externo de credenciais.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campos da credencial SNMPv3

Campo	Valor de entrada
	Nota: Um contexto é uma coleção de informações de gerenciamento acessadas por uma credencial SNMPv3 que faz referência a um OID específico. Às vezes, os contextos são referenciados para coletar informações sobre o dispositivo que não podem ser acessadas pela credencial normal. Um contexto pode ser fornecido pelo fabricante ou configurado separadamente. Para obter informações adicionais, consulte Nome de contexto e ID de contexto. Se você tiver várias credenciais SNMPv3 com o mesmo nome de usuário e chaves, mas alguns de seus dispositivos precisarem de um contexto e outros não, será necessário criar registros separados para cada dispositivo.
Nome do contexto	Insira o valor do nome de contexto desta credencial. Isso só deve ser usado se você tiver dispositivos que exigem este valor para acesso total. Este campo fica visível apenas quando a caixa de seleção **Usar contexto** é marcada.

Credenciais SSH

Descoberta, Orquestração e Integration Hub exploram dispositivos UNIX e Linux usando as credenciais SSH para executar comandos sobre o SSH (Secure Shell). Os comandos SSH devem ser executados com privilégios de root, com credenciais de root ou por meio do uso de sudo. As credenciais de chave privada SSH fornecem segurança adicional.

Conceder privilégios de root

Antes de conceder privilégios de root, revise sua política de segurança e opções com a equipe de segurança da sua organização.

Use uma dessas abordagens para permitir que os usuários executem comandos SSH com privilégios de root:

- Forneça outras credenciais para Descoberta, Orquestração ou Integration Hub, mas conceda ao usuário nessas credenciais o direito de executar determinados comandos com privilégios de root, usando sudo. Esta é uma maneira segura de conceder privilégios limitados. Descoberta, Orquestração ou Integration Hub usam sudo em qualquer probe que tenha o parâmetro `must_sudo`definido como **verdadeiro** (o padrão é **falso**). No entanto, cada sistema deve ser configurado para permitir que o sudo funcione. Isso é feito editando o arquivo **/etc/sudoers** usando o comando **visudo**.
- Forneça credenciais de **root**. Essas são, obviamente, as credenciais mais poderosas, mas podem não ser desejáveis do ponto de vista da segurança. Se Descoberta, Orquestração ou Integration Hub tiver as credenciais de root para qualquer sistema UNIX ou Linux, nenhuma configuração adicional será necessária.

Comandos privilegiados

A plataforma fornece comandos privilegiados padrão para o MID Server usar e a capacidade de adicionar comandos adicionais ao sistema. Para obter detalhes sobre como usar sudo e outros comandos privilegiados, consulte Comandos privilegiados do MID Server.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tipo de credencial de chave privada SSH

Nota: As credenciais de chave privada SSH devem ser usadas na maioria dos casos, pois fornecem melhor segurança do que as credenciais de senha SSH.

Campo	Valor de entrada
Nome	Nome exclusivo e descritivo desta credencial. Por exemplo, você pode chamá-la de **SSH Atlanta**.
Ativo	Habilite ou desabilite essas credenciais para uso.
Nome de usuário	Insira um nome de usuário UNIX ou Linux. Evite espaços iniciais ou finais em nomes de usuário. Um aviso vai ser exibido se a plataforma detectar espaços iniciais ou finais no nome de usuário.
Senha	Insira a senha UNIX ou Linux. Para credenciais de tipo **Chave Privada SSH**, insira a senha sudo se for necessária para o nome de usuário.
Senha SSH	Digite uma senha longa de SSH. Este campo está disponível somente para credenciais de **Chave Privada SSH**.

Chave privada de SSH	Insira uma chave privada RSA, DSA, ECDSA ou ED25519 segura.
	
	A chave privada deve ser inserida no formato apropriado para garantir que esteja criptografada corretamente. A chave privada deve iniciar com a cadeia de caracteres `-----BEGIN`.
	
	Aqui está um exemplo de uma chave privada RSA formatada corretamente:
	`-----BEGIN RSA PRIVATE KEY-----`
	`MIIEogIBAAKCAQEAsEK65scPssPSobpDFMpR+Btv3MS4Q7NP8ERaStRZs`
	`h3IWz+x...`
	`...7hrxV2dbSug60FahyupGWBGtPnXm5PaE2X5WPLuUj94ue48i1Fs`
	`-----END RSA PRIVATE KEY-----`
	
	Um exemplo de chave DSA:
	`-----BEGIN DSA PRIVATE KEY-----`
	`MIIEogIBAAKCAQEAsEK65scPssPSobpDFMpR+Btv3MS4Q7NP8ERaStRZs`
	`h3IWz+x...`
	`...7hrxV2dbSug60FahyupGWBGtPnXm5PaE2X5WPLuUj94ue48i1Fs`
	`-----END DSA PRIVATE KEY-----`
	
	Um exemplo de chave ECDSA:
	`-----BEGIN EC PRIVATE KEY-----`
	`MIIEogIBAAKCAQEAsEK65scPssPSobpDFMpR+Btv3MS4Q7NP8ERaStRZs`
	`h3IWz+x...`
	`...7hrxV2dbSug60FahyupGWBGtPnXm5PaE2X5WPLuUj94ue48i1Fs`
	`-----END EC PRIVATE KEY-----`
	
	E um exemplo de uma chave privada ED25519:
	`-----BEGIN OPENSSH PRIVATE KEY-----`
	`b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAAAM`
	`wAAAAtzc2gtZW`
	`QyNTUxOQAAACAlYlqhcdwx8VQzZ5XaIC5ltQpjRr3lIlq/aE66mufmiwA`
	`AAKDQUtxZ0FLc`

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Valor de entrada

	<pre>WQAAAAtzc2gtZWQyNTUxOQAAACAlYlqhcdwx8VQzZ5XaIC5ltQpjRr3lIlq/aE66mufmiw
	AAAECuvsTkFUPdpTh0kw23i8TYx19qsFOZ3TRgowkkHBh6wSViWqFx3DHxVDNnldogLmW1
	CmNGveUiWr9oTrqa5+aLAAAAGmFiaGluYXYuc3V0YXJATVJFTUE3OTAzMkI3AQID
	-----END OPENSSH PRIVATE KEY-----</pre>
	Nota: Para uma chave privada ED25519, somente o formato de chave OpenSSH é compatível, que é gerado usando o utilitário OpenSSH SSH-keygen.
	
	O Now Platform oferece suporte a chaves privadas no formato PEM gerado pelo utilitário OpenSSH ssh-keygen. Para converter chaves PPK que foram geradas pelo PuTTY:
	
	• Abra sua chave privada no PuTTYGen.
	• Exporte-a no formato OpenSSH no menu **Conversões** > **Exportar chave OpenSSH**.
	• Salve a nova chave OpenSSH.

Certificado SSH	Insira um certificado OpenSSH baseado em RSA ou ED25519. Quando o certificado é inserido, uma chave privada é usada para autenticação baseada em certificados. Essa autenticação é compatível com OpenSSH versão 7.8 ou mais recente.
Alias de credencial	• Permita que os designers de fluxo usem aliases para gerenciar informações de conexão e de credencial. O uso de um alias elimina a necessidade de configurar várias credenciais e perfis de informações de conexão ao usar vários ambientes. Se as informações de conexão ou de credencial forem alteradas, não será necessário atualizar nenhuma ação que use a conexão. Para obter mais informações, consulte Conexões e credenciais. • Permita que os criadores do fluxo de trabalho atribuam credenciais individuais a qualquer atividade em um fluxo de trabalho do Orquestração ou atribuam credenciais diferentes a cada ocorrência do mesmo tipo de atividade em um fluxo de trabalho do Orquestração.
Armazenamento externo de credenciais	Marque esta caixa de seleção para usar um sistema de armazenamento externo de credenciais externas. Quando você seleciona esta opção, os campos **Nome de usuário** e **Senha** são substituídos pelo campo **ID de credencial**. Atualmente, o único sistema de armazenamento externo compatível é o CyberArk.
MID servers	Selecione um ou mais MID Servers na lista de MID Servers disponíveis. As credenciais configuradas neste registro estão disponíveis para os MID Servers nesta lista. Este campo está disponível somente quando você seleciona **MID Servers específicos** no campo **Aplica-se a**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Valor de entrada
Aplica-se a	Selecione se deseja aplicar essas credenciais a **Todos os MID Servers** em sua rede, ou a um ou mais **MID Servers específicos**. Especifique os MID Servers que devem usar essas credenciais no campo **Servidores MID**.
Ordem	A ordem (sequência) na qual a plataforma experimenta esta credencial ao tentar fazer login nos dispositivos. Quanto menor o número, mais alta será a exibição dessa credencial na lista. Estabeleça a ordem de credenciais ao usar um grande número de credenciais ou quando a segurança bloquear usuários após três tentativas de login com falha. Se todas as credenciais tiverem o mesmo número de pedido (ou nenhum), a Descoberta ou Orquestração tentará as credenciais em uma ordem aleatória.

Tipo de credencial SSH

Esses campos estão disponíveis no formulário de credenciais SSH.

Campo	Descrição
Nome	Insira um nome exclusivo e descritivo para esta credencial.
Ativo	Habilite ou desabilite essas credenciais para uso.
Nome de usuário	Insira o nome de usuário a ser criado na tabela Credenciais. Evite espaços iniciais ou finais em nomes de usuário. Um aviso vai ser exibido se a plataforma detectar espaços iniciais ou finais no nome de usuário. Para a descoberta CIM, o usuário deve ter a função de administrador.
Senha	Insira a senha.
ID da Credencial	Insira a chave exclusiva configurada para credenciais externas no arquivo JAR carregado no MID Server para um sistema de credenciais externas. O campo **ID de credencial** tem um limite de 40 caracteres. Este campo só estará visível quando a caixa de seleção **Armazenamento de credenciais externas** estiver marcada.
Alias de credencial	• Permita que os designers de fluxo usem aliases para gerenciar informações de conexão e de credencial. O uso de um alias elimina a necessidade de configurar várias credenciais e perfis de informações de conexão ao usar vários ambientes. Se as informações de conexão ou de credencial forem alteradas, não será necessário atualizar nenhuma ação que use a conexão. Para obter mais informações, consulte Conexões e credenciais. • Permita que os criadores do fluxo de trabalho atribuam credenciais individuais a qualquer atividade em um fluxo de trabalho do Orquestração ou atribuam credenciais diferentes a cada ocorrência do mesmo tipo de atividade em um fluxo de trabalho do Orquestração. Para usar a credencial para descobrir ICs que não pertencem a este tipo de IC usando o Mapeamento de serviços e os Padrões de descoberta, insira o nome da tabela para o tipo de IC ao qual o IC pertence, por exemplo, cmdb_ci_apache_web_server.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Armazenamento externo de credenciais	Marque esta caixa de seleção para usar um sistema de armazenamento externo de credenciais externas. Quando você seleciona esta opção, os campos **Nome de usuário** e **Senha** são substituídos pelo campo **ID de credencial**. O armazenamento externo de credenciais só está disponível quando o plug-in Armazenamento externo de credenciais está ativado. **Nota:** Atualmente, o único sistema de armazenamento externo compatível é o CyberArk.
Aplica-se a	Selecione se deseja aplicar essas credenciais a **Todos os MID Servers** em sua rede, ou a um ou mais **MID Servers específicos**. Especifique os MID Servers que devem usar essas credenciais no campo **MID Servers**.
MID servers	Selecione um ou mais MID Servers na lista de MID Servers disponíveis. As credenciais configuradas neste registro estão disponíveis para os MID Servers nesta lista. Este campo está disponível somente quando você seleciona **MID Servers específicos** no campo **Aplica-se a**.
Ordem	A ordem (sequência) na qual o Descoberta testa esta credencial ao tentar fazer login nos dispositivos. Quanto menor o número, mais alta será a exibição dessa credencial na lista. Estabeleça a ordem de credenciais ao usar um grande número de credenciais ou quando a segurança bloquear usuários após três tentativas de login com falha. Se todas as credenciais tiverem o mesmo número na ordem (ou número nenhum), a instância vai tentar usar as credenciais em uma ordem aleatória.

Comandos que exigem privilégios de root para Descoberta, Orquestração e Integration Hub

Esses exemplos presumem que o nome de usuário é **Disco**. Substitua o nome de usuário real e certifique-se de que os caminhos dos comandos correspondam aos caminhos no sistema.

Nota: Comandos sudo não funcionam com credenciais de chave privada, porque não há senha para fornecer ao comando sudo. Uma solução é adicionar a opção *NOPASSWD* à configuração do sudo. Por exemplo, você pode inserir: `disco ALL=(root) NOPASSWD:/usr/sbin/dmidecode,/usr/sbin/lsof,/sbin/ifconfig`.

Comandos do UNIX e Linux que exigem privilégios de root

Comando	Finalidade
HP-UX	
adb	Reúne velocidade da CPU e memória. • **/etc/exemplo de sudoers**: Disco ALL=(root) /usr/bin/adb • **Usado por**: Descoberta
Todas as versões do Linux e UNIX	
mudança	Altera o número de dias entre as mudanças de senha e a data da última mudança de senha.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Comandos do UNIX e Linux que exigem privilégios de root

Comando	Finalidade
	• **Exemplo da linha /etc/sudoers**: Disco ALL=(root) /usr/bin/chage • **Usado por**: Orquestração e Integration Hub
chpasswd	Altera as senhas do usuário. • **Exemplo da linha /etc/sudoers**: Disco ALL=(root) /etc/chpasswd • **Usado por**: Orquestração e Integration Hub
Todos os Linux	
dmidecode	Reúne várias informações sobre o hardware, incluindo o número de série incorporado à placa-mãe. • **Exemplo da linha /etc/sudoers**: Disco ALL=(root) /sbin/dmidecode • **Usado por**: Descoberta
fdisk	Reúne os discos e as informações de tamanho no sistema. • **Exemplo da linha /etc/sudoers**: Disco ALL=(root) /usr/bin/fdisk -l • **Usado por**: Descoberta
multipath	Reúne mapeamentos de dispositivo para MPIO. • **Exemplo da linha /etc/sudoers**: Disco ALL=(root) /usr/bin/multipath -ll • **Usado por**: Descoberta
Linux e Solaris	
dmsetup	Examina um volume de nível baixo. • **exemplo de linha /etc/sudoers**: ◦ Disco ALL=(root) /usr/bin/dmsetup table* ◦ Disco ALL=(root) /usr/bin/dmsetup ls • **Usado por**: Descoberta
Todas as versões do UNIX	
lsof	Determina o relacionamento entre os processos e as conexões feitas com o sistema. • **Exemplo da linha /etc/sudoers**: Disco ALL=(root) /sbin/lsof • **Usado por**: Descoberta
oratab	Concede acesso de leitura ao arquivo oratab para localizar a página inicial do Oracle e o pfile.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Comandos do UNIX e Linux que exigem privilégios de root

Comando	Finalidade
	• **Exemplo da linha /etc/sudoers**: N/A • **Usado por**: Descoberta
Solaris	
iscsiadm	Obtém IQNs iSCSI • **Exemplo de linha /etc/sudoers**: $ {sudo: iscsiadm list target -S} • **Usado por**: Descoberta
fcinfo	Obtém WWPNs para portas. • **Exemplo de linha /etc/sudoers**: $ {sudo: fcinfo remote-port -sl -p $port} • **Usado por**: Descoberta
prtvtoc	Relata informações sobre partições de disco. • **Exemplo da linha /etc/sudoers**: Disco ALL=(root) /usr/bin/prtvtoc • **Usado por**: Descoberta
pfiles	Usado para coletar informações de conexões TCP. • **Exemplo da linha /etc/sudoers**: Disco ALL=(root) /usr/bin/pfiles • **Usado por**: Descoberta
pgrep	Usado para listar IDs de processo de uma região específica para executar pfiles. • **Exemplo da linha /etc/sudoers**: Disco ALL=(root) /usr/bin/pgrep • **Usado por**: Descoberta
/usr/bin/ps	Lista o processo em execução. Como alternativa à execução com acesso raiz, adicione uma função proc_owner. • **Exemplo da linha /etc/sudoers**: Disco ALL=(root) /usr/bin/ps • **Usado por**: Descoberta
/usr/ucb/ps	Lista o processo em execução. Como alternativa à execução com acesso raiz, adicione uma função proc_owner.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Comandos do UNIX e Linux que exigem privilégios de root

Comando	Finalidade
	O uso do comando `/usr/ucb/ps` foi descontinuado no Solaris 11. Como Descoberta, Orquestraçãoe Integration Hub exigem o uso deste comando para todas as versões do Solaris, você deve instalar o utilitário ucb manualmente nos sistemas Solaris 11. Para obter instruções, consulte KB0564262. • **Exemplo da linha /etc/sudoers**: Disco ALL=(root) /usr/ucb/ps • **Usado por**: Descoberta

Para obter uma lista de comandos privilegiados necessários para Descoberta e Mapeamento de serviços, consulte Comandos do Mapeamento de serviços que requerem um usuário privilegiado para acessar uma lista dos comandos que exigem direitos elevados para descobrir e mapear hosts baseados em Unix na sua organização.

Requisitos de acesso para credenciais não root

Se você não fornecer credenciais de acesso root a Descoberta, deverá fornecer credenciais com os seguintes requisitos de acesso.

Aplicação	Arquivo ou diretório	Acesso Necessário
Apache	httpd.conf	Leitura
Hbase	hbase-site.xml	Leitura
JBoss	jboss-service.xml	Leitura
	Diretório inicial do JBoss	Leitura
	web.xml	Leitura
MySQL	my.cnf	Leitura
NGINX	nginx.conf	Leitura
Oracle	oratab	Leitura
	Arquivos associados (s)	Leitura
Oracle Listener	lsnrctl	Executar
	listener.ora	Leitura
Tomcat	catalina.jar	Leitura
	server.xml	Leitura
	web.xml	Leitura
Unix	/etc/*release	Leitura
	/ etc / bashrc	Leitura
	/etc/profile	Leitura
	/proc/cpuinfo	Leitura
	/proc/vmware/sched/ncpus	Leitura
	/var/log/dmesg	Leitura

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Aplicação	Arquivo ou diretório	Acesso Necessário
	Diretório APD	Leitura
WebSphere	cell.xml	Leitura
	server.xml	Leitura
	serverindex.xml	Leitura

Credenciais do VMware

O tipo de credenciais do VMware gerencia o acesso às credenciais do vCenter.

As aplicações que acessam recursos de nuvem do VMware precisam de acesso às credenciais do VMware. Por exemplo, o tipo de credencial do VMware permite que a Descoberta explore o vCenter do VMware em execução em uma máquina Windows para descobrir máquinas ESX, máquinas virtuais e grupos de recursos. A API de automação e do VMware Descoberta (API do vCenter) agora fornece o número de série exclusivo globalmente para ICs de computador. As credenciais CIM não são necessárias para permitir o acesso a cada host VMware.

Nota: As credenciais do Windows não são necessárias para Descoberta do vCenter quando credenciais válidas do VMware são usadas.

Importante: Não use credenciais de Tipo **VMware** para atividades do Orquestração que executam trabalho nas máquinas virtuais individuais clonadas pelo vCenter (por exemplo, reiniciar uma VM do Linux). Para essas atividades, o **Tipo** de credencial depende do sistema operacional da máquina virtual (**SSH** ou **Windows**).

Formulário de credenciais do VMWare

Campo	Descrição
Nome	Insira um nome exclusivo e descritivo para as credenciais do VMware.
Ativo	Habilite ou desabilite essas credenciais para uso.
Nome de usuário	Insira o nome de usuário que você usa para sua conta do VMware. Evite espaços iniciais ou finais nos nomes de usuário. Um aviso vai ser exibido se a plataforma detectar espaços iniciais ou finais no nome do usuário. As credenciais do VMware devem ter a função somente leitura no vCenter.
Senha	Insira a senha da conta do VMware.
Aplica-se a	Selecione um ou mais MID Servers na lista de MID Servers disponíveis. As credenciais configuradas neste registro estão disponíveis para MID Servers nesta lista. Este campo está disponível somente quando você seleciona **MID Servers específicos** no campo **Aplica-se a**.
Ordem	A ordem (sequência) na qual o Descoberta testa esta credencial ao tentar fazer login nos dispositivos. Quanto menor o número, mais alta será a exibição dessa credencial na lista. Estabeleça a ordem de credenciais ao usar um grande número de credenciais ou quando a segurança bloquear usuários após três tentativas de login com falha. Se todas as credenciais tiverem o mesmo número na ordem (ou número nenhum), a instância vai tentar usar as credenciais em uma ordem aleatória.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Credenciais do Windows

As credenciais do Windows concedem acesso a computadores Windows. Este tipo de credencial está disponível para Descoberta e Orquestração.

Requisitos de credencial

Descoberta e Orquestração possuem os seguintes requisitos para credenciais Windows:

- Instale um MID Server em um host Windows como um serviço.
- Adicione credenciais Windows a um destes locais:
  - Uma entrada na tabela Credenciais `[windows_credentials]`
  - Uma conta de serviço do MID Server a ser executada como uma conta de domínio ou usuário do Windows específica.

Concedendo permissões apropriadas

Para conceder permissões suficientes, as credenciais Windows devem ser um das seguintes:

- Um usuário de domínio com acesso de administrador local nos hosts de destino Windows.
- Uma conta local que tem privilégios de administrador e UAC (User Access Control) desabilitados no mesmo host de destino.
- Um usuário que atende os requisitos de Windows probes e permissões (Descoberta apenas).
- Um usuário que atende os requisitos da atividade Orquestração a ser executada (Orquestração apenas).

Nota: Nenhum privilégio de logon é necessário. A conta NÃO precisa ser interativa.

A segurança em torno da concessão de acesso privilegiado pode ser aprimorada usando perfis JEA para executar Descoberta. Para obter mais informações, consulte JEA (Microsoft Just Enough Administration) para Descoberta.

Computadores do grupo de trabalho

Para executar comandos do Powershell para descobrir um computador do Grupo de trabalho, configure as credenciais do MID Server para um desses usuários:

- Conta de administrador interna no computador do Grupo de trabalho.
- Usuário do domínio no computador do Grupo de trabalho.

Configuração de vários domínios

Para habilitar as credenciais do Windows para funcionar em vários domínios, certifique-se de usar os formatos de nome e a configuração do MID Server corretos.

Descoberta e Orquestração suportamWindows credenciais de domínio em ambos os formatos de nome de usuário **Nome principal do usuário** e **Nome de login de nível inferior**. Por exemplo, **Domain\UserName** ou **UserName@example.domain.com**. É possível fornecer credenciais de grupo de trabalho Windows no seguinte formato: WORKGROUP\UserName.

Nota: Também é possível fornecer uma conta local usando o nome de usuário `.\`.

Essas ações adicionais são necessárias para habilitar as credenciais para funcionar em vários domínios Windows.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Condição	Ações adicionais necessárias
Host MID Server no mesmo domínio que o destino Windows.	Nenhum
Host MID Server em um domínio diferente do destino Windows.	Certifique-se de que PowerShell 3.0 (ou superior até 5.1) esteja instalado no host MID Server.
O host MID Server em um domínio diferente do destino Microsoft SQL Server.	Consulte Descoberta do servidor MSSQL.

Tipo de credenciais do Windows

Esses campos estão disponíveis no formulário Credenciais para Windows:

Campo	Descrição
Nome	Insira um nome exclusivo e descritivo para esta credencial.
Ativo	Habilite ou desabilite essas credenciais para uso.
Nome de usuário	Insira o nome de usuário a ser criado na tabela Credenciais. Evite espaços iniciais ou finais em nomes de usuário. Um aviso vai ser exibido se a plataforma detectar espaços iniciais ou finais no nome de usuário. Para a descoberta CIM, o usuário deve ter a função de administrador.
Senha	Insira a senha.
ID da Credencial	Insira a chave exclusiva configurada para credenciais externas no arquivo JAR carregado no MID Server para um sistema de credenciais externas. O campo **ID de credencial** tem um limite de 40 caracteres. Este campo só estará visível quando a caixa de seleção **Armazenamento de credenciais externas** estiver marcada.
Alias de credencial	Permita que os criadores do fluxo de trabalho atribuam credenciais individuais a qualquer atividade em um fluxo de trabalho do Orquestração ou atribuam credenciais diferentes a cada ocorrência do mesmo tipo de atividade em um fluxo de trabalho do Orquestração. Para usar a credencial para descobrir ICs que não pertencem a este tipo de IC usando o Mapeamento de serviços e os Padrões de descoberta, insira o nome da tabela para o tipo de IC ao qual o IC pertence, por exemplo, cmdb_ci_apache_web_server.
Armazenamento externo de credenciais	Marque esta caixa de seleção para usar um sistema de armazenamento externo de credenciais externas. Quando você seleciona esta opção, os campos **Nome de usuário** e **Senha** são substituídos pelo campo **ID de credencial**. O armazenamento externo de credenciais só está disponível quando o plug-in Armazenamento externo de credenciais está ativado. **Nota:** Atualmente, o único sistema de armazenamento externo compatível é o CyberArk.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Aplica-se a	Selecione se deseja aplicar essas credenciais a **Todos os MID Servers** em sua rede, ou a um ou mais **MID Servers específicos**. Especifique os MID Servers que devem usar essas credenciais no campo **MID Servers**.
MID servers	Selecione um ou mais MID Servers na lista de MID Servers disponíveis. As credenciais configuradas neste registro estão disponíveis para os MID Servers nesta lista. Este campo está disponível somente quando você seleciona **MID Servers específicos** no campo **Aplica-se a**. **Nota:** Selecionar **MID Servers específicos** não afeta a seleção do MID Server. Ele é usado somente para decidir quais MID Servers devem ter visibilidade para a credencial. **MID Servers específicos** não são compatíveis com atividades do Orquestração.
Ordem	A ordem (sequência) na qual o Descoberta testa esta credencial ao tentar fazer login nos dispositivos. Quanto menor o número, mais alta será a exibição dessa credencial na lista. Estabeleça a ordem de credenciais ao usar um grande número de credenciais ou quando a segurança bloquear usuários após três tentativas de login com falha. Se todas as credenciais tiverem o mesmo número na ordem (ou número nenhum), a instância vai tentar usar as credenciais em uma ordem aleatória.
Conta de serviço Windows MID Server	Quando ativa, a credencial definida representa a conta de serviço do MID Server.

Configurar credenciais do Windows para o MID Server

Configure o MID Server para usar as credenciais de seu próprio serviço Windows ou as credenciais da tabela Credentials [discovery_credentials].

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Configure o MID Server para usar credenciais da conta de serviço do MID Server.
   a. Defina Configurar credenciais de serviço do Windows MID Server para um usuário que atende aos requisitos de permissão.
   b. Verifique se o nome de usuário atende aos requisitos de formato de nome.
   c. Preencha os campos no formulário, conforme apropriado.
   d. Verifique se as credenciais atendem aos requisitos de domínio.
2. Configure o MID Server para usar credenciais da tabela Credenciais [discovery_credentials].

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Adicione as credenciais Windows individuais para a tabela Credenciais `[windows_credentials]`.
   - Verifique se cada credencial atende aos requisitos de permissão.
   - Verifique se cada nome de usuário atende aos requisitos de formato de nome.
   - Verifique se cada credencial atende aos requisitos de domínio Windows.

b. Opcional: Configure o MID Server para usar o Powershell configurando o parâmetro `mid.use_powershell` para **verdadeiro**.
   Consulte Configurar MID Servers.

c. Marque a caixa de seleção da Conta de serviço do Windows MID Server para criar uma credencial que representa a conta de serviço windows MID Server a ser executada como uma conta específica de domínio ou de usuário do Windows.

Credenciais do repositório de imagens do contêiner

As credenciais do repositório de imagens do contêiner gerenciam o acesso aos repositórios privados para fins de verificação das imagens do contêiner. Esse tipo de credencial está disponível para Descoberta.

Estes campos estão disponíveis no formulário "Credenciais" para as credenciais do tipo de repositório de imagens do contêiner.

Formulário de credenciais do repositório de imagens do contêiner

Campo	Descrição
Nome	Nome da credencial atribuída ao usuário.
Nome de usuário	Nome de usuário com permissões de leitura para o repositório.
Senha	Senha com permissões de leitura para o repositório.
Repositório	Nome de domínio totalmente qualificado do repositório. Por exemplo: `docker.io/snow_images`.

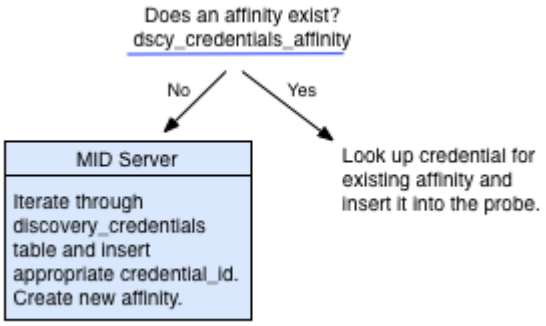
Afinidade de credencial para Descoberta e Orquestração

A afinidade de credencial é uma associação entre um conjunto de credenciais e um dispositivo em sua rede.

Quando o Descoberta ou a Orquestração tenta acessar primeiro um dispositivo, eles tentam todas as credenciais disponíveis até encontrar as corretas. Depois de identificar as credenciais para um dispositivo, o Descoberta e a Orquestração criam uma afinidade entre as credenciais e o dispositivo que usa a tabela Afinidade de credencial `[dscy_credentials_affinity]`. Todas as descobertas subsequentes ou atividades da Orquestração tentam corresponder as credenciais nesta tabela a um dispositivo para o qual existe uma afinidade. Se as credenciais de um dispositivo forem alteradas, o Descoberta e a Orquestração tentarão todas as credenciais disponíveis novamente até criarem uma nova afinidade.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Diagrama de afinidade de credenciais



Nota: Se a Orquestração e o Descoberta estiverem instalados e o alias de credencial estiver habilitado, poderão existir várias afinidades. Nesse caso, a plataforma pesquisa as credenciais de cada afinidade e insere a credencial da afinidade com a ordem mais baixa no probe.

Solução de problemas de credenciais

Analise a seção `<credentials_debug>` da carga da fila do ECC para resolver problemas com as credenciais.

Determinadas probes suportam depuração de credencial. A depuração de credenciais insere uma seção `<credentials_debug>` na carga que o MID Server retorna à fila do ECC de instância. É possível exibir a seção `<credentials_debug>` para ver as informações detalhadas sobre a pesquisa de credenciais.

A seção `<credentials_debug>` aparece na carga se:

- Falha nas credenciais do probe WMIRunner, probe PowerShell, JMS ou probe SSHCommand.
- Defina o parâmetro *`credentials_debug`* como **verdadeiro** para as probes WMIRunner, PowerShell ou SSHCommand. Se definir o parâmetro como verdadeiro, a seção `<credentials_debug>` aparecerá mesmo se a pesquisa de credenciais for bem sucedida.

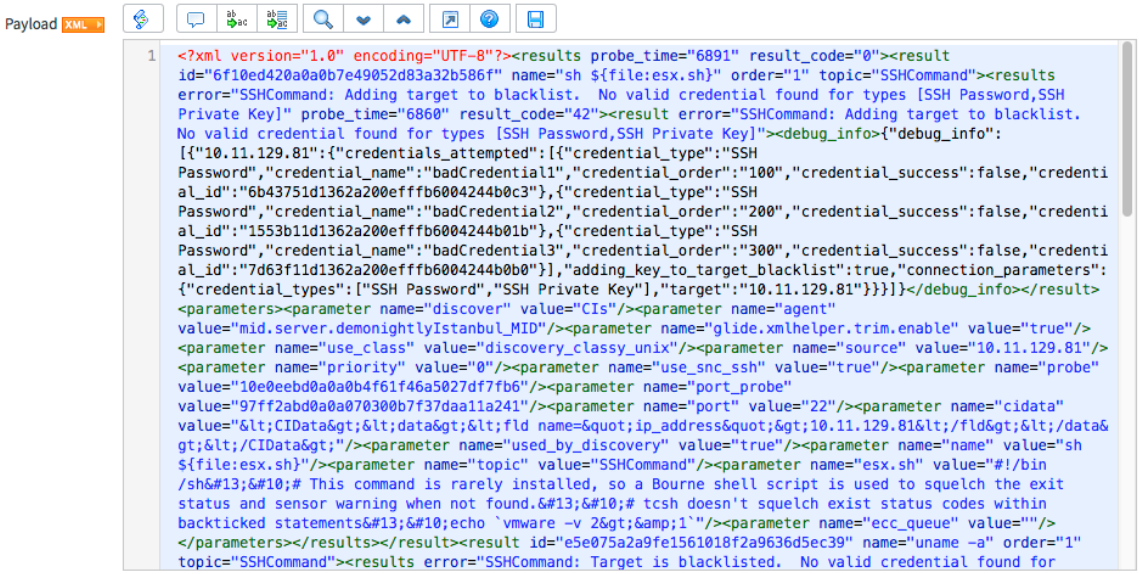
A seção `<credentials_debug>` mostra:

- Informações sobre a pesquisa de credencial, tais como tipos de credencial, marcadores e afinidades.
- O endereço IP de destino.
- Informações sobre cada credencial (em ordem) que o MID Server usou, incluindo o tipo, a classificação, o marcador, o nome, o ID Sys e o ID de credencial externo, se presente.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Carga de amostra exibindo as credenciais inválidas

Payload XML




```
<?xml version="1.0" encoding="UTF-8"?><results probe_time="6891" result_code="0"><result
id="6f10ed420a0a0b7e49052d83a32b586f" name="sh ${file:esx.sh}" order="1" topic="SSHCommand"><results
error="SSHCommand: Adding target to blacklist.  No valid credential found for types [SSH Password,SSH
Private Key]" probe_time="6860" result_code="42"><result error="SSHCommand: Adding target to blacklist.
No valid credential found for types [SSH Password,SSH Private Key]"><debug_info>{"debug_info":
[{"10.11.129.81":{"credentials_attempted":[{"credential_type":"SSH
Password","credential_name":"badCredential1","credential_order":"100","credential_success":false,"credenti
al_id":"6b43751d1362a200efffb6004244b0c3"},{"credential_type":"SSH
Password","credential_name":"badCredential2","credential_order":"200","credential_success":false,"credenti
al_id":"1553b11d1362a200efffb6004244b01b"},{"credential_type":"SSH
Password","credential_name":"badCredential3","credential_order":"300","credential_success":false,"credenti
al_id":"7d63f11d1362a200efffb6004244b0b0"}],"adding_key_to_target_blacklist":true,"connection_parameters":
{"credential_types":["SSH Password","SSH Private Key"],"target":"10.11.129.81"}}}]}</debug_info></result>
<parameters><parameter name="discover" value="CIs"/><parameter name="agent"
value="mid.server.demonightlyIstanbul_MID"/><parameter name="glide.xmlhelper.trim.enable" value="true"/>
<parameter name="use_class" value="discovery_classy_unix"/><parameter name="source" value="10.11.129.81"/>
<parameter name="priority" value="0"/><parameter name="use_snc_ssh" value="true"/><parameter name="probe"
value="10e0eebd0a0a0b4f61f46a5027df7fb6"/><parameter name="port_probe"
value="97ff2abd0a0a070300b7f37daa11a241"/><parameter name="port" value="22"/><parameter name="cidata"
value="&lt;CIData&gt;&lt;data&gt;&lt;fld name=&quot;ip_address&quot;&gt;10.11.129.81&lt;/fld&gt;&lt;/data&
gt;&lt;/CIData&gt;"/><parameter name="used_by_discovery" value="true"/><parameter name="name" value="sh
${file:esx.sh}"/><parameter name="topic" value="SSHCommand"/><parameter name="esx.sh" value="#!/bin
/sh&#13;&#10;# This command is rarely installed, so a Bourne shell script is used to squelch the exit
status and sensor warning when not found.&#13;&#10;# tcsh doesn't squelch exist status codes within
backticked statements&#13;&#10;echo `vmware -v 2&gt;&amp;1`"/><parameter name="ecc_queue" value=""/>
</parameters></results></result><result id="e5e075a2a9fe1561018f2a9636d5ec39" name="uname -a" order="1"
topic="SSHCommand"><results error="SSHCommand: Target is blacklisted.  No valid credential found for
```


Detalhes aparecem para o parâmetro do PowerShell:

- Se as credenciais do MID Server local foram usadas depois que todas as credenciais do Windows falharam.
- Se as credenciais foram ignoradas porque você está tentando descobrir a mesma máquina em que está o MID Server.
- Se o parâmetro mid.powershell.use_credentials estiver definido como `verdadeiro`.

Detalhes aparecem para o SSHCommand:

- Se a pesquisa de credencial foi ignorada porque o IP de destino foi excluído.
- Se o IP de destino foi adicionado à lista de exclusões.

Nota: O MID Server salva os endereços IP para pesquisas de credencial que falharam em uma lista de exclusões na memória cache. Esta lista de exclusões especifica quais dispositivos o MID Server devem parar de tentar acessar. Os endereços IP são adicionados à lista de exclusões após a falha de cada credencial. Os endereços IP são limpos do cache da lista de exclusões após cinco minutos, se o MID Server for reiniciado ou se os registros de credencial na instância forem atualizados.

Armazenamento externo de credenciais

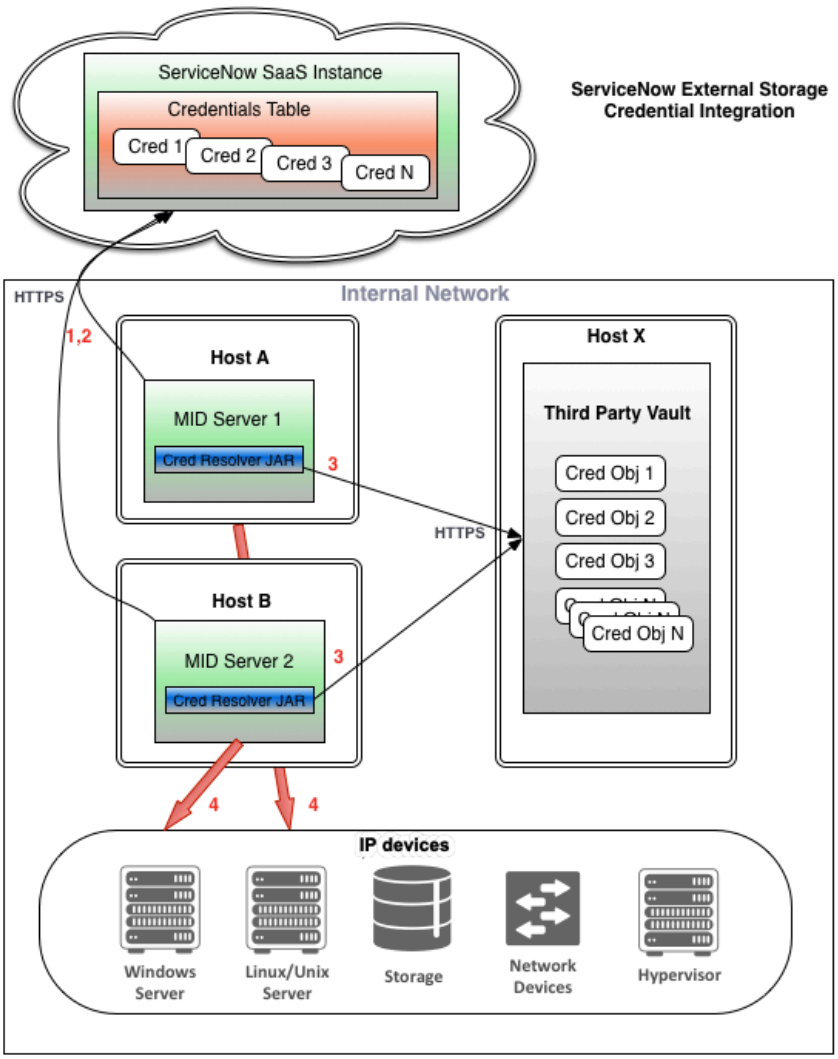
Uma instância pode armazenar credenciais usadas por Descoberta, Orquestração e Mapeamento de serviços em um repositório de credencial externo em vez de diretamente em um registro de credenciais ServiceNow.

A instância mantém um identificador exclusivo para cada credencial, o tipo de credencial (como SSH, SNMP ou Windows) e todas as afinidades de credencial. O MID Server obtém o identificador de credencial da instância e usa um arquivo JAR fornecido pelo cliente para resolver o identificador do repositório em uma credencial utilizável. Atualmente, a plataforma ServiceNow® dá suporte ao uso do cofre do CyberArk ou BeyondTrust para armazenamento externo de credenciais.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Arquitetura de armazenamento externo de credenciais

Arquitetura de armazenamento externo de credenciais



Fluxo do processo de credencial

O MID Server recupera as credenciais de um armazenamento externo usando este processo:

1. O MID Server baixa objetos de credencial da tabela ServiceNow Credenciais [discovery_credentials] que contêm o ID de credencial correspondente a partir do cofre de destino.
2. Conforme cada probe ou padrão é executado a partir de trabalhos Descoberta ou Orquestração, o MID Server solicita a credencial passando informações como ID de credencial, endereço IP de destino e tipo de credencial para o arquivo Java JAR do Resolvedor de credencial. Os detalhes sobre o objeto de credencial correto a ser recuperado do cofre são determinados pelo Resolvedor de Credencial.

   Muitos Resolvedores de Credencial, como o CyberArk, chamam uma aplicação fornecida pelo fornecedor do cofre de terceiros em execução na mesma máquina do MID Server. esse aplicativo geralmente pode ser configurada para armazenar credenciais em cache e sabe como atualizar o cache quando uma credencial muda no cofre, o que é muito importante para evitar chamadas de rede desnecessárias para o cofre cada

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

vez que o MID Server solicita uma credencial. O Resolvedor de Credencial (usando a aplicação opcional do fornecedor, se presente) faz uma chamada para o cofre para obter o nome de usuário real, a senha etc.

Para Resolvedores de credenciais fornecidos prontos para uso (somente a CyberArk hoje), o MID Server somente armazena em cache uma credencial por até vários segundos usando criptografia na memória do processo do MID Server. Isso significa que o MID Server pode fazer várias solicitações ao Resolvedor de credencial para a mesma credencial, mesmo ao descobrir um único dispositivo. Contate fornecedores de terceiros para obter informações sobre implementações de cache para outros Resolvedores de credencial.

3. O MID Server executa a probe com a credencial apropriada.

Nota: A afinidade de credencial ainda se aplica. O mecanismo permanece o mesmo, já que a única diferença real da perspectiva do MID Server é que os detalhes reais das credenciais (nome de usuário e senha) vêm do cofre de terceiros.

Log de armazenamento de credenciais externas

O MID Server publica mensagens de log sobre o armazenamento externo de credenciais.

Se o repositório encontrar um erro ao tentar resolver uma solicitação de credenciais, o MID Server publicará mensagens de log com este prefixo: `Problem with client's CredentialResolver:`

Componentes instalados com Armazenamento externo de credenciais

Regra de negócios

A regra de negócio de armazenamento externo de credenciais executa as seguintes tarefas quando um administrador faz alguma mudança na propriedade Habilitar armazenamento externo de credenciais:

- Altera a exibição da lista de registros de credenciais e do formulário para a exibição Armazenamento externo. Esta exibição permite que os usuários vejam a coluna **ID de credencial** na lista.
- Instrui o MID Server a atualizar o cache de credenciais em preparação para uma mudança na maneira como as credenciais são obtidas.

Propriedade

Uma propriedade chamada Habilitar armazenamento externo de credenciais [com.snc.use_external_credentials] habilita ou desabilita o plug-in Armazenamento externo de credenciais depois que ele é ativado. A propriedade está localizada em**Definição da Descoberta** > **Propriedades**e **Orquestração** > **Propriedades do MID Server**, e é habilitada quando você ativa o plug-in.

Se você desabilitar o armazenamento externo de credenciais com a propriedade do sistema, o sistema definirá automaticamente todas as credenciais externas para inativas na instância. Se você reativar o recurso com esta propriedade, o sistema não redefinirá os registros de credenciais externas para ativos. Você deve reativar cada registro de credencial manualmente.

Solicite armazenamento externo de credenciais para Descoberta e Orquestração

O plug-in Armazenamento externo de credenciais está disponível por solicitação.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Função necessária: administrador

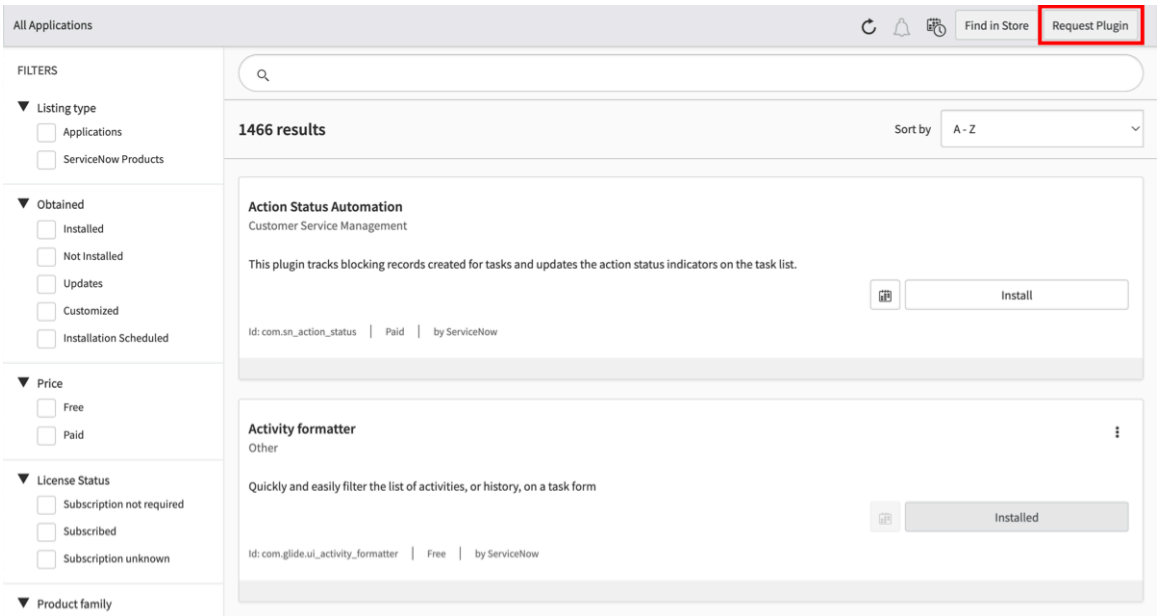
Por Que e Quando Desempenhar Esta Tarefa

Existem duas maneiras de solicitar um plug-in:

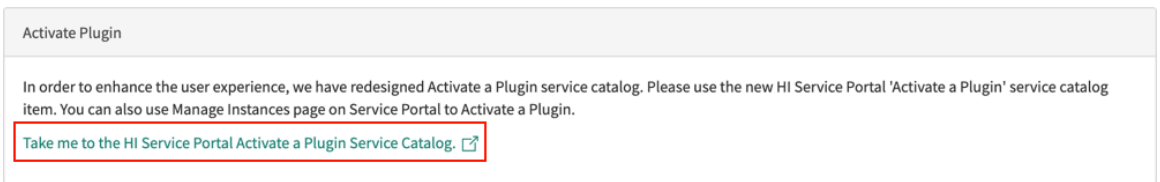
- Acesse o Now Support Catálogo de serviços diretamente clicando em **Todos** > **Catálogo de serviços** > **Ativar plug-in** no Now Support.
- Acesse o Now Support Catálogo de serviços por meio da página Todos os Aplicativos em sua instância, seguindo estas etapas.

Procedimento

1. Navegue até **Todas** > **Aplicações do sistema** > **Todas os aplicações disponíveis** > **Todas**.
2. Na página Todas as Aplicações, selecione **Solicitar plug-in** para abrir o formulário **Ativar plug-in** em Now Support.



3. No Now Support, selecione o link para acessar o Now Support Portal de serviços Catálogo de serviços.



4. Selecione sua instância.
5. Selecione **Ações > Ativar plug-in**.
6. No formulário **Ativar plug-in**, forneça as seguintes informações.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

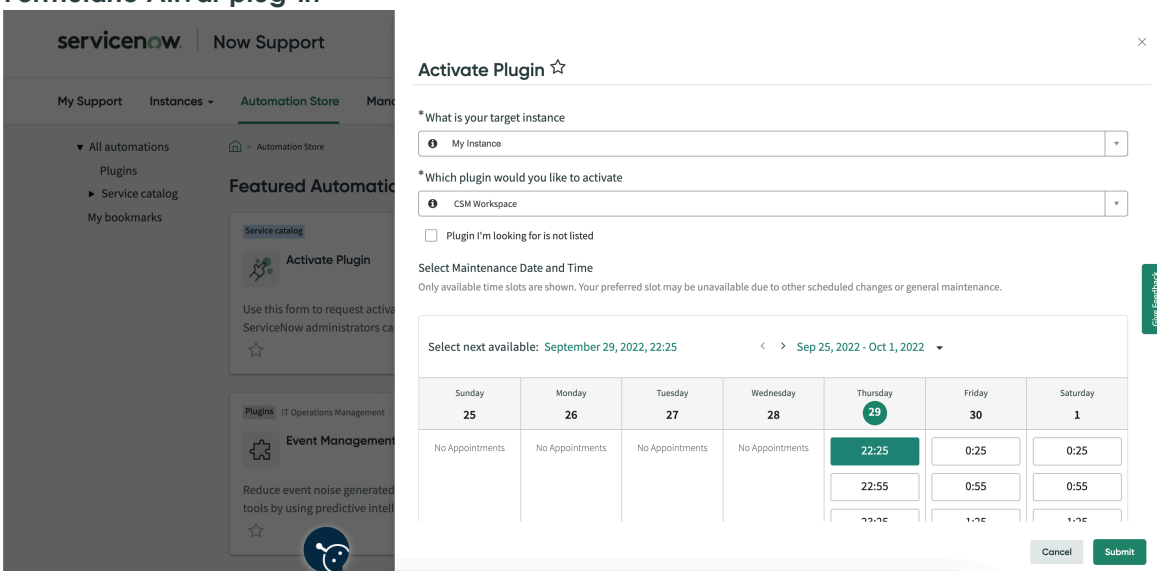
Formulário Ativar plug-in

Campo	Descrição
Qual é a sua instância de destino	Instância na qual o plug-in será ativado.
Qual plug-in você deseja ativar	Nome do plug-in a ser ativado. **Nota:** Se o sistema não listar o plug-in desejado ou se você estiver ativando o plug-in em uma instância do OEM ou no local, marque a caixa de seleção O **plug-in que estou procurando não está listado** e insira o nome do plug-in.
Selecionar data e hora de manutenção	A data e a hora para ativar o plug-in. **Nota:** Os plug-ins são ativados em dois lotes, uma pela manhã e outra à noite, em todos os dias úteis no fuso horário do Pacífico dos EUA. Se o plug-in deve ser ativado em um momento específico, insira a solicitação no campo **Motivo/ Comentários**.

Example

Por exemplo, consulte o formulário a seguir para ativar o plug-in Espaço de trabalho CSM em uma instância chamada Minha instância.

Formulário Ativar plug-in



© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

7. Selecione **Enviar**.
   Para obter detalhes adicionais sobre como solicitar um plug-in, consulte Solicitar um plug-in no artigo do Catálogo de serviços [KB0751715] em Now Support Base de conhecimento.

Configuração de armazenamento externo de credenciais

Configure a sua instância para obter credenciais de um repositório remoto.

Esses procedimentos assumem que você já tenha um repositório externo configurado com as credenciais que deseja proteger. O identificador de credencial configurado na instância ServiceNow deve ser mapeado para a credencial real no repositório através do arquivo JAR.

Nota: A ServiceNow oferece suporte a dois cofres externos por vez: um resolvedor de credencial padrão CyberArk e um resolvedor de credencial externo personalizado. Para criar um resolvedor de credencial personalizado CyberArk, ainda é necessário usar o segundo cofre externo personalizado. Além disso, nenhum cofre externo personalizado pode ser usado.

Para configurar o Armazenamento externo de credenciais, conclua as tarefas a seguir em ordem.

Crie um arquivo JAR para resolver credenciais

Crie um arquivo JAR para resolver identificadores de credenciais enviados do MID Server para credenciais reais do repositório.

Antes de Iniciar

Função necessária: agent_admin ou admin

Certifique-se de incluir todos os elementos de credencial que a instância espera, como a chave privada.

Para criar um arquivo JAR para resolver as credenciais:

Procedimento

Use os modelos fornecidos no github ServiceNow ou no arquivo Java de amostra.

CUIDADO: Essas amostras são apenas um modelo. **NÃO** use este código em produção sem modificá-lo para o seu ambiente.

a. Baixe os arquivos JAR de código aberto com instruções do github ServiceNow:
   - Resolvedor de credencial externa da HashiCorp
   - Resolvedor de credencial externa da CyberArk

b. Use o seguinte arquivo Java de amostra como modelo e modifique-o para se adequar ao seu ambiente:

Example

```
package com.snc.discovery;

import java.util.*;
import java.io.*;
```

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

```
/**
 * Basic implementation of a CredentialResolver that uses a properties
 file.
 */

public class CredentialResolver {

 private static String ENV_VAR = "CREDENTIAL_RESOLVER_FILE";
 private static String DEFAULT_PROP_FILE_PATH =
 "C:\\dummycredentials.properties";

 // These are the permissible names of arguments passed INTO the
 resolve()
 // method.

 // the string identifier as configured on the ServiceNow instance...
 public static final String ARG_ID = "id";

 // a dotted-form string IPv4 address (like "10.22.231.12") of the
 target
 // system...
 public static final String ARG_IP = "ip";

 // the string type (ssh, snmp, etc.) of credential as configured on
 the
 // instance...
 public static final String ARG_TYPE = "type";

 // the string MID server making the request, as configured on the
 // instance...
 public static final String ARG_MID = "mid";

 // These are the permissible names of values returned FROM the
 resolve()
 // method.

 // the string user name for the credential, if needed...
 public static final String VAL_USER = "user";

 // the string password for the credential, if needed...
 public static final String VAL_PSWD = "pswd";

 // the string pass phrase for the credential if needed:
 public static final String VAL_PASSPHRASE = "passphrase";

 // the string private key for the credential, if needed...
 public static final String VAL_PKEY = "pkey";

 // the string authentication protocol for the credential, if needed...
 public static final String VAL_AUTHPROTO = "authprotocol";

 // the string authentication key for the credential, if needed...
 public static final String VAL_AUTHKEY = "authkey";

 // the string privacy protocol for the credential, if needed...
 public static final String VAL_PRIVPROTO = "privprotocol";
```

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

```
// the string privacy key for the credential, if needed...
public static final String VAL_PRIVKEY = "privkey";


private Properties fProps;

public CredentialResolver() {
}

private void loadProps() {
 if(fProps == null)
  fProps = new Properties();

 try {
  String propFilePath = System.getenv(ENV_VAR);
  if(propFilePath == null) {
   System.err.println("Environment var "+ENV_VAR+" not found. Using
default file: "+DEFAULT_PROP_FILE_PATH);
   propFilePath = DEFAULT_PROP_FILE_PATH;
  }

  File propFile = new File(propFilePath);
  if(!propFile.exists() || !propFile.canRead()) {
   System.err.println("Can't open "+propFile.getAbsolutePath());
  }
  else {
   InputStream propsIn = new FileInputStream(propFile);
   fProps.load(propsIn);
  }

//fProps.load(CredentialResolver.class.getClassLoader().getResourceAsS
tream("dummycredentials.properties"));
 } catch (IOException e) {
  System.err.println("Problem loading credentials file:");
  e.printStackTrace();
 }
}

/**
 * Resolve a credential.
 */
public Map resolve(Map args) {
 loadProps();
 String id = (String) args.get(ARG_ID);
 String type = (String) args.get(ARG_TYPE);
 String keyPrefix = id+"."+type+".";

 if(id.equalsIgnoreCase("misbehave"))
  throw new RuntimeException("I've been a baaaaaaaaad
CredentialResolver!");

 // the resolved credential is returned in a HashMap...
 Map result = new HashMap();
 result.put(VAL_USER, fProps.get(keyPrefix + VAL_USER));
 result.put(VAL_PSWD, fProps.get(keyPrefix + VAL_PSWD));
 result.put(VAL_PKEY, fProps.get(keyPrefix + VAL_PKEY));
```

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

```
  result.put(VAL_PASSPHRASE, fProps.get(keyPrefix + VAL_PASSPHRASE));
  result.put(VAL_AUTHPROTO, fProps.get(keyPrefix + VAL_AUTHPROTO));
  result.put(VAL_AUTHKEY, fProps.get(keyPrefix + VAL_AUTHKEY));
  result.put(VAL_PRIVPROTO, fProps.get(keyPrefix + VAL_PRIVPROTO));
  result.put(VAL_PRIVKEY, fProps.get(keyPrefix + VAL_PRIVKEY));

  System.err.println("Error while resolving credential
 id/type["+id+"/"+type+"]");

  return result;
 }


 /**
  * Return the API version supported by this class.
  */
 public String getVersion() {
  return "1.0";
 }

 public static void main(String[] args) {
  CredentialResolver obj = new CredentialResolver();
  obj.loadProps();

  System.err.println("I spy the following credentials: ");
  for(Object key: obj.fProps.keySet()) {
   System.err.println(key+": "+obj.fProps.get(key));
  }

 }
}
```

Importe um arquivo JAR para resolver credenciais

Importe um arquivo JAR criado para resolver identificadores de credencial enviados do MID Server para credenciais reais do repositório.

Antes de Iniciar

Função necessária: agent_admin ou admin

Depois de criar o arquivo JAR, importe-o na instância, onde ele se torna acessível ao MID Server.

Procedimento

1. Depois de criar o JAR e arquivos de propriedades, copie o arquivo de propriedades para o MID Server.
2. Navegue até **MID Server** > **Arquivos JAR**.
3. Clique em **Nova**.
4. Preencha os seguintes campos:

Campo	Descrição
Nome	Um nome exclusivo e descritivo para identificar o arquivo na instância.
Versão	Um número de versão para o arquivo, se houver uma disponível.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Fonte	Local do arquivo JAR para fins de referência. As informações de origem não são usadas pelo sistema.
Descrição	Descrição resumida do arquivo JAR e seu propósito na instância.

5. Clique no ícone de clipe de papel na faixa e anexe o arquivo JAR ao registro.

Example

Anexação de um arquivo JAR

6. Clique em **Enviar**.
7. Reinicie o serviço do MID Server.
   A plataforma disponibiliza o arquivo JAR para qualquer MID Server configurado para se comunicar com a instância.

Configure o identificador de credencial

Configure o identificador de credencial na instância.

Antes de Iniciar

Função necessária: administrador
Verifique os seguintes itens:

- O plug-in Armazenamento externo de credenciais deve estar ativo.
- A propriedade Descoberta Habilitar armazenamento externo de credenciais está habilitada.

Procedimento

1. Navegue até **Todos** > **Descoberta** > **Credenciais** ou **Orquestração** > **Credenciais**.
2. Clique em **Nova**.
3. Selecione um tipo de credencial.
4. Marque a caixa de seleção **Armazenamento de credenciais externas**.
   Os campos **Nome de usuário** e **Senha** desaparecem e o campo **ID de credencial** e o menu **Cofre de armazenamento de credencial** aparecem.
5. No menu do **Cofre de armazenamento de credenciais**, selecione Nenhum, o cofre CyberArk ou um cofre de armazenamento externo de credenciais personalizado.

Nota:

Se o cofre do CyberArk for selecionado, o menu **Chave de pesquisa** aparecerá com quatro opções de chave de pesquisa: "ID da credencial", "Endereço IP", "FQDN" e "Todas a opções acima". Selecionar Todas as opções acima pode prejudicar o desempenho porque requer o acesso ao cofre várias vezes.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Para usar um cofre de armazenamento de credenciais externas personalizado, navegue até Configurações de cofre [vault_configuration.list] na instância.

b. Crie um novo registro usando um nome associado a um arquivo JAR importado para um resolvedor de credenciais personalizado.

Consulte os procedimentos Crie um arquivo JAR para resolver credenciais e Importe um arquivo JAR para resolver credenciais para obter informações sobre a criação de um cofre de armazenamento externo de credenciais personalizado.

6. Preencha o formulário Credenciais usando os campos da seguinte tabela.

Campo	Descrição
Nome	Insira um nome exclusivo e descritivo para esta credencial.
Ativo	Habilite ou desabilite essas credenciais para uso.
ID da Credencial	Insira a chave exclusiva configurada para credenciais externas no arquivo JAR carregado no MID Server para um sistema de credenciais externas. Este é o ID passado para a classe Java no mapa de parâmetros: `public static final String ARG_ID   = "id";` O MID Server usa este identificador para resolver as credenciais reais no repositório. **Nota:** Este campo só está visível quando a caixa de seleção **Armazenamento de credenciais externas** está marcada.
Marcador	Permita que os criadores do fluxo de trabalho atribuam credenciais individuais a qualquer atividade em um fluxo de trabalho do Orquestração ou atribuam credenciais diferentes a cada ocorrência do mesmo tipo de atividade em um fluxo de trabalho do Orquestração.
Armazenamento externo de credenciais	Marque esta caixa de seleção para usar um sistema de armazenamento externo de credenciais externas. Quando você seleciona esta opção, os campos **Nome de usuário** e **Senha** são substituídos pelo campo **ID de credencial**. O Armazenamento externo de credenciais fica disponível apenas quando o plug-in Armazenamento externo de credenciais está ativado.
Cofre de armazenamento de credenciais	Escolha o cofre de Armazenamento externo de credenciais em uma lista de cofres disponíveis. O menu é composto por registros das Configurações do cofre [vault_configuration.list]. Novos registros podem ser adicionados e usar nomes associados aos arquivos JAR do resolvedor de credencial personalizado. Consulte os procedimentos Crie um arquivo JAR para resolver credenciais e Importe um arquivo JAR para resolver credenciais para obter informações sobre a criação de um cofre de armazenamento externo de credenciais personalizado.
Aplica-se a	Selecione se deseja aplicar essas credenciais a **Todos os MID Servers** em sua rede, ou a um ou mais **MID Servers específicos**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Especifique os MID Servers que devem usar essas credenciais no campo **MID Servers**.
MID servers	Selecione um ou mais MID Servers na lista de MID Servers disponíveis. As credenciais configuradas neste registro estão disponíveis para os MID Servers nesta lista. Este campo está disponível somente quando você seleciona **MID Servers específicos** no campo **Aplica-se a**.
Ordem	Insira a ordem (sequência) na qual a plataforma testa esta credencial ao tentar fazer login nos dispositivos. Quanto menor o número, mais alta será a exibição dessa credencial na lista. Estabeleça a ordem de credenciais ao usar um grande número de credenciais ou quando a segurança bloquear usuários após três tentativas de login com falha. Se todas as credenciais tiverem o mesmo número de ordem (ou nenhum), a Descoberta ou a Orquestração tentarão usar as credenciais em uma ordem aleatória.

7. Clique em **Enviar**.

Configure o identificador de credencial para AWS

Configure a sua instância para obter credenciais de um repositório remoto.

Antes de Iniciar

Função necessária: cloud_admin

Verifique se esses plug-ins estão ativos e se o MID Server foi instalado:

- Descoberta [com.snc.discovery]
- Cloud Provisioning and Governance [com.snc.cloud.mgmt]
- Armazenamento externo de credenciais [com.snc.discovery.external_credentials]

Por Que e Quando Desempenhar Esta Tarefa

Esses procedimentos assumem que você já tenha um repositório externo configurado com as credenciais que deseja proteger. O identificador de credencial configurado na instância ServiceNow deve ser mapeado para a credencial real no repositório através do arquivo JAR.

Procedimento

1. Navegue até **Todos** > **Descoberta** > **Credenciais**.
2. Selecione uma credencial suportada por seu provedor de armazenamento externo de credenciais.
3. Preencha o formulário, usando os campos da tabela.

Campo	Descrição
Nome	Um nome exclusivo e descritivo desta credencial. Por exemplo, Amazon Web Services.
Aplica-se a	Selecione os MID Servers que podem usar essas credenciais. As opções são **Todos os MID Servers** ou **MID Servers específicos**. Se você selecionar o último, aparecerá o campo **MID Servers**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Ativo	Marque a caixa para habilitar ou desabilitar a credencial.
Conta da AWS	Insira seu ID de conta AWS se suas credenciais AWS estiverem em um provedor de armazenamento externo.
Servidores MID	Selecione um ou mais MID Servers que podem usar essas credenciais.
ID da Credencial	Insira o Nome sob o qual esta credencial está armazenada no provedor de Armazenamento externo de credenciais.
ID de credencial de privacidade	Insira o nome de uma chave de privacidade SNMPv3 da CyberArk. Este campo fica visível apenas para SNMPv3 quando você selecionar a **CyberArk** do campo **Tipo de armazenamento de credencial**. Se você não estiver usando uma chave de privacidade para CyberArk, deixe este campo em branco.
Alias de credencial	Selecione um alias para esta credencial que contenha comportamentos específicos. Consulte Aliases de credencial da Descoberta para obter mais informações.
Armazenamento externo de credenciais	Marque esta caixa de seleção para usar um sistema de armazenamento externo de credenciais externas. Quando o armazenamento externo está habilitado, aparece o campo **ID de credencial**. Se esta caixa de seleção não estiver visível, clique no ícone de menu na barra de cabeçalho e selecione **Exibir** > **Armazenamento externo** no menu de contexto.
Tipos de armazenamentos de credenciais	Selecione **CyberArk** somente se estiver usando uma chave de privacidade CyberArk SNMPv3. O campo **ID de credencial de privacidade** aparece para permitir a entrada da chave.

4. Clique em **Enviar**.

CyberArk integração de armazenamento de credenciais

A integração MID Server com o cofre CyberArk permite que ServiceNow® Orquestração, ServiceNow® Descoberta e ServiceNow® Mapeamento de serviços sejam executados sem armazenar qualquer credencial na instância.

Introdução para CyberArk

O produto CyberArk AIM (Application Identity Management) usa a solução Privileged Account Security para eliminar a necessidade de senhas do aplicativo da loja integradas em aplicações, scripts ou arquivos de configuração e permite que essas senhas altamente confidenciais sejam centralmente armazenadas, registradas e gerenciadas no cofre CyberArk. Esta abordagem permite que as organizações cumpram os requisitos internos e regulatórios de substituição periódica de senha e monitorem as atividades associadas a todos os tipos de identidades privilegiadas, seja no local ou na nuvem.

A instância mantém um identificador exclusivo para cada credencial, um tipo de credencial (tal como SSH, SNMP ou Windows) e qualquer afinidade de credencial. O MID Server obtém o identificador de credencial, o tipo de credencial e o endereço IP da instância e usa o cofre CyberArk para resolver esses elementos em uma credencial utilizável. O resolvedor de credenciais também pode pesquisar o nome do host, fqdn e usar a pesquisa de DNS reversa para obter fqdn.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A integração CyberArk requer que o ServiceNow® plug-in Armazenamento externo de credenciais, que fica disponível em**plug-ins** > **System Definitions**. O cliente AIM/API MID Server e CyberArk devem ser instalados na mesma máquina. A versão 12.0.1 dos Provedores de credenciais do CyberArk Application Access Manager (AAM) e superiores são compatíveis.

Instalação com CyberArk

- **Regra de negócio**: a regra de negócio de Armazenamento externo de credenciais executa as seguintes tarefas quando um administrador faz alguma mudança na propriedade de Armazenamento externo de credenciais:
  - Altera a exibição da lista de registros de credenciais e do formulário para a exibição Armazenamento externo. Esta exibição permite que os usuários vejam a coluna ID de credencial na lista.
  - Instrui o MID Server a atualizar o cache de credenciais não externas em preparação para uma mudança na maneira como as credenciais são obtidas.
- **Propriedade do sistema**: uma propriedade chamada habilitar armazenamento externo de credenciais [com.snc.use_external_credentials] habilita ou desabilita o plug-in de Armazenamento externo de credenciais depois que ele é ativado. Esta propriedade está localizada em **Definição da Descoberta** > **Propriedades** e **Orquestração** > **Propriedades do MID Server** e é habilitada quando você ativa o plug-in.

Nota: Se você desabilitar o Armazenamento externo de credenciais com a propriedade do sistema, o sistema definirá automaticamente todas as credenciais externas para inativas na instância. Se você reativar o recurso com esta propriedade, o sistema não redefinirá os registros de credenciais externas para ativos. Você deve reativar cada registro de credencial manualmente.

Tipos de credenciais suportados

A integração CyberArk suporta esses tipos de credenciais ServiceNow:

- GCP
- Azure
- CIM
- JMS
- Forum SNMP
- SNMPv3
- Autorização básica
- Par de chaves SSH
- Chave privada SSH (com chave, frase secreta e senha)
- VMware
- Windows
- Credenciais de Aplicativo

Nota: Para usar a integração CyberArk com o tipo de credencial do GCP, você deve modificar o jar de armazenamento externo de credenciais. Para obter detalhes, consulte Resolvedor de credenciais do GCP da ServiceNow usando o CyberArk.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Recursos Now Platform que usam esses protocolos de rede também suportam o uso de credenciais armazenadas em um cofre CyberArk.

Credenciais suportadas com o protocolo de rede

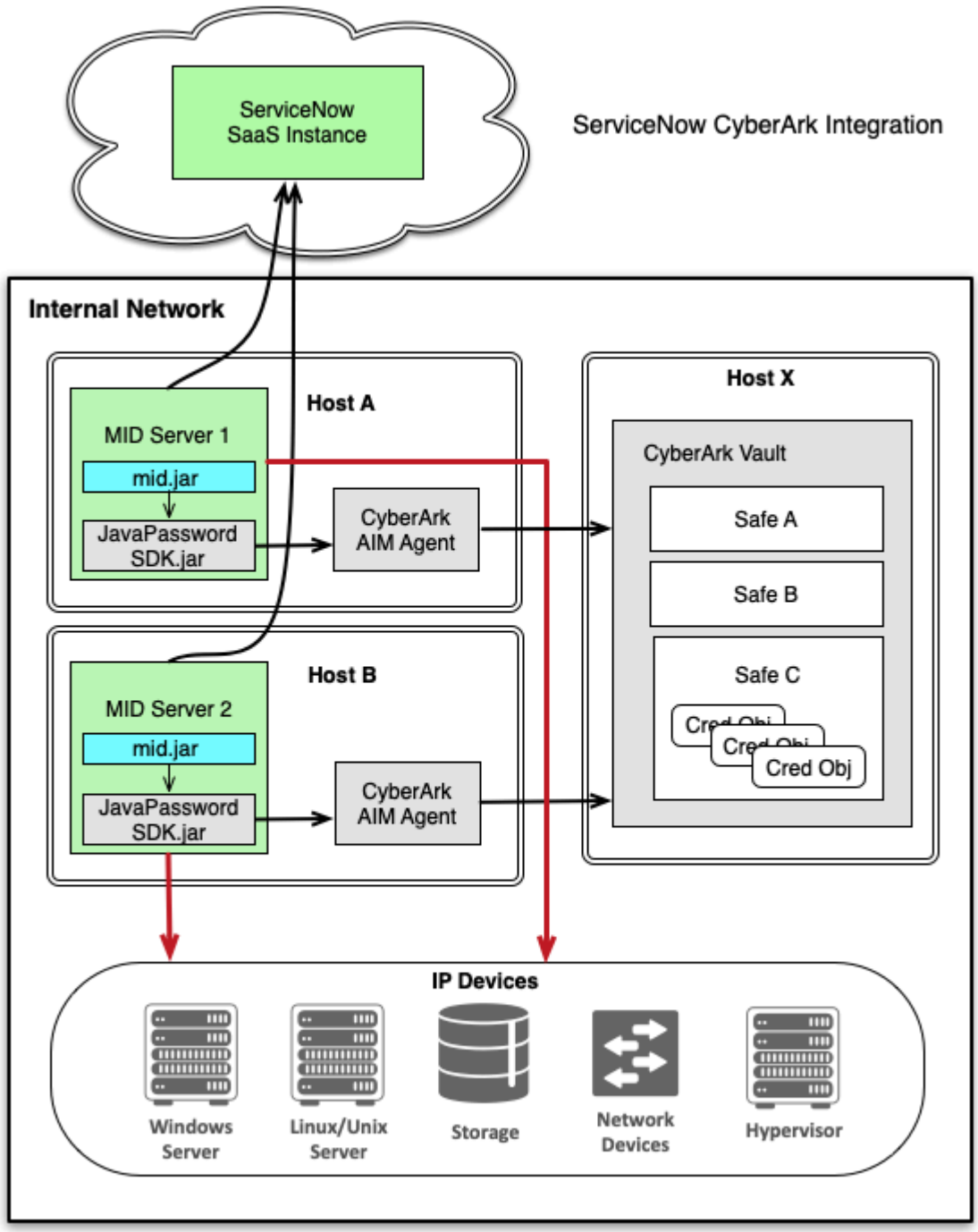
Protocolo de rede	Suporte ServiceNow® Flow Designer	Suporte Orquestração
SOAP	Etapa SOAP	Criar uma atividade SOAP Web Services com substituições de autenticação básica
REST	Etapa REST	Criar uma atividade REST Web Services com substituições de autenticação básica
JDBC	Etapa JDBC	Atividade JDBC
SSH	Etapa de SSH	Atividade SSH
PowerShell	Etapa de PowerShell	Atividade PowerShell
SFTP	Etapa SFTP	Atividade SFTP
JMS		Atividade JMS

Importante: Não é possível gerenciar as credenciais armazenadas em um cofre CyberArk e um sistema personalizado de armazenamento externo de credenciais usando o mesmo MID Server. O cliente AIM/API MID Server e CyberArk devem ser instalados na mesma máquina.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Arquitetura CyberArk

Arquitetura de armazenamento CyberArk



Nota: CyberArk usa o arquivo *mid.jar* do sistema base para resolver as credenciais.

Como MID Server lida com contas Windows

A pesquisa de credencial tenta inicialmente corresponder o ID de credencial especificado a um valor existente no campo **Nome** do cofre CyberArk. Se uma correspondência for encontrada, essa credencial será retornada. Se nenhuma correspondência for encontrada,

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a pesquisa de credencial tentará encontrar uma correspondência usando o endereço IP. Se a pesquisa de endereço IP corresponder a mais de uma credencial, como Windows e Tomcat no mesmo servidor, a pesquisa falhará. Para evitar esse problema, defina o parâmetro *ext.cred.type_specifier* no arquivo MID Server config.xml como **verdadeiro** para forçar CyberArk a retornar credenciais que correspondam ao tipo de credencial e ao endereço IP. Por exemplo, se um endereço IP for compartilhado por Windows e Tomcat, um tipo de credencial de Windows retornará somente a credencial Windows.

Como fazer upgrade da biblioteca do CyberArk

Se for necessário inserir um parâmetro de configuração protegido, será possível fazer upgrade da biblioteca do CyberArk.

Verifique o seguinte parâmetro de configuração em **config.xml**:

```
<parameter name="mid.secure_config.provider"
value="com.service_now.mid.services.config.CyberArkSecuredConfigProvider"/>
```

Caso já exista a configuração de um parâmetro de configuração protegido, siga as etapas abaixo para realizar o upgrade.

1. Renomeie a versão do cliente CyberArk para `JavaPasswordSDK_MajorVersion_minorVersion_patchNum.jar`.
2. Crie uma nova entrada jar na tabela `ecc_agent` à qual é possível anexar o jar renomeado. A nova entrada é baixada no MID Server. Essa etapa resulta em dois jars (Passworsdk.jar e JavaPasswordSDK _12_X_X.jar).
3. Exclua a antiga entrada ecc_agent da instância. Essa etapa exclui o Passworsdk.jar do MID Server, enquanto o JavaPasswordSDK _12_X_X.jar permanece no sistema.

Configuração de Integração CyberArk

Esses procedimentos incluem tarefas de configuração da CyberArk e da ServiceNow, incluindo referências à documentação apropriada da CyberArk.

O identificador de credencial configurado na instância ServiceNow deve ser mapeado para o nome da credencial no cofre da CyberArk. Ao pesquisar uma credencial, o MID Server encontra a credencial correspondendo o identificador de credencial a um nome no cofre, que deve ser exclusivo. Se o identificador de credencial estiver em branco, o MID Server encontrará a credencial por endereço IP. Para identificar a credencial por endereço IP, o sistema verifica o tipo de credencial para garantir que haja apenas uma credencial desse tipo nesse endereço. Um exemplo disso pode ser quando um servidor Windows e o vCenter estão sendo executados no mesmo endereço IP. Para suportar requisitos rigorosos de credenciais como este em um ambiente SSH, um parâmetro de configuração MID Server permite que você exija que o tipo de credencial solicitado corresponda ao tipo retornado pela CyberArk.

> **Nota:** O campo **ID de credencial** é o único campo necessário para mapear suas credenciais para a CyberArk, em todos os casos, exceto para SNMPv3. O campo **ID de credencial de privacidade** é opcional e é necessário somente ao usar credenciais SNMPv3 e usar um protocolo de privacidade para as credenciais. Consulte Configure o identificador de credencial da CyberArk para obter mais detalhes.

Para configurar sua instância para obter credenciais de um cofre da CyberArk, conclua essas tarefas na ordem em que aparecem abaixo.

Configure o cofre da CyberArk e instale a API AIM

Configure o cofre da CyberArk para permitir o acesso ao MID Server e instalar a API AIM da CyberArk na máquina do MID Server.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Função necessária: administrador

Antes de iniciar este procedimento, certifique-se de que o plug-in Armazenamento externo de credenciais esteja ativado. As versões 12.0.1 e superiores dos Provedores de Credenciais do Application Access Manager (AAM) do CyberArk são compatíveis.

Procedimento

1. Configure o cofre da CyberArk com o ID da aplicação e os detalhes de autenticação que serão usados por todos os MID Servers que solicitam as credenciais.
   Para obter detalhes, consulte o Provedor de credenciais da CyberArk e o Guia de implementação do ASCP.

   a. Certifique-se de que a CyberArk esteja configurada para permitir que o MID Server acesse o cofre criando um App-ID na CyberArk chamada *`ServiceNow_MID_Server`*.

   b. Certifique-se de que cada credencial que o MID Server precisa tenha acesso concedido ao App-ID *`ServiceNow_MID_Server`*.

      Nota: É possível substituir o App-ID **ServiceNow_MID_Server** padrão no arquivo `config.xml` do MID Server usando o parâmetro ext.cred.app_id. Se você alterar o valor neste parâmetro, certifique-se de configurar um valor correspondente no cofre.

2. Instale o Provedor de Credenciais da CyberArk, incluindo a API AIM, em cada máquina que hospeda um serviço do MID Server usado para acessar o armazenamento de credenciais.
3. Provisione as contas da CyberArk e defina permissões de acesso à aplicação.
   Para obter detalhes, consulte o Guia de Implementação de Segurança de Conta Privilegiada da CyberArk.
   a. No Cofre de Senha da CyberArk, crie as contas privilegiadas exigidas pelo Descoberta, Orquestração ou Mapeamento de serviços para acessar diferentes dispositivos e garantir que essas contas sejam membros dos cofres nos quais as credenciais necessárias são armazenadas.
   b. Adicione o Provedor de credencial e os usuários da aplicação como membros dos Cofres de senha em que as senhas da aplicação ficam armazenadas.

Importe o arquivo JAR da CyberArk

Importe o arquivo JavaPasswordSDK.jar da CyberArk para a instância para torná-lo acessível para o MID Server.

Antes de Iniciar

Função necessária: agent_admin ou admin

Antes de iniciar este procedimento, certifique-se de que a CyberArk esteja configurada para permitir que o MID Server acesse às credenciais. Certifique-se de que a API AIM da CyberArk esteja instalada em cada servidor que hospeda um MID Server usado para acessar o cofre.

Por Que e Quando Desempenhar Esta Tarefa

Use este processo mesmo se o arquivo JavaPasswordSDK.jar já existir no MID Server.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegue até **Todos** > **MID Server** > **Arquivos JAR**.
2. Clique em **Novo**.
3. Preencha o formulário usando os campos da tabela.

Campos de formulário do arquivo JAR

Campo	Descrição
Nome	Nome exclusivo e descritivo para identificar o arquivo na instância.
Versão	Número da versão opcional do arquivo, se houver uma disponível.
Fonte	Provedor do arquivo JAR. As informações de origem não são usadas pelo sistema.
Descrição	Descrição resumida opcional do arquivo JAR e sua finalidade na instância.

4. Anexe o arquivo JAR a este registro.
   O arquivo `JavaPasswordSDK.jar` AIM vem com os arquivos de instalação AIM SDK e fica localizado geralmente no MID Server no diretório de instalação AIM em `<install_dir>/CyberArk/ApplicationPasswordSdk`.
5. Clique em **Enviar**.
6. Reinicie o serviço do MID Server.
   A plataforma disponibiliza o arquivo JAR para qualquer MID Server configurado para se comunicar com a instância.

Configure o MID Server para CyberArk

Configure o arquivo `config.xml` para conceder acesso ao MID Server ao cofre da CyberArk.

Antes de Iniciar

Função necessária: administrador
Antes de iniciar este procedimento, importe o arquivo `JavaPasswordSDK.jar` na instância.

Procedimento

Configure manualmente o arquivo MID Server Adicione um parâmetro MID Server com esses parâmetros.

Esta configuração não pode ser feita a partir da instância.

Parâmetros de configuração necessários

Parâmetro	Valor	Descrição
ext.cred.safe_folder	NameOfFolder	Pasta a ser usada para todas as pesquisas de credencial. Por exemplo, **root**.
ext.cred.use_cyberark	verdadeiro	Parâmetro booleano que indica que este MID Server está integrado à CyberArk.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Parâmetros de configuração opcional

Parâmetro	Valor	Descrição
ext.cred.safe_timeout	5 (segundos)	Tempo limite de cada pesquisa de credencial no cofre, especificado em segundos.
ext.cred.safe_name	NameOfSafe	Nome de cofre padrão usado para todas as pesquisas de credencial. Se os parâmetros estiverem em vários cofres, o ID de credencial poderá ser especificado no formato *<safeName>:<CredentialID>*. Quando configurado dessa forma, o campo **NameOfSafe** é ignorado. Se todas as credenciais externas tiverem seus IDs de credencial especificados neste formato, deixe de fora o campo **NameOfSafe**. **Nota:** Por padrão, o caractere separador neste formato é dois pontos. Para atribuir qualquer caractere que você queira como separador, adicione esta linha ao arquivo `CredMap.properties`: `safe.cred.split.string=<string>`.
ext.cred.app_id	ServiceNow_MID_Server	Especifica o App-ID usado para conceder permissão ao MID Server para acessar o cofre CyberArk. O valor padrão, **ServiceNow_MID_Server**, deve ser definido no cofre CyberArk. É possível usar este parâmetro para substituir o padrão e especificar seu próprio App-ID. Se você editar o App-ID neste parâmetro, certifique-se de configurar a CyberArk para corresponder.
ext.cred.type_specific	verdadeiro	Força uma pesquisa de endereço IP a retornar credenciais que correspondam ao ID da plataforma CyberArk e ao endereço IP. Por exemplo, se um endereço IP for compartilhado pelo Windows e pelo Tomcat, uma credencial com um ID de plataforma com **Win** retornará apenas a credencial Windows. Quando este parâmetro é definido como verdadeiro, o CyberArk procura IDs de plataforma que começam com: • Win: Windows • Unix: SSH • VMWare: VMware
ext.cred.check_ssh_type	falso	Quando definido como verdadeiro, requer que o tipo de credencial SSH

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Parâmetro	Valor	Descrição
		retornado da CyberArk corresponda ao tipo de credencial solicitado. Por exemplo, se uma credencial de nome de usuário/ senha SSH normal for solicitada e somente as chaves SSH estiverem disponíveis, a pesquisa de credencial falhará.

Configure a CyberArk para credenciais SNMPv2

Se o seu sistema usa SNMPv2, é possível criar um arquivo especial para mapear o atributo em uma credencial para a cadeia de caracteres da comunidade.

Antes de Iniciar

Função necessária: administrador
Antes de iniciar este procedimento, configure o MID Server para que tenha acesso ao cofre CyberArk.

Por Que e Quando Desempenhar Esta Tarefa

Nota: Se a cadeia de caracteres da comunidade aparecer no campo de senha da credencial CyberArk, não será necessário executar este procedimento.

O SNMPv2 não é suportado nativamente na CyberArk. Se a sua organização criou credenciais SNMPv2 personalizadas nas quais a cadeia de caracteres de comunidade não aparece no campo de senha da credencial, use este procedimento para mapear o atributo na credencial para a cadeia de caracteres da comunidade.

Procedimento

1. Em um editor de texto, crie um arquivo chamado `CredMap.properties`, contendo este código:
   `SNMPv2.Community=attribute_name`
2. Salve o arquivo no diretório `/agent` da sua instalação MID Server.
   Na pesquisa de credencial, o MID Server tenta encontrar este atributo para a credencial. Se o atributo não for encontrado, o MID Server procurará o campo de senha. Se o campo de senha estiver vazio, a pesquisa de credencial falhará.

Configure o identificador de credencial da CyberArk

Crie a chave exclusiva que a CyberArk pode usar para identificar credenciais específicas no repositório externo.

Antes de Iniciar

Função necessária: administrador
Antes de iniciar este procedimento, certifique-se de que o plug-in Armazenamento externo de credenciais esteja ativado e que a propriedade do sistema com.snc.use_external_credentials esteja definida como verdadeiro.

Procedimento

1. Navegue até **Todos** > **Descoberta** > **Credenciais** ou **Orquestração** > **Credenciais**.
2. Clique em **Nova**.
3. Na lista de tipos de credenciais, selecione um tipo que suporte armazenamento externo CyberArk.
4. Preencha o formulário usando os campos do seu tipo de credencial.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Marque a caixa de seleção **Armazenamento de credenciais externas**.
   Os campos **Nome de usuário** e **Senha** são substituídos pelo campo **ID de credencial**.

   Nota: Se a caixa de seleção não estiver visível, clique no ícone de menu na barra de cabeçalho e selecione **Exibir** > **Armazenamento externo**.

6. No campo **ID de Credencial**, insira uma expressão usando um destes formatos:
   - Se todas as suas credenciais estiverem no mesmo cofre, configure o nome do cofre no arquivo `config.xml` do MID Server usando o parâmetro ext.cred.safe_name e, em seguida, especifique o ID da credencial apenas por nome, como **<credential ID>**.
   - Para nomear credenciais para uma determinada plataforma que reside em um cofre específico, defina o ID de credencial como **<safe>:<credential ID>:<platform ID>**.
   - Se as suas credenciais estiverem em vários cofres, especifique o ID de credencial neste formato: **<safe>:<credential ID>**.
   - Se deseja que a CyberArk pesquise a credencial por endereço IP, usando um cofre alternativo, especifique o ID de credencial neste formato: **<safe>:**.
   - Se deseja que a CyberArk pesquise a credencial para um ID de plataforma alternativa no mesmo cofre, use este formato: **::<platform ID>**
   - Se deseja que a CyberArk pesquise a credencial em um cofre configurado pelo endereço IP em vez do ID de credencial, deixe esse campo em branco. Esta é a prática recomendada para lidar com instalações nas quais cada servidor possui uma credencial exclusiva. Sem este tipo de pesquisa, você deve criar um registro de ID de credencial em sua instância para cada servidor em seu ambiente.

   Nota: O ID de credencial deve corresponder ao valor no campo **Nome** para a conta CyberArk. O campo **ID de credencial** possui um limite de 180 caracteres.

7. Se você estiver armazenando as credenciais SNMPv3 na CyberArk e estiver usando o protocolo de privacidade e a chave de privacidade, configure o ID da seguinte maneira:

   a. No campo **Tipo de armazenamento de credencial**, selecione **CyberArk**.
      O campo **ID de credencial de privacidade** aparece.

   b. Insira o **Nome** da conta da privacidade CyberArk SNMPv3 no campo **ID de credencial de privacidade**.

8. Clique em **Enviar**.

Configure as credenciais AWS em um cofre CyberArk

Configure seu cofre CyberArk com as credenciais AWS para que sejam recuperadas para uso por sua instância.

Antes de Iniciar
Função necessária: admin

Por Que e Quando Desempenhar Esta Tarefa
Armazene as credenciais como uma chave SSH no cofre da CyberArk. Ao configurar o acesso ao cofre em sua instância, o nome dado à chave SSH também deve ser usado como o ID de credencial.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Na CyberArk, acesse **Contas** > **Adicionar chave SSH**.
2. Insira as seguintes informações:

Credenciais CyberArk

Campo	valor
Tipo de dispositivo	Selecione **Serviço em nuvem**.
Nome de plataforma	Selecione **Amazon Web Services - AWS - Chaves de acesso**.
ID da chave de acesso AWS	Insira a Chave de acesso AWS, conforme fornecido pelo AWS.
Nome de usuário AWS IAM	Digite novamente a Chave de acesso AWS, conforme fornecido pelo AWS.
Senha	Insira a chave de acesso secreto AWS, conforme fornecido por AWS.
Nome	Insira um nome para esta chave.

3. Escolha **Salvar**.

O que Fazer Depois

Se isso ainda não foi feito, crie um identificador de credencial em sua instância para configurar o acesso ao cofre da CyberArk. Para obter mais detalhes, consulte Configurar acesso ao Armazenamento externo de credenciais para AWS.

Configure as credenciais Azure em um cofre CyberArk

Configure seu cofre CyberArk com as credenciais Azure para que sejam recuperadas para uso por sua instância.

Antes de Iniciar

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

Para armazenar uma credencial Azure, primeiro crie um modelo de credencial Azure no cofre da CyberArk. Este processo só precisa ser concluído uma vez para o cofre.

Procedimento

1. Faça login na CyberArk no modo Administração.
2. Navegue até a guia **Administração**.
3. Em **Configuração do sistema**, edite **Gerenciamento de plataforma**.
4. Navegue até **Modelo de provedor em nuvem** e duplique-o.
5. Edite o modelo para credenciais do Azure.
6. Adicione as duas propriedades a seguir:
   - *Name* como *Username* e *Display Name* como *Client ID*
   - *Name* como *Address* e *DisplayName* como *Tenant ID*

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

7. Aplique as mudanças.
8. Navegue até a seção **Conta** e selecione **Adicionar conta**.
9. Selecione **Cofre**.
10. Defina o **Tipo de dispositivo** como **Serviço em nuvem**.
11. Selecione o modelo do Azure que foi editado anteriormente.
12. Preencha as informações para os campos **ID de cliente**, **ID de locatário** e **Senha**.
13. Selecione **Salvar**.

Autenticação OAuth 2.0 por meio do MID Server usando armazenamento externo de credenciais

Armazene as credenciais de ID e segredo do cliente OAuth 2.0 no cofre do CyberArk, e não na instância da ServiceNow. O MID Server obterá as credenciais do cofre do CyberArk, quando isso for necessário para obter o token OAuth. O token será armazenado no MID Server e atualizado automaticamente após a expiração.

O produto CyberArk AIM (Application Identity Management) usa a solução Privileged Account Security para eliminar a necessidade de armazenar senhas de aplicação integradas em aplicações, scripts ou arquivos de configuração. Ele também permite o armazenamento, o registro em log e a gestão centrais dessas senhas altamente confidenciais no cofre do CyberArk. É possível configurar o cofre do CyberArk para armazenar credenciais do OAuth 2.0, em vez de armazená-las diretamente em um registro de credenciais da ServiceNow. Para saber mais sobre o CyberArk, consulte CyberArk integração de armazenamento de credenciais.

Arquitetura de autenticação OAuth 2.0 da solicitação do MID Server

A arquitetura tem duas partes: a instância da ServiceNow e o ambiente de configuração do MID Server e do cliente do AIM (Application Identity Manager). Alguns exemplos de ambiente são a nuvem ou um ambiente do cliente.

É necessário configurar o MID Server e o cliente do AIM no mesmo ambiente. Além disso, é preciso configurar o AIM para interagir com o cofre externo do CyberArk. É possível hospedar o cofre externo do CyberArk no mesmo ambiente do MID Server e do AIM ou em um ambiente diferente.

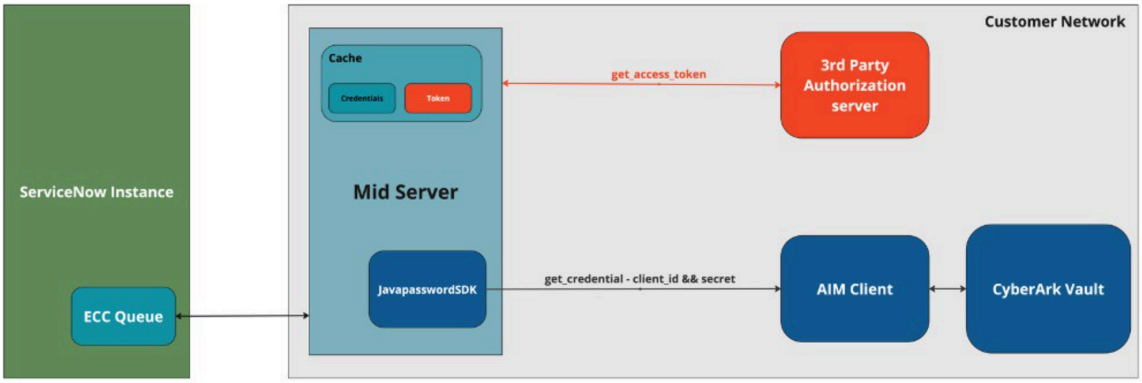
A instância da ServiceNow mantém identificadores de credenciais que se mapeiam às credenciais do OAuth 2.0 específicas armazenadas no cofre do CyberArk. Antes de enviar uma solicitação de token OAuth, o MID Server obtém o identificador de credencial da instância e usa um arquivo JAR fornecido pelo cliente para enviar o identificador ao cliente do AIM. O cliente do AIM envia a solicitação ao cofre do CyberArk. O cofre do CyberArk envia as credenciais do OAuth 2.0 de volta para o MID Server por meio do cliente do AIM. Depois de receber as credenciais do OAuth 2.0, o MID Server envia a solicitação de token OAuth ao servidor de autorização de terceiros. A solicitação de token compreende informações como cliente e segredo do cliente que o CyberArk armazena, o escopo do OAuth e a URL de token que a instância armazena. Depois que o servidor de autorização emite o token OAuth, o MID Server o armazena em sua memória cache.

Nota: Esse recurso dá suporte ao tipo de concessão de credenciais do cliente.

A imagem mostra o processo de autenticação da solicitação do MID Server.

Nota: Presume-se que o servidor de autorização de terceiros e o cofre do CyberArk estejam hospedados na rede do cliente.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Como configurar um arquivo JAR e identificadores de credencial

Configure um arquivo JAR e identificadores de credencial para que o arquivo JAR resolva os identificadores de credencial em credenciais reais do cofre externo do CyberArk. O processo permite que o MID Server obtenha e inclua credenciais do OAuth 2.0 na solicitação de tokens OAuth.

Antes de Iniciar

Função necessária: agent_admin ou admin

O cofre externo do CyberArk armazena credenciais confidenciais, e a instância da ServiceNow armazena identificadores de credencial que se associam aos nomes de credencial específicos que o cofre armazena. O arquivo JAR permite o mapeamento de um identificador de credencial a um nome de credencial específico no cofre externo. O mapeamento permite que o MID Server adquira e inclua a credencial necessária na solicitação de tokens OAuth. É necessário configurar os identificadores de credencial e o arquivo JAR na instância da ServiceNow e no MID Server, respectivamente.

Procedimento

1. Importe o arquivo JAR da CyberArk.
2. Como configurar uma conexão para enviar uma solicitação do OAuth por meio do MID Server usando o cofre externo.

Configuração do CyberArk

Configure o cofre do CyberArk para armazenar credenciais do OAuth 2.0 e responder às solicitações do MID Server por credenciais do OAuth 2.0.

Antes de Iniciar

Confirme se você assinou o ServiceNow IntegrationHub Standard Pack Installer. Para obter mais informações, consulte https://www.servicenow.com/content/dam/servicenow-assets/public/en-us/doc-type/legal/snc-addendum-integrationhub.pdf.

Função necessária: agent_admin ou admin

Procedimento

1. Configure o cofre da CyberArk e instale a API AIM.
2. Importe o arquivo JAR da CyberArk.
3. Como configurar credenciais OAuth 2.0 no CyberArk.
4. Como configurar uma conexão para enviar uma solicitação do OAuth por meio do MID Server usando o cofre externo.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países. Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Como configurar credenciais OAuth 2.0 no CyberArk

Configure seu cofre CyberArk com as credenciais OAuth 2.0 que a instância da ServiceNow solicita.

Antes de Iniciar

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

Para armazenar credenciais OAuth 2.0, crie um modelo de credencial OAuth 2.0 no cofre CyberArk. Somente realize esse processo uma vez para o cofre.

Procedimento

1. Siga as etapas abaixo se estiver configurando as credenciais OAuth 2.0 pela primeira vez.

   a. Faça login no CyberArk no modo "Administração".

   b. Navegue até a guia **Administração**.

   c. Selecione **Gestão da plataforma**.
   A página "Gestão da plataforma" exibe as plataformas na guia "Destinos".

   d. Expanda um tipo de plataforma.

   e. Selecione o ícone de configurações ( ) que corresponde a um modelo de plataforma e selecione **Duplicar**.

   f. Na janela "Duplicar plataforma", digite um nome para o modelo e selecione **Criar**.

   > **Nota:** Observe o tipo de sistema em que você criou um modelo duplicado. Por exemplo, "Serviço em nuvem" é um tipo de sistema.

   g. Selecione o ícone de configurações ( ) que corresponde ao modelo de plataforma duplicado que você criou e selecione **Editar**.

   h. Adicione a propriedade.
   "Nome" deve ser o "Nome de usuário", e "Nome de exibição" deve ser o "ID do cliente".

   i. Renomeie as outras propriedades.

   > **Dica:** Escolha nomes de propriedade relevantes para OAuth 2.0.

   j. Selecione **Aplicar**.
   As atualizações serão aplicadas.

   k. Selecione **OK**.

   l. No painel esquerdo, navegue até "Contas".

   m. Selecione **Adicionar conta**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

n. No título "Tipo de sistema", selecione o tipo de sistema em que você criou o modelo de plataforma.
O tipo de sistema mostrará os modelos de plataforma.

o. No título "Selecionar plataforma", selecione o modelo de plataforma que você criou.

p. Selecione "Cofre".
Salve o valor do Cofre para uso posterior.

q. Preencha as informações de "ID do cliente", "Senha" (informe o "Segredo do cliente" como valor) e outros campos conforme necessário.

r. Selecione **Adicionar**.
A conta será adicionada.

s. Na página "Exibição da conta", abra uma conta.

t. Selecione a guia **Detalhes**.

u. Copie o valor armazenado na seção "Nome da conta" e o salve para uso posterior.
O valor que você copiou e armazenou é usado como o identificador de credencial na instância da ServiceNow.

2. Siga as etapas abaixo se você não estiver configurando as credenciais OAuth 2.0 pela primeira vez.

a. Faça login no CyberArk no modo "Administração".

b. Navegue até a seção **Conta** e selecione **Adicionar conta**.

c. Em **Tipo de sistema**, selecione o tipo de sistema no qual existe o modelo para armazenar o OAuth 2.0.

d. Selecione o modelo de plataforma necessário que você criou e selecione **Cofre**.
Salve o valor do Cofre para uso posterior.

e. Preencha as informações de "ID do cliente", "Senha" (informe o "Segredo do cliente" como valor) e outros campos conforme necessário.

f. Selecione **Adicionar**.
A conta será adicionada.

g. Na página "Exibição da conta", abra uma conta.

h. Selecione a guia **Detalhes**.

i. Copie o valor armazenado na seção "Nome da conta" e o salve para uso posterior.
O valor que você copiou e armazenou é usado como o identificador de credencial na instância da ServiceNow.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Como configurar uma conexão para enviar uma solicitação do OAuth por meio do MID Server usando o cofre externo

Configure uma conexão para enviar solicitações de tokens OAuth 2.0 a um servidor de autenticação de terceiros por meio do MID Server. O MID Server adiciona credenciais do OAuth 2.0 (ID e segredo do cliente) à solicitação a partir do cofre externo CyberArk, do escopo do OAuth e da URL do token da instância e os envia ao servidor de autenticação de terceiros.

Antes de Iniciar
Verifique os itens abaixo.

- Confirme se você assinou o ServiceNow IntegrationHub Standard Pack Installer. Para obter mais informações, consulte https://www.servicenow.com/content/dam/servicenow-assets/public/en-us/doc-type/legal/snc-addendum-integrationhub.pdf.
- Você criou um arquivo JAR que permite que o MID Server resolva credenciais com o cofre externo CyberArk. Consulte Crie um arquivo JAR para resolver credenciais.
- Você importou o arquivo JAR no MID Server.
- O MID Server está configurado para CyberArk. Consulte Configure o MID Server para CyberArk.
- O OAuth 2.0 está configurado no armazenamento externo CyberArk. Consulte Como configurar credenciais OAuth 2.0 no CyberArk.

Função necessária: nenhuma

Por Que e Quando Desempenhar Esta Tarefa
É possível configurar a conexão e a credencial com um modelo de configuração ou manualmente. Um modelo de configuração define os componentes do formulário de registro da conexão e é reutilizável para outros registros de conexão. Manualmente, somente é possível configurar a conexão para um só registro. O tópico mostra as duas abordagens.

Procedimento
1. Configure a conexão com um modelo de configuração.

   a. Navegue até **Todos** > **IntegrationHub** > **Modelos de configuração**.

   b. Selecione **Novo**.

   c. Selecione **Conexão HTTP com tipo de concessão de Credenciais de cliente OAuth (armazenamento externo)**.

   d. Atualize o formulário conforme necessário.
   Por exemplo, é possível informar o escopo nos campos `oauth_entity_profile_scope` e `oauth_entity_scope` da seção "Modelo de dados padrão". Para aprender a criar um modelo de configuração, consulte Crie um modelo de configuração.

   e. Selecione **Enviar**.
   Você criou o modelo de configuração.

   f. Navegue até **Todos** > **IntegrationHub** > **Aliases de conexão e credencial**.

   g. Atualize o formulário.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Alias de conexão e credencial

Campo	Descrição
Nome	Nome do alias. Um alias só pode conter caracteres alfa, número e sublinhado. Durante um upgrade, o marcador no registro de credencial migra para um alias de credencial e conexão. Se o marcador de credencial contiver caracteres especiais diferentes de alfabetos, números e sublinhados, isso preserva o nome do marcador após um upgrade. Ainda é possível usar esse alias migrado, mas não é possível atualizá-lo até que você mude o nome para atender às restrições de nomenclatura.
Aplicação	Identificador exclusivo do alias de conexão e credencial, com base no formato `scope_name.alias_name`. ▪ Se o escopo for Global, o ID será o nome do alias. Por exemplo, se você criar um alias do Workday no escopo global, ele definirá o ID para `workday`. ▪ Se você criar um alias do workday no escopo do app de RH, ele definirá o ID como `x_hr_app.workday`.
Alias primário	Opção para selecionar o alias sob o qual você está criando esse alias de conexão e credencial. O alias de conexão e credencial que você está criando é um alias secundário. Um alias secundário é listado na guia **Aliases secundários**, na página do alias primário de conexão e credencial.
Tipo	Opção para indicar o tipo de alias que você está criando. Escolha dentre as seguintes opções. ▪ Credencial: alias que contém um registro de credencial. ▪ Conexão e credencial: alias que contém um registro de conexão e credencial. Essa opção é selecionada por padrão.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Confirme se a opção "Conexão e credencial" está selecionada.
Suporte a várias conexões ativas	Designador que indica se o alias suporta várias conexões ativas. Adicione conexões usando a tabela Conexões e as associe ao alias usando a lista relacionada às Conexões.
Política de nova tentativa padrão	Tente novamente a política para o alias. Para obter mais informações, consulte Política de nova tentativa.
Modelo de configuração	Opção para selecionar o modelo de configuração com base no qual você está criando o alias de conexão e credencial. Selecione o modelo do tipo **Conexão HTTP com tipo de concessão de Credenciais de cliente OAuth (armazenamento externo)** que você criou.

h. Selecione **Enviar**.
Você criou o registro de alias de conexão e credencial.

i. Navegue até **Todos** > **IntegrationHub** > **Painel de conexões**.

j. No campo "Pesquisar todas as conexões", digite o nome do registro de alias de conexão e credencial que você criou.

k. No registro, selecione **Exibir detalhes**.

l. Selecione **Configurar**.

m. Preencha o formulário

Formulário "Configurar conexão"

Campo	Descrição
Nome da conexão	O nome da conexão. Não é possível atualizar o nome.
URL de conexão	URL para o servidor de terceiros.
Usar MID	Opção para habilitar o MID Server. **Importante:** Confirme se a opção está selecionada.
Seleção de MID	Opção para especificar a configuração do MID para conexão.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	▪ **MID Server específico**: opção para indicar a seleção manual de um MID Server específico. ▪ **Selecionar automaticamente o MID Server**: opção para indicar que você deseja que o MID Server seja selecionado automaticamente. ▪ **Cluster do MID específico**: opção para indicar a seleção manual de um cluster de MID Servers. **Importante:** Confirme se o MID Server que você selecionou reside na mesma máquina que o Cliente CyberArk AIM que está configurado para acessar o cofre CyberArk. Consulte Configure o cofre da CyberArk e instale a API AIM.
MID Server	Opção para especificar um MID Server manualmente. Essa opção aparecerá se você selecionar **MID Server específico** no campo **Seleção de MID**.
Cluster do MID	Opção para especificar um cluster do MID manualmente. Essa opção aparecerá se você selecionar **Cluster do MID específico** no campo **Seleção de MID**.
Armazenamento externo de credenciais	Opção para usar o armazenamento externo de credenciais CyberArk. Quando você seleciona essa opção, o MID Server obtém as credenciais do OAuth 2.0 (ID e segredo do cliente) do armazenamento externo de credenciais. **Importante:** Confirme se a opção está selecionada.
ID da credencial	Identificador da conta CyberArk que contém os detalhes do ID e do segredo do cliente. Para exibir o procedimento para obter o identificador de credencial, consulte Como configurar credenciais OAuth 2.0 no CyberArk. No campo "ID da credencial", digite uma expressão usando um desses formatos. ▪ Se todas as suas credenciais estiverem no mesmo cofre, configure o nome desse cofre no arquivo `config.xml` do MID Server usando o parâmetro ext.cred.safe_name e, em seguida,

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	especifique o ID da credencial apenas por nome, como **<ID da credencial>**. ▪ Para nomear credenciais para uma determinada plataforma que reside em um cofre específico, defina o ID de credencial como **<safe>:<credential ID>:<platform ID>**. ▪ Se as suas credenciais estiverem em vários cofres, especifique o ID da credencial neste formato: **<cofre>:<ID da credencial>**.
URL do token OAuth	URL que especifica o endpoint para obter o token de acesso do servidor OAuth.

n. Selecione **Configurar conexão**.

2. Configure uma conexão manualmente.

a. Navegue até **Todos** > **OAuth de sistema** > **Registro de aplicações**.

b. Selecione **Novo**.

c. Selecione **Conectar-se a um provedor de OAuth de terceiros usando um cofre externo**.

d. Preencha o formulário

Detalhes do novo registro de aplicação

Campo	Descrição
Nome	Nome para identificar o registro da aplicação. Por exemplo, digite: solicitação de token OAuth 2.0 via app MID.
Aplicação	Opção para especificar os nomes das aplicações que podem acessar esse registro de aplicação. O campo é somente leitura.
Tipo de concessão padrão	Método padrão para que a aplicação cliente obtenha o token de acesso do servidor OAuth. O tipo de concessão padrão e somente leitura é "Credenciais do cliente".
Acessível de	Opção para especificar quais aplicações podem acessar esse registro de aplicação.
URL de token	URL que especifica o endpoint para obter o token de acesso do servidor OAuth.
Enviar credenciais	Opção para especificar o método de envio do OAuth 2.0 no corpo da solicitação.
Comentários	Insira comentários relacionados.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

e. Na coluna **Escopo do OAuth**, crie um ou mais escopos do OAuth seguindo as etapas abaixo.

   i. Na coluna "Nome", clique duas vezes no campo e insira um nome de escopo do OAuth.

   ii. Na coluna "Escopo do OAuth", clique duas vezes no campo e insira o escopo.

f. Selecione **Enviar**.
Você criou um perfil de entidade do OAuth e o registro da aplicação.

g. Navegue até **Todos** > **IntegrationHub** > **Conexões e credenciais** > **Credenciais**.

h. Selecione **Novo**.

i. Selecione **Credenciais do OAuth 2.0**.

j. Selecione **Exibição de armazenamento externo**.

> **Importante:** Somente selecione **Exibição de armazenamento externo** se a exibição for diferente de um formulário de armazenamento externo de credenciais do OAuth 2.0.

k. Preencha o formulário

Credenciais do OAuth 2.0

Campo	Descrição
Nome	Nome do registro da credencial.
Aplica-se a	Opção para especificar se o registro da credencial é aplicável a todos os MID Servers ou a um MID Server específico. Em caso de MID Servers específicos, adicione-os. Escolha dentre as seguintes opções. ▪ Todos os MID Servers: o MID Server é selecionado automaticamente de uma coleção de MID Servers. ▪ MID Servers específicos: opção para especificar um ou mais MID Servers.
MID Servers	Opção para especificar um ou mais MID Servers. **Nota:** Esse campo aparecerá se você selecionar **MID Servers específicos** no campo "Aplica-se a".
Ativo	Opção para especificar se o registro da credencial está disponível para uso. Por padrão, ele fica disponível.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Perfil de entidade OAuth	Opção para especificar um perfil de entidade OAuth que a credencial usa. Selecione o perfil de entidade OAuth que você criou acima. Consulte Como configurar um perfil de entidade OAuth.
Armazenamento externo de credenciais	Opção para especificar que as credenciais sejam armazenadas em um armazenamento externo e não na instância da ServiceNow. **Importante:** Confirme se a opção está selecionada.
ID da credencial	Opção para especificar o identificador de credencial da conta CyberArk que contém o ID e o segredo do cliente. Para exibir o procedimento para obter o identificador de credencial, consulte Como configurar credenciais OAuth 2.0 no CyberArk.
Cofre de armazenamento de credenciais	Opção para especificar o nome do cofre de armazenamento externo de credenciais. Verifique se você selecionou CyberArk.

l. Selecione **Enviar**.
Você criou o registro da credencial.

m. Crie um alias de conexão e credencial.
Para saber as etapas, consulte Crie um alias de Conexão e Credenciais.

n. Navegue até **Todos** > **IntegrationHub** > **Conexões**.

o. Selecione **Novo**.

p. Selecione **Conexão HTTP(s)**.

q. Preencha o formulário

Formulário de conexão

Campo	Descrição
Nome	O nome exclusivo dessa conexão HTTP(s).
Ativo	Opção para definir como ativa a conexão que você está criando. A opção é selecionada por padrão.
Credencial	Selecione o registro de credencial usado para autorizar a conexão. Selecione a credencial que você criou acima.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Alias de conexão	Selecione o registro de alias a ser associado a esta conexão. Usar um alias permite que você atualize o registro de conexão sem precisar reconfigurar nenhuma ação ou atividade que use o alias.
Construtor de URL	Insira manualmente o URL de conexão ou use o sistema para construir o URL baseado em entradas. O padrão é desmarcado. Se verificado, o URL de conexão é calculado dos seguintes campos: ▪ Autenticação mútua — Marque a caixa, se a autenticação mútua for usada. ▪ Protocolo — se a autenticação mútua não for usada, insira o protocolo. O padrão é HTTPs. ▪ Perfil de protocolo — Se a autenticação mútua for usada, insira o perfil de protocolo de sys_protocol_profile. ▪ Host ▪ Porta ▪ Caminho base — Caminho da cadeia de caracteres de conexão. **Nota:** Se a autenticação mútua estiver marcada, o URL de conexão será criado: Protocolo + :// + host:port +URL. Se a autenticação mútua estiver desmarcada, a URL de conexão será criada desta forma: Perfil do protocolo + :// + host:porta +URL
URL de conexão	Se o construtor de URL estiver desmarcado, insira o URL de conexão neste campo. **Nota:** Se a autenticação mútua estiver marcada, o URL de conexão será criado: Protocolo + :// + host:port +URL. Se a autenticação mútua estiver desmarcada, a URL de conexão será criada desta forma: Perfil do protocolo + :// + host:porta +URL
Usar MID Server	Opção para especificar que você deseja enviar solicitações de token OAuth por meio de um MID Server.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Importante: Confirme se a opção está selecionada.
Tempo limite de conexão	Número de milissegundos que o sistema espera por uma conexão de host bem-sucedida. Se uma conexão bem-sucedida não ocorrer durante esse tempo, a solicitação de conexão expirará. Deixe este campo em branco para usar o valor de tempo limite de conexão padrão do sistema.
Seleção de MID	Opção para especificar uma das seguintes opções. ▪ Selecionar automaticamente o MID Server: seleciona dentre os MID Servers com base nos critérios de MID Server, independentemente de eles serem ou não membros de um cluster. ▪ MID Server específico: selecione um MID Server manualmente. ▪ Cluster do MID específico: a reatribuição automática para outro MID Server somente seleciona dentre membros do cluster especificado. **Importante:** Confirme se o MID Server que você selecionou reside na mesma máquina que o Cliente CyberArk AIM que está configurado para acessar o cofre CyberArk. Consulte Configure o cofre da CyberArk e instale a API AIM.
MID Server	Selecione um MID Server manualmente. Essa opção aparecerá se você selecionar "MID Server específico" no campo "Seleção de MID".
Cluster do MID	Selecione um cluster do MID manualmente. Essa opção aparecerá se você selecionar "Cluster do MID específico" no campo "Seleção de MID".
Aplicação de MID	Selecione uma aplicação MID manualmente.

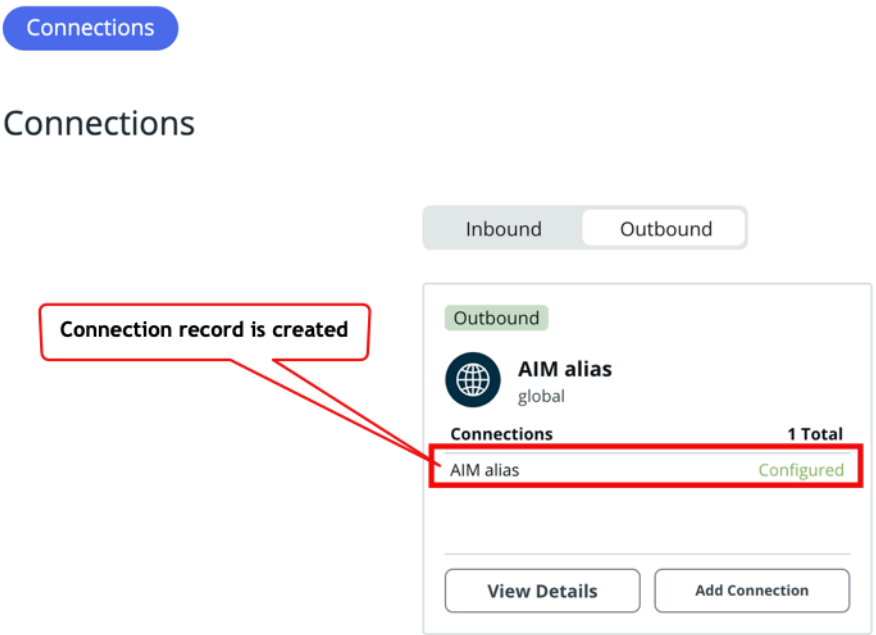
r. Selecione **Enviar**.
Você criou um registro de conexão HTTP(s).

s. Navegue até **Todos** > **Automação de processo** > **IntegrationHub** > **Painel de conexões**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

t. No campo "Pesquisar todas as conexões", digite o nome do registro de conexão que você criou.
O registro do alias de conexão será exibido.

O registro de conexão do OAuth 2.0 é criado



Algoritmos de autenticação

Verifique a identidade do remetente usando Algoritmos de autenticação

Permita que as etapas de integração sejam autenticadas com serviços da Web que exijam mecanismos de conexão ou de credenciais complexos ou não padrão. Associe algoritmos de autenticação a aliases de credenciais e de conexão para reduzir ou eliminar a necessidade de configurar manualmente as etapas de integração.

É possível usar um algoritmo de autenticação para gerar dados de autenticação personalizados para suas etapas de integração. As etapas de integração podem usar esses dados dinâmicos para criar quaisquer artefatos personalizados necessários para autenticação com o serviço Web de destino. Por exemplo, uma etapa REST pode criar um cabeçalho de autenticação, parâmetros de consulta ou um token.

Os algoritmos de autenticação suportam as seguintes etapas:

- Etapa Obter informações de conexão
- Etapa REST
- Etapa SOAP

Para obter mais informações, consulte Etapas de integração

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tipos do algoritmo de autenticação

- **Assinatura da Amazon Versão 4**: este é um algoritmo de autenticação pré-criado para se conectar ao Amazon Web Services.
- **Autenticação personalizada**: este é um modelo que os desenvolvedores podem usar para criar seus próprios algoritmos de autenticação.

Para saber mais sobre como configurar o algoritmo de autenticação, consulte Configure um algoritmo de autenticação.

Scripts

Os scripts de autenticação de instância fazem parte dos scripts de instância da tabela *sys_script_include*.

Scripts de autenticação da instância

RequestAuthInternal	Script somente leitura na instância, que oferece suporte à geração de assinatura AWS V4 ou autenticação personalizada que é enviada com solicitação de saída.
RequestAuthAWSV4Signer	Script que estende RequestAuthInternal para implementar o signatário para gerar a assinatura do AWS V4.
RequestAuthTwitterSigner	Script que estende RequestAuthInternal para implementar o signatário para gerar a assinatura Twitter usando OAuth 1.0a.
RequestAuthSampleCustomSigner	Script de amostra que estende RequestAuthInternal para entender como escrever um signatário personalizado na instância.

Os Scripts de autenticação MID estão na parte de scripts MID da tabela *ecc_agent_script_include*.

Scripts de autenticação MID

RequestAuthInternal	Leia apenas o script no MID, que suporta a geração da assinatura AWS V4 ou a autenticação personalizada que é enviada com a solicitação de saída.
RequestAuthAWSV4MIDSigner	Script que estende RequestAuthInternal para implementar o signatário para gerar a assinatura do AWS V4.
RequestAuthTwitterSigner	Script que estende RequestAuthInternal para implementar o signatário para gerar a assinatura Twitter usando OAuth 1.0a.
RequestAuthSampleMidCustomSigner	Script de amostra que estende RequestAuthInternal para entender como gravar o signatário personalizado no MID.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

APIs JavaScript

A seguir estão as APIs do JavaScript para o algoritmo de autenticação.

- AuthCredential
- HttpRequestAuthedData
- HttpRequestData
- RequestAuthAPI

Configure um algoritmo de autenticação

Configure um algoritmo de autenticação para que você possa assinar solicitações HTTP de saída.

Antes de Iniciar

Você deve ter uma inclusão de script configurada antes de configurar um algoritmo de autenticação.
Função necessária: administrador

Procedimento

1. Navegue até **Todos** > **Credenciais e conexões** > **Algoritmos de autenticação** e clique em **Novo**.
2. No formulário, preencha os campos.
   A seleção do banco de dados no campo **Formato** determina quais campos estão disponíveis.

Formulário de autenticação

Campo	Descrição
Nome	Nome exclusivo deste algoritmo.
Algoritmo	Tipo de solicitação de saída
Descrição	Descrição do que o seu algoritmo faz.
Aplicação	Escopo no qual sua aplicação é executada.
Script de autenticação da instância	Script que você seleciona na tabela Inclusões de script.
Script de autenticação MID	Script que você seleciona da tabela Inclusões de script MID Server [exibição da Descoberta].

3. Clique em **Enviar**.

Configure um Amazon Algoritmo personalizado baseado em assinatura

Gere os dados baseados em Assinatura Amazon necessários para autenticar em um serviço Web executando o script.

Antes de Iniciar

- Conhecimento JavaScript
- Conhecimento REST

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Conhecimento de API de serviço Web de destino
- Conhecimento de conexão, credencial e alias
- Função necessária: desenvolvedor

Por Que e Quando Desempenhar Esta Tarefa

Use um alias de conexão e de credencial e o algoritmo baseado em Assinatura Amazon Versão 4 para autenticação.

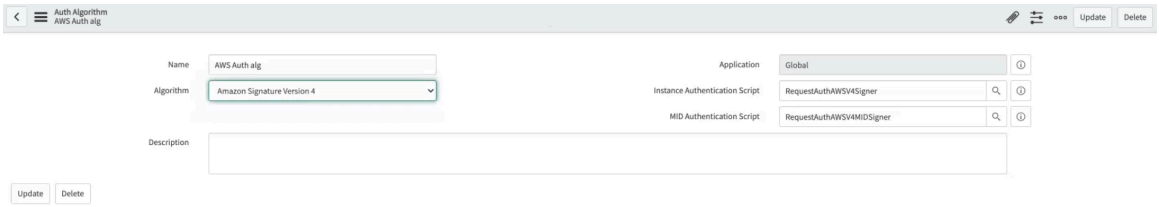
Procedimento

1. Navegue até **Todos** > **Credenciais e conexões** > **Algoritmos de autenticação** e clique em **Novo**.
2. No formulário, preencha os campos.
   A seleção do banco de dados no campo **Formato** determina quais campos estão disponíveis.

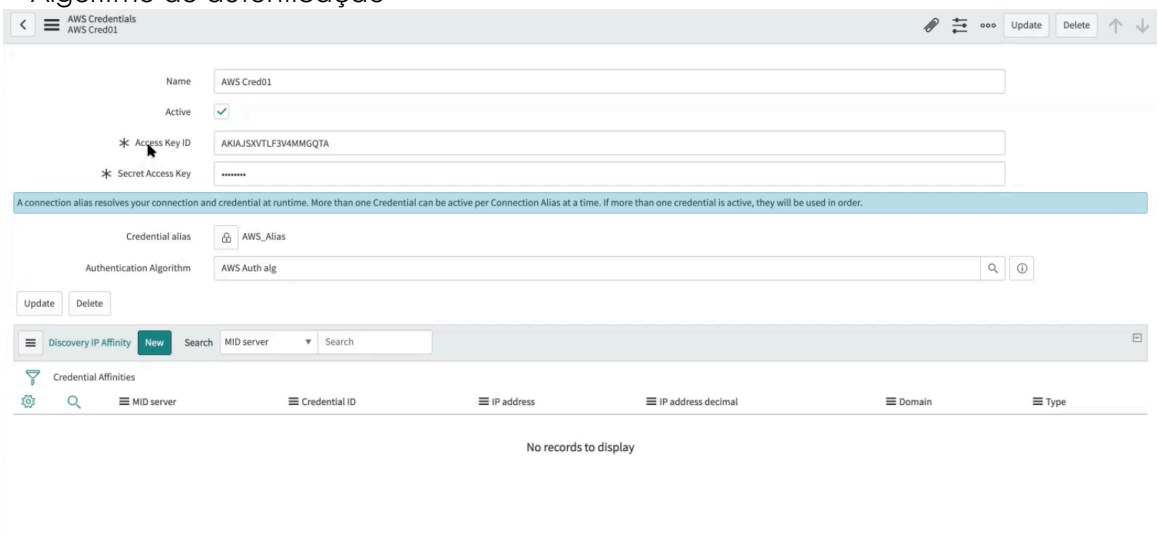
Formulário de autenticação

Campo	Descrição
Nome	Nome exclusivo deste algoritmo.
Algoritmo	Tipo de solicitação de saída. Selecione **Assinatura Amazon Versão 4**.
Descrição	Descrição do que o seu algoritmo faz.
Aplicação	Escopo no qual sua aplicação é executada.
Script de autenticação da instância	Script que você seleciona na tabela Inclusões de script. No caso do algoritmo **Assinatura da Amazon Versão 4**, escolha **RequestAuthAWSV4Signer**. Os scripts disponíveis são os seguintes: ◦ RequestAuthAWSV4Signer ◦ RequestAuthInternal ◦ RequestAuthSampleCustomSigner ◦ RequestAuthTwitterSigner **Nota:** Para saber mais sobre o script, clique no ícone de informações junto ao campo. São exibidos detalhes do script, tais como Nome, Nome de API, Aplicação, Acessível de, Script e assim por diante.
Script de autenticação MID	Script que você seleciona da tabela Inclusões de script MID Server [exibição da Descoberta]. Os scripts disponíveis são os seguintes: ◦ RequestAuthAWSV4Signer ◦ RequestAuthInternal ◦ RequestAuthSampleCustomSigner ◦ RequestAuthTwitterSigner

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. Clique em **Atualizar**.
4. Navegue até **Todos** > **Conexões e credenciais** > **Credenciais**.
5. Clique em **Nova**.
6. Crie Credenciais AWS com algoritmo de autenticação.
   Neste caso, o **Algoritmo de autenticação AWS**.
7. Especifique o seguinte:
   - Nome
   - Ativo
   - ID da chave de acesso
   - Chave secreta de acesso
   - Alias de credencial
   - Algoritmo de autenticação



8. Clique em **Atualizar**.

Resultados

Com base nos scripts selecionados e algoritmo de autenticação, as credenciais configuradas (**ID de chave de acesso** e **Chave de acesso secreto**) ou as credenciais do usuário (**ID de chave de acesso**, **Chave de acesso secreto** e **Token de sessão**) geram uma assinatura V4 Amazon que é enviada como solicitação de saída de ServiceNow para o provedor (neste caso, AWS).

Example: Etapa REST com o AWS

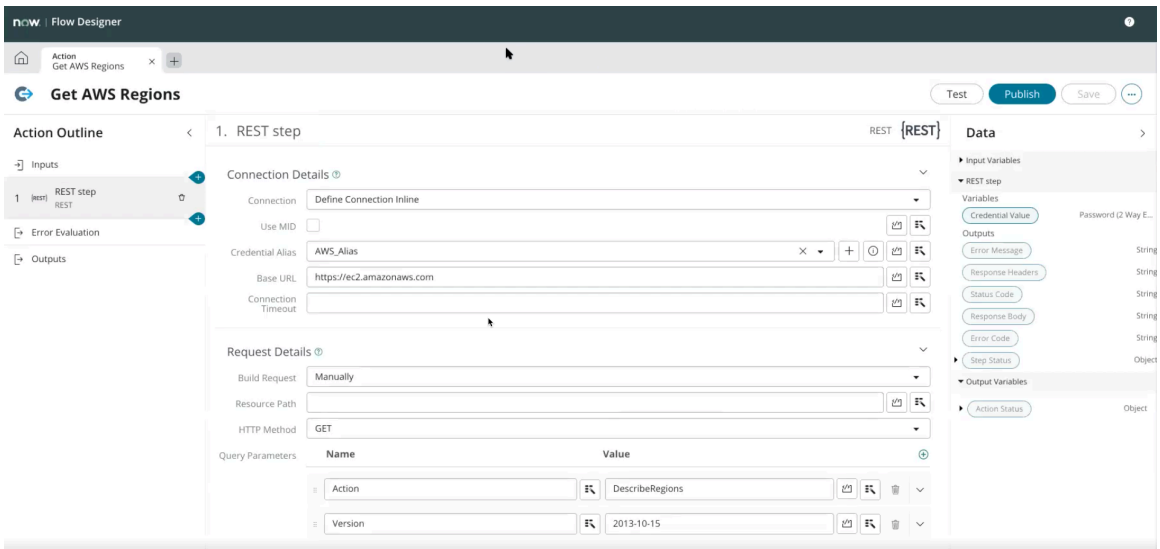
Nota: A autenticação baseada em assinatura Amazon V4 também pode ser usada a partir do plano de fundo do Script.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Ação: obter regiões AWS

Etapa REST de entrada com AWS da seguinte forma:

- **Alias de credenciais**: o alias que é criado para AWS.
- **URL de base**: detalhes de URL de base de AWS.
- **Método HTTPS**: neste caso, é o método GET.
- **Parâmetros de consulta**: **Action** como **DescribeRegions**.



É possível testar a ação, as regiões associadas são exibidas. O corpo da resposta é o seguinte:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Amazon V4 é definido com o conjunto padrão de algoritmo que suporta o mecanismo de autenticação. Este algoritmo quando usado adiciona a assinatura como cabeçalho de autorização para autenticação (solicitação HTTP) usando a etapa REST.

Configure um algoritmo de autenticação personalizado

Gere os dados personalizados necessários para autenticar o serviço Web executando o script.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

- Conhecimento JavaScript
- Conhecimento REST
- Conhecimento de API de serviço Web de destino
- Conhecimento de conexão, credencial e alias
- Função necessária: desenvolvedor

Por Que e Quando Desempenhar Esta Tarefa

Use um alias de conexão e de credencial e o algoritmo baseado em autenticação personalizada para autenticação.

Procedimento

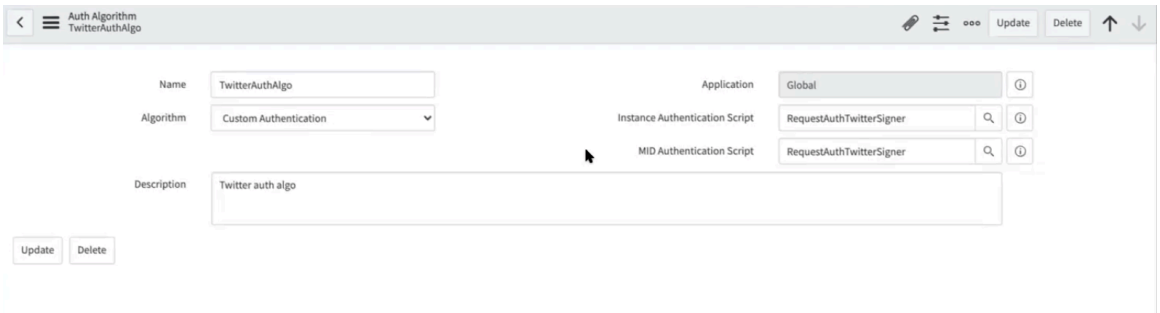
1. Navegue até **Todos** > **Credenciais e conexões** > **Algoritmos de autenticação** e clique em **Novo**.
2. No formulário, preencha os campos.
   A seleção do banco de dados no campo **Formato** determina quais campos estão disponíveis.

Formulário de autenticação

Campo	Descrição
Nome	Nome exclusivo deste algoritmo.
Algoritmo	Tipo de solicitação de saída Selecione **Autenticação personalizada**.
Descrição	Descrição do que o seu algoritmo faz.
Aplicação	Escopo no qual sua aplicação é executada.
Script de autenticação da instância	Script que você seleciona na tabela Inclusões de script. Os scripts disponíveis são os seguintes: ◦ RequestAuthAWSV4Signer ◦ RequestAuthInternal ◦ RequestAuthSampleCustomSigner ◦ RequestAuthTwitterSigner **Nota:** ◦ Para saber mais sobre o script, clique no ícone de informações junto ao campo. São exibidos detalhes do script, tais como Nome, Nome de API, Aplicação, Acessível de, Script e assim por diante. ◦ No caso da autenticação personalizada com Twitter, é possível escolher **RequestAuthTwitterSigner**, já que ele usa um método de autenticação OAuth 1.0a. Isso requer informações como **Chave de API e segredo** e **Token de acesso e segredo** que podem ser usadas para criar assinaturas para passar em um cabeçalho de autorização. Para obter mais informações, consulte Autenticação no Twitter.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

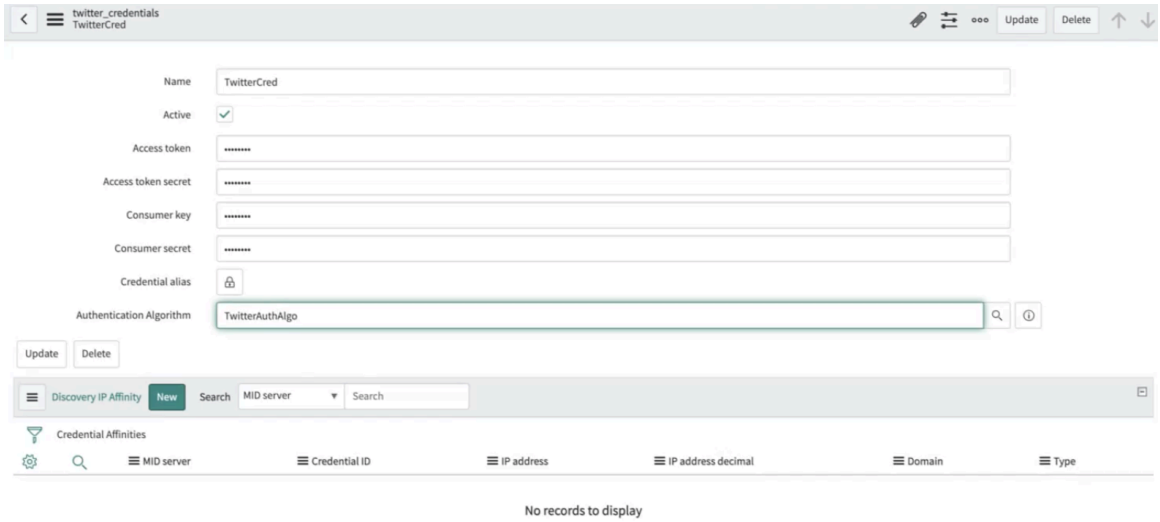
Campo	Descrição
Script de autenticação MID	Script que você seleciona da tabela Inclusões de script MID Server [exibição da Descoberta]. Os scripts disponíveis são os seguintes: ◦ RequestAuthAWSV4Signer ◦ RequestAuthInternal ◦ RequestAuthSampleCustomSigner ◦ RequestAuthTwitterSigner



Com base nos scripts selecionados e no algoritmo de autenticação, as credenciais configuradas são enviadas como solicitação de saída a partir do ServiceNow para o provedor.

3. Clique em **Atualizar**.
4. Navegue até **Todos** > **Conexões e credenciais** > **Credenciais**.
5. Clique em **Nova**.
6. Crie Credenciais Twitter com algoritmo de autenticação.
   Neste caso, **TwitterAuthAlgo**.
7. Especifique os campos:
   - Nome
   - Ativo
   - Token de acesso
   - Segredo do token de acesso
   - Chave do consumidor
   - Segredo do consumidor
   - Alias de credencial
   - Algoritmo de autenticação

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



8. Clique em **Atualizar**.

Example: Etapa REST com Twitter

No caso de Twitter, você deve garantir que os seguintes spokes ou credenciais estejam disponíveis:

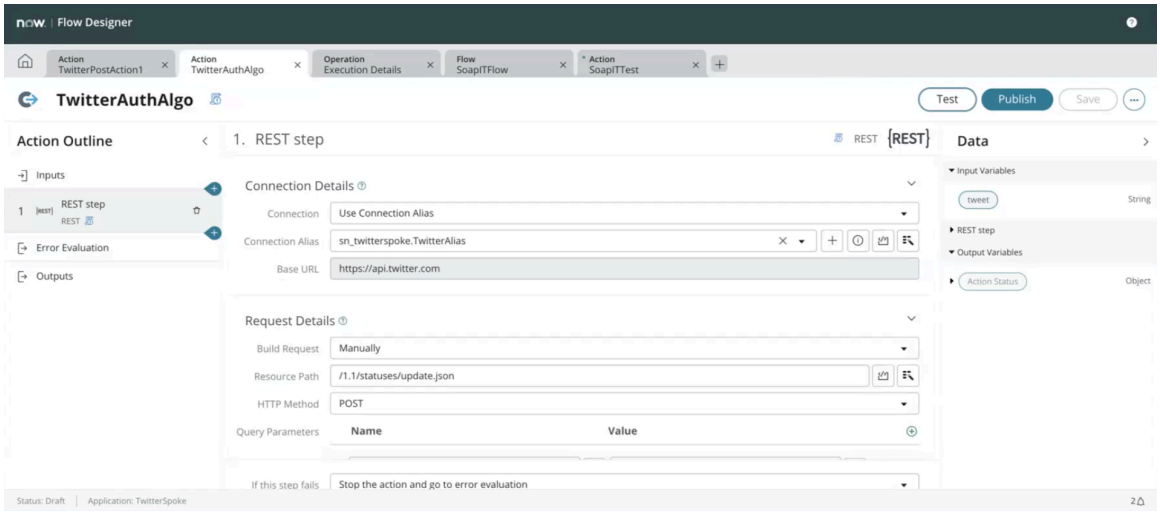
- Token de acesso
- Segredo do token de acesso
- Chave do consumidor
- Segredo do consumidor
- Algoritmo de autenticação

Ação: TwitterAuthAlgo.

Etapa REST de entrada com Twitter da seguinte forma:

- **Alias de credenciais**: o alias que é criado para Twitter.
- **URL de base**: detalhes de URL de base de Twitter.
- **Método HTTPS**: neste caso, é o método POST. Publicação de um tweet.
- **Parâmetros de consulta**: **Action** como **tweet**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



É possível testar a ação. O tweet é publicado na página Twitter.

Verifique a afinidade de serviço IP para Descoberta e Orquestração

É possível verificar a tabela Serviços IP para uma lista de endereços IP que estão associados a um protocolo.

Antes de Iniciar

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

A tabela Serviços IP mapeia uma porta para um protocolo. São fornecidos vários mapeamentos, por padrão, para as combinações de protocolo de porta geralmente usadas, como porta 80 para HTTP, porta 22 para SSH e porta 161 para SNMP.
Uma propriedade do sistema denominada *glide.discovery.ip_service_affinity* permite que Descoberta se lembre da última porta do endereço IP que foi descoberta. Esta propriedade é definida como **falsa** por padrão.

Importante: Você não deve modificar os serviços IP, a menos que sua organização use portas personalizadas.

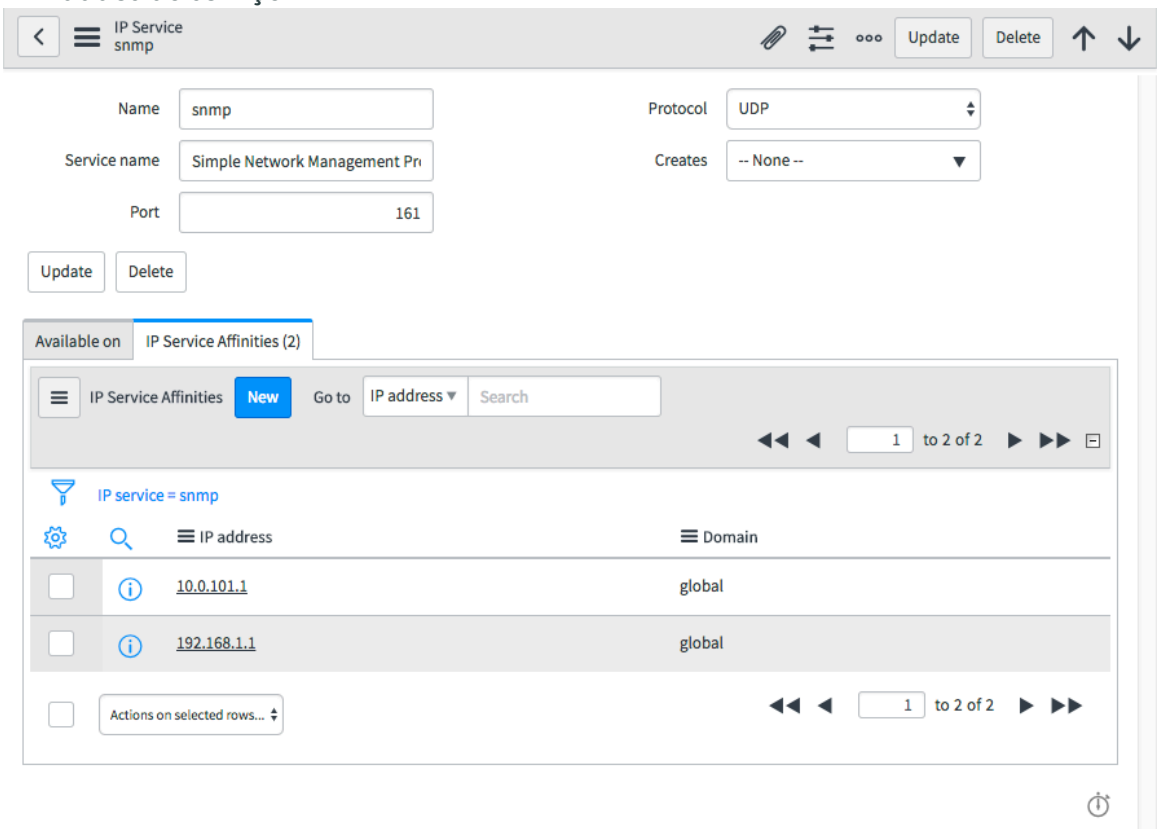
Procedimento

1. Navegue até **Todos** > **Definição do Descoberta** > **Serviços IP**.
2. Filtre a lista para encontrar o serviço IP apropriado.
3. Clique no nome do serviço para ir até essa página de serviço IP.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Clique na guia **Afinidades de serviço IP** para obter a lista de endereços IP associados a esse serviço.

Afinidades do serviço IP



ServiceNow® controle de acesso

O plug-in de controle de acesso do SNC (com.snc.snc_access_control) permite que você controle quais funcionários de Suporte e atendimento ao cliente podem acessar sua instância e quando.

Explore o controle de acesso da ServiceNow

Conheça os recursos do controle de acesso do ServiceNow®.

Ative o controle de acesso da ServiceNow

Ative o controle de acesso do ServiceNow®.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configure o controle de acesso da ServiceNow

Entenda como configurar o controle de acesso do ServiceNow®.

Controle de acesso de referência

Conheça e analise o registro em log de auditoria de controle de acesso ServiceNow®.

Explorar o controle de acesso do ServiceNow®

O plug-in de controle de acesso do SNC (com.snc.snc_access_control) permite que você controle quais funcionários de Suporte e atendimento ao cliente podem acessar sua instância e quando.

Quando você ativa o plug-in pela primeira vez, os funcionários de Suporte e atendimento ao cliente não podem fazer login na instância. Todos os funcionários de Suporte e atendimento ao cliente conectados no momento permanecem conectados. Você cria registros na tabela do SNC Access Control que concede acesso a funcionários específicos do SNC ou a todos os funcionários.

O plug-in evita que a equipe de Suporte e atendimento ao cliente acesse as instâncias sem sua permissão expressa. No entanto, outra equipe de operações autorizada da ServiceNow, em sua capacidade de oferecer suporte e gerenciar o produto e verificar o uso, é obrigada a executar ações administrativas na infraestrutura subjacente. Essa infraestrutura inclui servidores e bancos de dados, entre outros componentes de infraestrutura que compõem a solução SaaS. Este método de acesso é totalmente auditável e rastreado.

Este plug-in permite que você restrinja o acesso à sua instância sem sua permissão expressa, portanto, isso pode afetar os níveis de serviço de suporte e o ANS de disponibilidade. O ANS de disponibilidade é medido a partir do momento em que a equipe de suporte recebe acesso à sua instância.

Segurança de login

A segurança para logins de funcionários de Suporte e atendimento ao cliente autorizados em instâncias emprega tokens criptografados gerados por um servidor seguro. Somente funcionários de Suporte e atendimento ao cliente autenticados corretamente têm acesso a uma instância. Sem o plug-in SNC Access Control, o servidor de segurança garante que os direitos de acesso sejam impostos em hi.service-now.com. Quando o plug-in está habilitado, os tokens de login criptografados devem corresponder aos nomes na lista de acesso fornecida pelo plug-in, usando os critérios definidos nesses registros. Este método de autenticação permite determinar com precisão quais funcionários de Suporte e atendimento ao cliente poderão acessar suas instâncias e quando esses funcionários poderão fazer isso.

A arquitetura escolhida para este sistema tem vários recursos projetados para aprimorar a segurança de suas instâncias:

- Servidor de segurança

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O servidor de segurança é um host Linux bloqueado que somente a equipe de segurança da ServiceNow pode acessar. Este servidor é o único sistema que tem acesso à chave de criptografia privada crítica necessária para produzir os tokens de login. Ao usar essa compartimentalização (uma prática de segurança padrão), a chave privada é protegida, mesmo no caso improvável de um invasor comprometer a instância do HI.

Usuário sintético

O recurso em instâncias que permite aos funcionários de Suporte e atendimento ao cliente autorizados fazer login em sua instância não requer que uma conta seja provisionada nessa instância. Não há registro de usuário provisionado e credenciais permanentes ou persistentes. Em vez disso, um usuário sintético é criado para cada logon de funcionário de Suporte e atendimento ao cliente. Este usuário existe somente na memória e não fornece privilégios contínuos. Se o plug-in SNC Access Control estiver habilitado, você poderá desautorizar qualquer funcionário de Suporte e atendimento ao cliente a qualquer momento.

Tokens

Os tokens de segurança são específicos para uma instância e um funcionário de Suporte e atendimento ao cliente específico. Além disso, o mecanismo que gera os tokens funciona somente com logins de funcionários de Suporte e atendimento ao cliente reais no HI, e não com usuários representados. Depois que um token de segurança é gerado, somente um funcionário de Suporte e atendimento ao cliente específico pode usá-lo para fazer login em uma instância.

Limite de tempo

Os tokens de segurança expiram quatro horas depois de serem gerados. Esta validade limita a utilidade de tokens sequestrados, que só podem ser usados durante esta janela curta.

Registro em Log

Os logins de funcionários de Suporte e atendimento ao cliente em instâncias são registrados como um evento de login.

- Cada ação realizada pelo funcionário de Suporte e atendimento ao cliente conectado é adicionada ao log de transações no banco de dados.
- Ela também é adicionado ao log da instância no sistema de arquivos, que está inacessível para a maioria dos funcionários de ServiceNow.
- Logins e ações de funcionários de Suporte e atendimento ao cliente são prontamente identificáveis, já que os nomes de usuário terminam em @snc (como frodo.baggins@snc).

Essas ações fornecem registro em log de segurança fácil de usar, robusto e confiável para acesso de não funcionários.

Fluxo de processamento de segurança

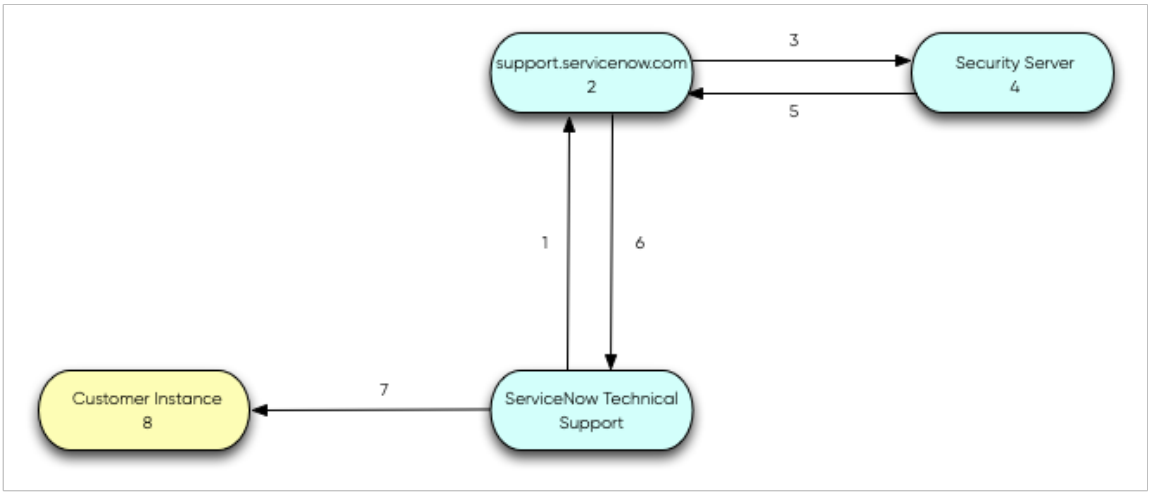
Quando um funcionário Suporte e atendimento ao cliente deseja fazer login em uma instância, o fluxo de processamento de segurança é o seguinte:

1. Um técnico de Suporte e atendimento ao cliente solicita um login para a instância por meio de hi.service-now.com.
2. O HI verifica se o técnico tem a função apropriada para autorizar o acesso às instâncias.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Se o usuário tiver a função apropriada, o HI enviará a solicitação de acesso ao Servidor de segurança.
4. O Servidor de segurança verifica se a solicitação veio do endereço IP HI e avalia a solicitação (usuário, função e endereço IP do solicitante). Se a solicitação for válida, o servidor de segurança a aprovará e criará um token. Este token contém o nome do usuário, as funções, o ID da instância e a hora (o início da vida útil do token de 4 horas). Por fim, o Servidor de segurança criptografa o token com a chave de criptografia privada.
5. O Servidor de segurança envia o token criptografado para o HI.
6. O HI envia o token para o navegador do técnico de suporte.
7. O navegador do técnico de suporte inicia um login na instância, usando o nome de usuário especial terminado em `@snc`.
8. A instância usa a chave pública para descriptografar o token. Para verificar o token, a instância a corresponde ao nome de usuário fornecido na etapa anterior, ao ID da instância e à janela de tempo autorizada. Se o plug-in SNC Access Control estiver habilitado, a instância verificará se o usuário está:
   - Listado
   - Ativo
   - Configurado para acessar a instância na janela de tempo atual
9. Se o usuário for autenticado, a instância criará um usuário sintético na memória com as funções fornecidas. Este usuário não persiste depois que o limite de tempo expira, o usuário faz logoff ou a instância é reiniciada.

Fluxo do processo de acesso à segurança da ServiceNow



Registro em log de Auditoria

O registro em log a seguir rastreia logins e atividades por funcionários de Suporte e atendimento ao cliente:

- Logs de eventos: os logs de eventos mostram todos os logins de Suporte e atendimento ao cliente de uma instância.
- Logs de transações: os logs de transações mostram todas as atividades na instância, incluindo todos os esforços para excluir logs.

Nota: Para saber mais sobre este plug-in, consulte Plug-in SNC Access Control nas Configurações de proteção de segurança da instância.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Ativar o controle do acesso ao ServiceNow®

Você solicita ativação do plug-in SNC Access Control (com.snc.snc_access_control).

Antes de Iniciar

Função necessária: administrador

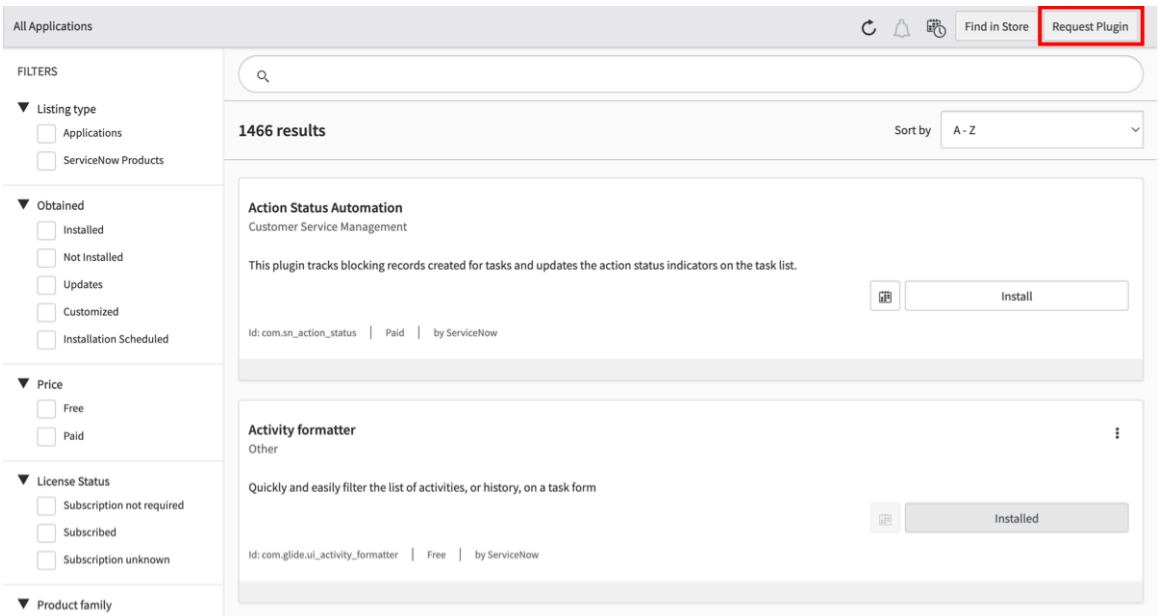
Por Que e Quando Desempenhar Esta Tarefa

Existem duas maneiras de solicitar um plug-in:

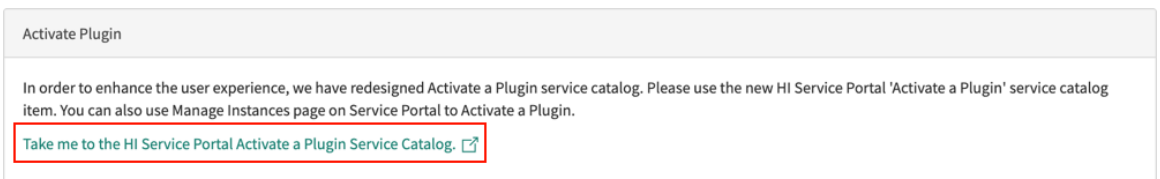
- Acesse o Now Support Catálogo de serviços diretamente clicando em **Todos** > **Catálogo de serviços** > **Ativar plug-in** no Now Support.
- Acesse o Now Support Catálogo de serviços por meio da página Todos os Aplicativos em sua instância, seguindo estas etapas.

Procedimento

1. Navegue até **Todas** > **Aplicações do sistema** > **Todas os aplicações disponíveis** > **Todas**.
2. Na página Todas as Aplicações, selecione **Solicitar plug-in** para abrir o formulário **Ativar plug-in** em Now Support.



3. No Now Support, selecione o link para acessar o Now Support Portal de serviços Catálogo de serviços.



4. Selecione sua instância.
5. Selecione **Ações > Ativar plug-in**.
6. No formulário **Ativar plug-in**, forneça as seguintes informações.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

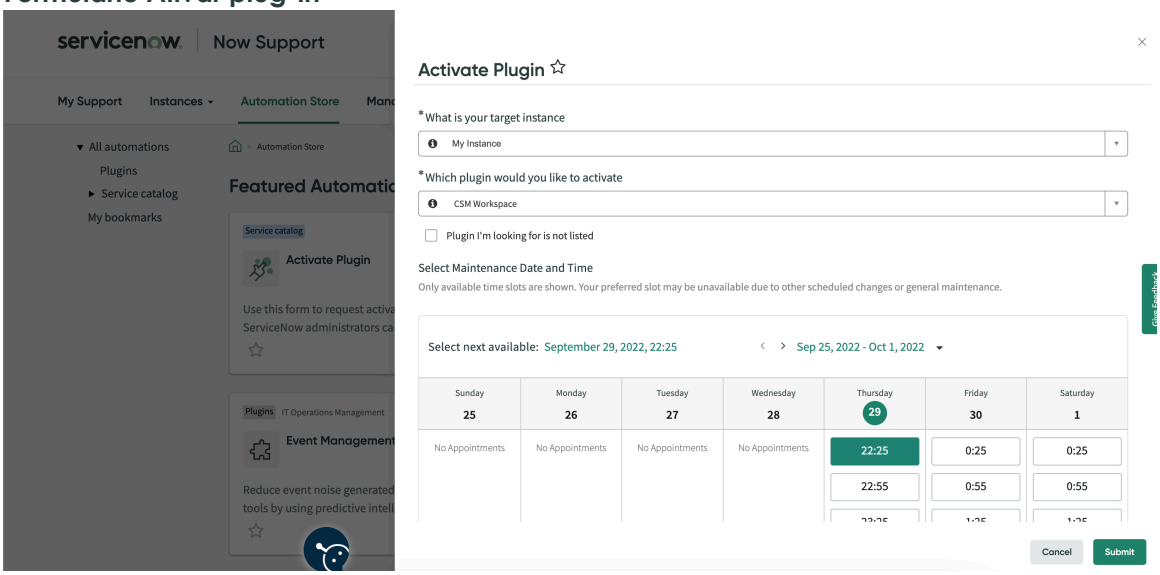
Formulário Ativar plug-in

Campo	Descrição
Qual é a sua instância de destino	Instância na qual o plug-in será ativado.
Qual plug-in você deseja ativar	Nome do plug-in a ser ativado. **Nota:** Se o sistema não listar o plug-in desejado ou se você estiver ativando o plug-in em uma instância do OEM ou no local, marque a caixa de seleção O **plug-in que estou procurando não está listado** e insira o nome do plug-in.
Selecionar data e hora de manutenção	A data e a hora para ativar o plug-in. **Nota:** Os plug-ins são ativados em dois lotes, uma pela manhã e outra à noite, em todos os dias úteis no fuso horário do Pacífico dos EUA. Se o plug-in deve ser ativado em um momento específico, insira a solicitação no campo **Motivo/ Comentários**.

Example

Por exemplo, consulte o formulário a seguir para ativar o plug-in Espaço de trabalho CSM em uma instância chamada Minha instância.

Formulário Ativar plug-in



© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

7. Selecione **Enviar**.
   Para obter detalhes adicionais sobre como solicitar um plug-in, consulte Solicitar um plug-in no artigo do Catálogo de serviços [KB0751715] em Now Support Base de conhecimento.

Configurar o controle de acesso ao ServiceNow®

Configure um registro de controle de acesso para especificar um ou mais funcionários de Suporte e atendimento ao cliente que tenham permissão para fazer login em sua instância.

Antes de Iniciar

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

Nota: O plug-in SNC Access Control (com.snc.snc_access_control) evita que a equipe de Suporte e atendimento ao cliente acesse as instâncias sem sua permissão expressa. No entanto, outra equipe de operações autorizada da ServiceNow, em sua capacidade de oferecer suporte e gerenciar o produto, é obrigada a executar ações administrativas na infraestrutura subjacente. Essa infraestrutura inclui servidores e bancos de dados, entre outros componentes de infraestrutura que compõem a solução SaaS. Este método de acesso é totalmente auditável e rastreado.

Este plug-in permite que você restrinja o acesso à sua instância sem sua permissão expressa, portanto, isso pode afetar os níveis de serviço de suporte e o ANS de disponibilidade. O ANS de disponibilidade é medido a partir do momento em que a equipe de suporte recebe acesso à sua instância.

Procedimento

1. Navegue até **All** > **Segurança do sistema** > **SNC Access Control**.
2. Clique em **Novo**.
3. Preencha os campos de formulário (consultar tabela).
4. Clique em **Enviar**.

SNC Access Control

Campos do formulário	Descrição
Nome	Nomeia cada funcionário de Suporte e atendimento ao cliente que tem permissão para fazer login nesta instância. ◦ Expresse os nomes como nome.sobrenome em letras minúsculas, separados por um ponto (por exemplo, `john.smith`). Cada nome deve ter um registro de usuário correspondente em *`support.servicenow.com`*. ◦ Se mais de um funcionário de Suporte e atendimento ao cliente tiver permissão para fazer login nesta instância, insira vários nomes e separe-os por vírgulas.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campos do formulário	Descrição
	◦ Para habilitar os direitos de login de todos os funcionários de Suporte e atendimento ao cliente para acessar a instância, insira um asterisco (*) no lugar do nome. ◦ Se você pretende restringir o acesso do funcionário de Suporte e atendimento ao cliente à instância, os valores no campo **Nome** não devem ter um asterisco (*****) em qualquer lugar do campo.
Motivo	Campo legível que descreve por que você está concedendo permissão de acesso. Este campo é opcional.
Início	Especifica a data e hora de início do período durante o qual os funcionários de Suporte e atendimento ao cliente especificados têm acesso de login. Este campo é obrigatório.
Fim	Especifica a data e hora de fim do período durante o qual os funcionários de Suporte e atendimento ao cliente especificados têm acesso de login. Este campo é obrigatório.
Ativo	Controla se este registro de permissão está ativo. O padrão é Ativo.

Registro em log de Auditoria

O registro em log a seguir rastreia logins e atividades por funcionários de ServiceNow.

Logs de eventos	Os logs de eventos mostram todos os logins da ServiceNow de uma instância do cliente.
Logs de transações	Os logs de transações mostram todas as atividades na instância, incluindo todos os esforços para excluir logs.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Identidade

Saiba mais sobre as identidades na instância.

Analisador de acesso

O Analisador de acesso é uma aplicação da Store da ServiceNow® que funciona como uma ferramenta de diagnóstico de acesso. Isso ajuda a determinar quem tem acesso a cada recurso.

Identidade global

Identidade Global é um app da Store da ServiceNow® que permite atualizar atributos do usuário de uma instância para outra (várias instâncias).

Central de identidade

A Central de identidade permite monitorar, gerenciar e minimizar o risco com base na identidade e lacunas de segurança.

Sistema de gerenciamento de identidade entre domínios (SCIM)

A API do Sistema de gerenciamento de usuários entre domínios (SCIM) fornece endpoints para criar, ler, atualizar e excluir operações em usuários e grupos usando o protocolo SCIM.

Auditoria de identidade e acesso

Use a Auditoria de identidade e acesso para entender as mudanças feitas em um usuário, grupo, função e ACL.

Análise de acessos

A Análise de acessos da ServiceNow® é uma ferramenta de diagnóstico de acesso que exibe as permissões de uma identidade em relação a um recurso.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Explorar

Conheça os recursos e o valor comercial do Analisador de Acesso.

Usar

Entenda como usar o Analisador de Acesso.

Avaliação de permissão

Saiba como as permissões são avaliadas.

Perguntas frequentes

Veja os detalhes sobre as perguntas mais comuns sobre a Análise de acessos.

Explorando o analisador de acesso

Analise identidades na instância do ServiceNow.

A Análise de acessos da ServiceNow é uma aplicação que ajuda os administradores a exibir permissões para o usuário, a função ou o grupo selecionado.

Nota:

- O Access Analyzer é um produto da loja ServiceNow. Acesse o site ServiceNow Store para ver todos as aplicações disponíveis e obter informações sobre como enviar solicitações para a loja.
- O Access Analyzer representa o registro de identidade para recuperar detalhes sobre as permissões e não lê ou armazena dados pessoais ou confidenciais da identidade.
- Os resultados da avaliação do Access Analyzer são os mesmos, independentemente de quaisquer políticas de acesso definidas para os usuários, como ZTA (Zero trust access, acesso de confiança zero). As políticas são avaliadas somente durante o login real do usuário e não são avaliadas durante o fluxo da Análise de acessos.
- O Access Analyzer tem limitações para avaliar com precisão o acesso dos recursos relacionados aos recursos do escopo gerenciado e ao Delegated Development.

Avaliar acesso

Avaliar acesso é um recurso da Análise de acessos da ServiceNow que ajuda os administradores a exibir permissões para o usuário, a função ou o grupo selecionado.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Ele permite que você analise e exiba as permissões dos usuários, dos grupos ou das funções para uma tabela, inclusões de script de cliente chamável, páginas de IU e endpoints REST.

Usando o Analisador de Acesso, as organizações podem melhorar sua postura de segurança, governança de identidade, gestão de riscos, atingir os objetivos de conformidade dela e entender quem (identidade) tem acesso ao quê (recursos).

Comparar acesso

Comparar acesso é um recurso da Análise de acessos V2 da ServiceNow que permite que os administradores comparem o acesso dos usuários e determinem o nível correto de acesso para os usuários em sua instância da ServiceNow.

É possível utilizar o recurso Comparar acesso entre os usuários para os registros de usuário e o controle de acesso.

Comprar acesso permite que você execute a seguinte análise:

- Nível 1: comparar registros do usuário para entender os atributos, funções e grupos.
- Nível 2: comparar os controles de acesso para executar a análise de causa raiz encontrando problemas de acesso.

Benefícios

Veja, a seguir, alguns benefícios do uso do Access Analyzer:

- Analise o acesso aos recursos (tabelas).
- Compare o acesso de 2 usuários.
- Compare as funções e os grupos de 2 usuários.
- Gere um relatório informando se uma identidade tem acesso a um recurso (tabela).
- Entenda quem tem acesso à higiene de segurança crítica.
- Ajude a impedir o provisionamento excessivo de permissões.
- Obtenha entidades com menos privilégios ao implementar controles de acesso.
- Limite o acesso a determinados dados, incluindo aplicações, tabelas, linhas ou colunas e outros recursos.
- Forneça recursos de emissão de relatórios para os resultados da análise.
- Compare o acesso entre os registros de usuário e os controles de acesso.
- Determine o nível correto de acesso para usuários em sua instância ServiceNow.

Uso do Analisador de acesso

Analise identidades e seu respectivo acesso na instância ServiceNow®.

Antes de Iniciar
Função necessária: admin

O procedimento a seguir descreve as etapas para acessar o Access Analyzer e usar vários recursos de análise de acesso.

Nota: O Access Analyzer é um produto da loja ServiceNow®.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegue até **"Todos"** > **"Access Analyzer"** > **"Analisar permissões"**.
   A página inicial de inicial de Analisar acesso e permissões será exibida.

   A Análise de acessos tem os seguintes recursos:

   - Avaliar acesso
   - Comparar registros de usuários
   - Comparar controles de acesso
2. Selecione a respectiva guia para usar a Análise de acessos com base em seus requisitos.

Usar recurso Avaliar acesso

Analise identidades na instância do ServiceNow®.

Antes de Iniciar

Função necessária: administrador

O procedimento a seguir contém a descrição das etapas para acessar a Análise de acessos e usar seus diversos recursos.

Nota: A Análise de acessos é um produto de ServiceNow Store.

Procedimento

1. Navegue até **Todos** > **Análise de acessos** > **Analisar permissões**.
   A página inicial de inicial de Analisar acesso e permissões será exibida.
2. Selecione a guia **Avaliar acesso**.
3. Selecione seus critérios da seguinte forma:

Selecione seus critérios para analisar acessos e permissões

Campo	Descrição
Analisar por *	Analisar o acesso de um usuário, uma função ou um grupo
Selecionar usuário *	Especifique um nome de usuário da lista.
Tipo de regra *	Analisar o acesso de uma tabela, uma página de IU, um REST Endpoint ou uma inclusão de script de cliente chamável.
Selecionar tabela *	Especifique um nome de tabela da lista para selecionar.
Selecione o registro	Especifique um nome de registro da lista para selecionar.
Selecionar campo	Especifique um nome de campo da lista para selecionar.

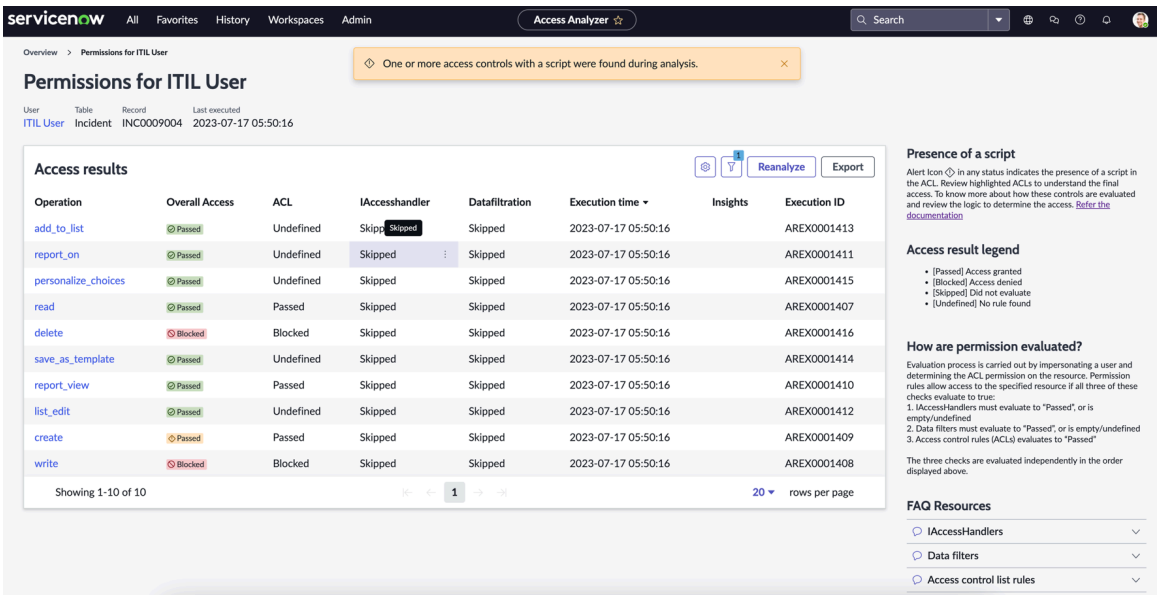
4. Especifique a descrição no campo **Descrição**.
5. Selecione **"Analisar permissões"**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Os resultados de acesso do usuário serão exibidos. Da mesma forma, você pode analisar as permissões de um Grupo ou Função para os seguintes tipos de regra:

- Tabela (registro)
- Inclusão de script de cliente chamável
- Endpoints REST

Os resultados de acesso serão exibidos.



A tabela "Resultados de acesso" inclui os seguintes campos:

Resultados de acesso

Campos	Descrição
Operação	O tipo de operação que o usuário, grupo ou função pode executar para a tabela, registro ou campo selecionado.
Acesso geral	Resultado do acesso geral. Os resultados são os seguintes: ◦ [Passado] Acesso concedido ◦ [Bloqueado] Acesso negado ◦ [Ignorado] Não foi avaliado ◦ [Indefinido] Nenhuma regra encontrada
ACL	Se foi definida uma ACL para a operação selecionada.
IAccesshandler	Trata-se de uma verificação interna do sistema que usa um código fonte oculto na plataforma. IAccessHandler pode conceder ou negar acesso a um recurso sem avaliar ACLs. Se IAccessHandler for ignorado, então as ACLs serão avaliadas.
Filtragem de dados	O filtro de dado é uma forma de controle de acesso projetada para funcionar com

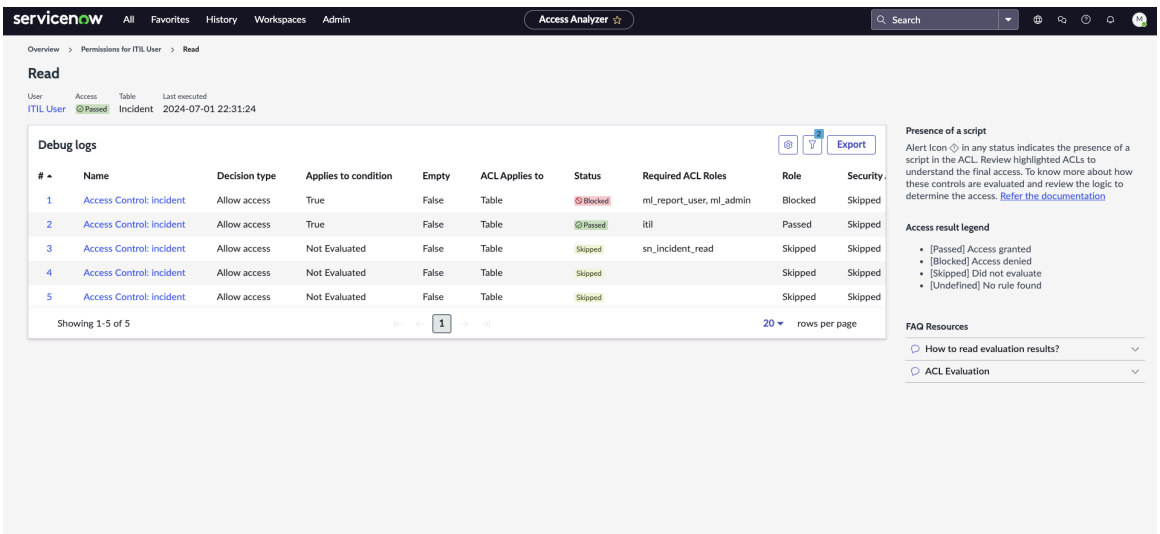
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campos	Descrição
	as ACLs (access control rules, regras de controle de acesso) existentes na instância.
Tempo de execução	A hora em que os resultados de acesso foram executados.
Informações	Mais informações sobre a operação selecionada.
ID da execução	ID exclusivo para cada execução de resultado de acesso.

6. Selecione a "Operação" para obter mais informações sobre a ACL.
   Por exemplo, se você selecionar **leitura**, o controle de acesso relacionado à leitura será exibido.

Detalhes da ACL

Campo	Descrição
Nome	O nome da ACL.
Tipo de decisão	Tipo de decisão configurado para a ACL. **Permitir acesso** ou **Negar acesso**.
Aplica-se à condição	Indica se a ACL é aplicada ou não a uma condição.
ACL se aplica a	Detalhes sobre o recurso ao qual se aplica a ACL.
Status	Status da ACL ou do resultado do acesso.
Funções de ACL necessárias	Detalhes da função necessária para acessar o recurso.
Função	Status da função. Aprovada, Omitida ou Bloqueada.



Permissões de visualização de usuários

Use o Acces Analyzer para visualizar as permissões de um usuário.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Função necessária: administrador

O procedimento a seguir exemplifica as etapas a serem seguidas para visualizar as permissões de um usuário (**ITIL User**) de ver as permissões da tabela **Incidente** usando a avaliação de acesso na Análise de acessos.

Nota: O Access Analyzer é um produto da loja ServiceNow®.

Procedimento

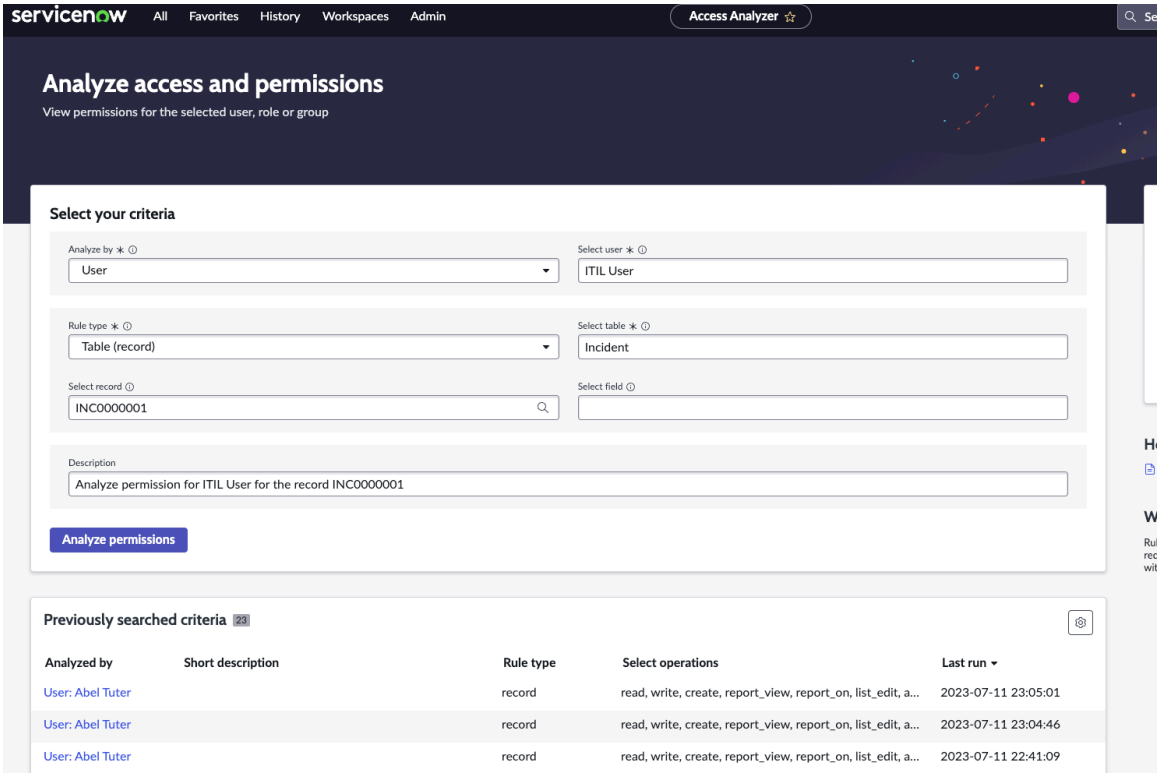
1. Navegue até **"Todos"** > **"Access Analyzer"** > **"Analisar permissões"**.
   A página inicial de inicial de Analisar acesso e permissões será exibida.
2. Selecione seus critérios da seguinte forma:

Selecione seus critérios para analisar acessos e permissões

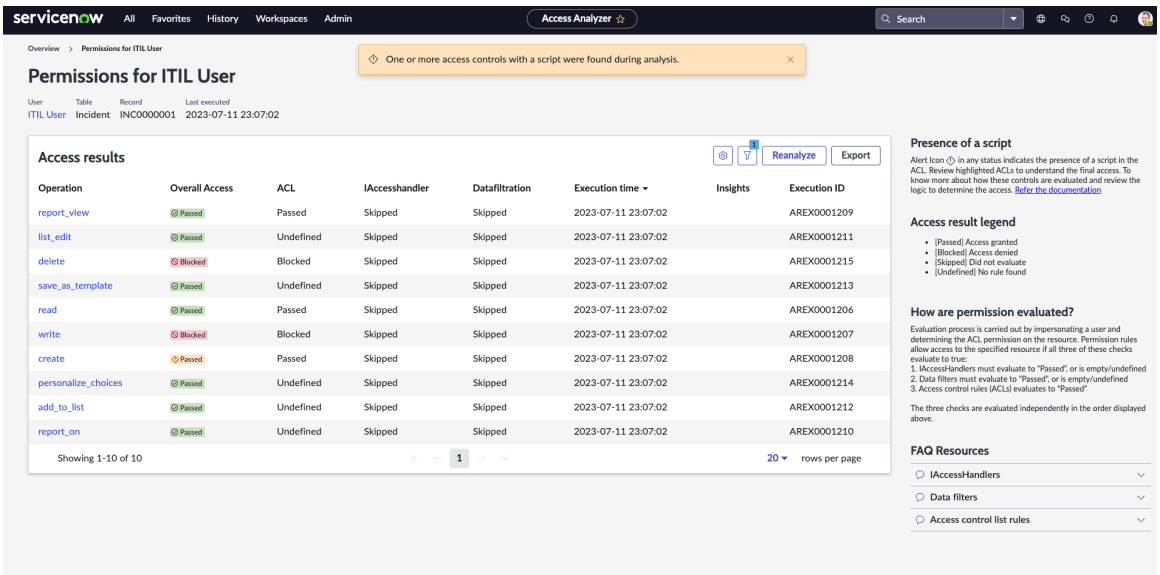
Campo	Descrição
Analisar por *	Selecione **"Usuário"**.
Selecionar usuário *	Especifique um nome de usuário da lista. Neste exemplo, **Usuário ITIL**.
Tipo de regra *	Analisar o acesso de uma **tabela**, uma **página de IU**, um **Endpoint REST** ou uma **inclusão de script de cliente chamável**. No exemplo, `Tabela`.
Selecionar tabela *	Especifique um nome de tabela da lista para selecionar. Neste exemplo, **Incidente**.
Selecione o registro	Especifique um nome de registro da lista para selecionar. Neste exemplo, **INC0000001**.
Selecionar campo	Especifique um nome de campo da lista para selecionar. Este campo pode ser usado para analisar permissão mesmo no nível de campo. Por exemplo, "ativo", "criado por" e assim por diante.

3. Especifique a descrição no campo **Descrição**.
4. Selecione **"Analisar permissões"**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Os **Resultados de acesso** para o **Usuário ITIL** são exibidos.



Os resultados podem ser lidos por referência às legendas, à ACL (access control list, lista de controle de acesso), ao IAccesshandler e aos filtros de dados.

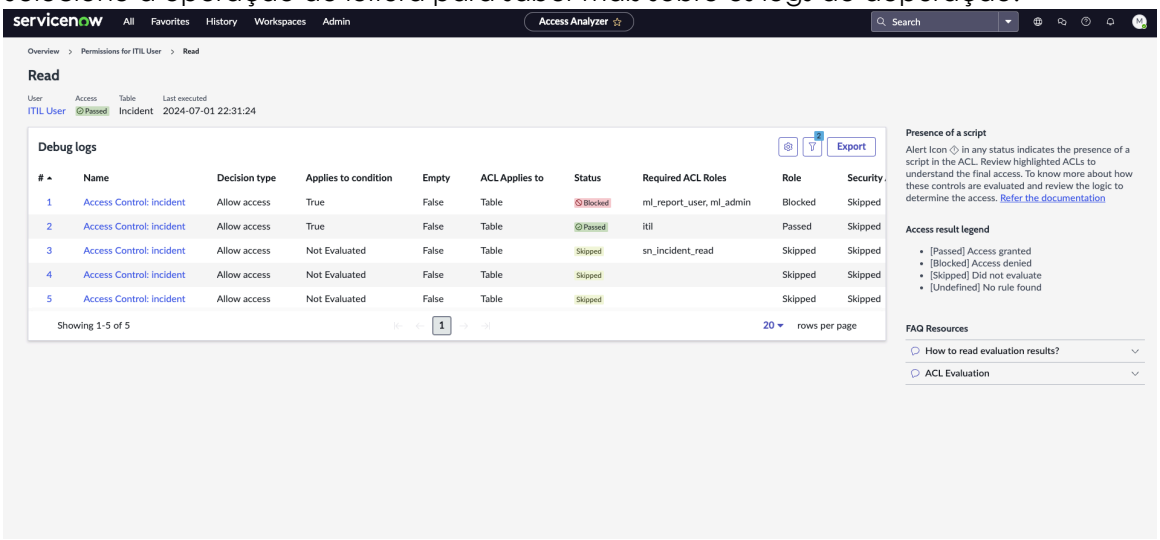
Vamos usar o exemplo da operação de **leitura**. Para o **Usuário ITIL**, o acesso geral é aprovado, o que significa que o usuário pode ler o registro com as permissões (ACL) corretas.

Da mesma forma, para a operação de **criação**, o acesso geral é aprovado com um ícone de alerta, o que significa que pode haver um script para a avaliação da ACL.

Nota: No exemplo, as operações de **escrita** e **exclusão** estão bloqueadas para o usuário selecionado, e ele não pode editar ou excluir o registro selecionado (INC0000001).

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Selecione a operação de leitura para saber mais sobre os logs de depuração.

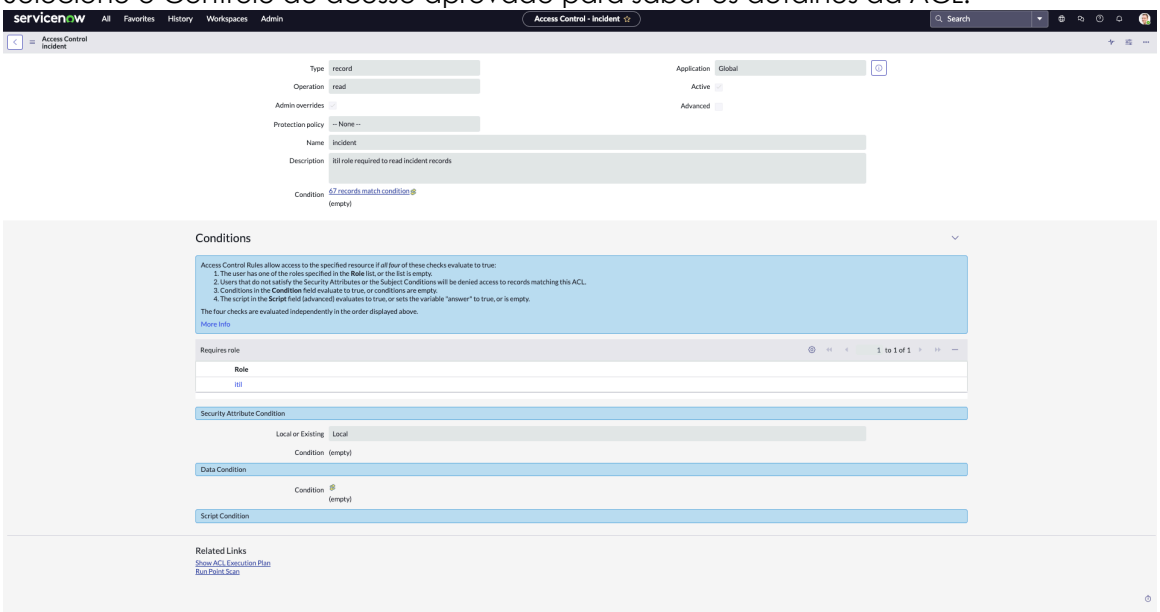


A página Logs de depuração exibiu a regra de negócio e as ACLs associadas que são necessárias para executar a operação de **leitura** do registro.

Os logs de depuração mostram que há uma regra de negócio e 4 ACLs associadas para a operação de leitura.

Há um status de **Aprovado** para uma das ACL, o que significa que, para ler o registro selecionado, o usuário tem a ACL necessária e pode ler o registro. Como uma das ACLs foi **Aprovada**, as outras avaliações da ACL serão **Ignoradas**.

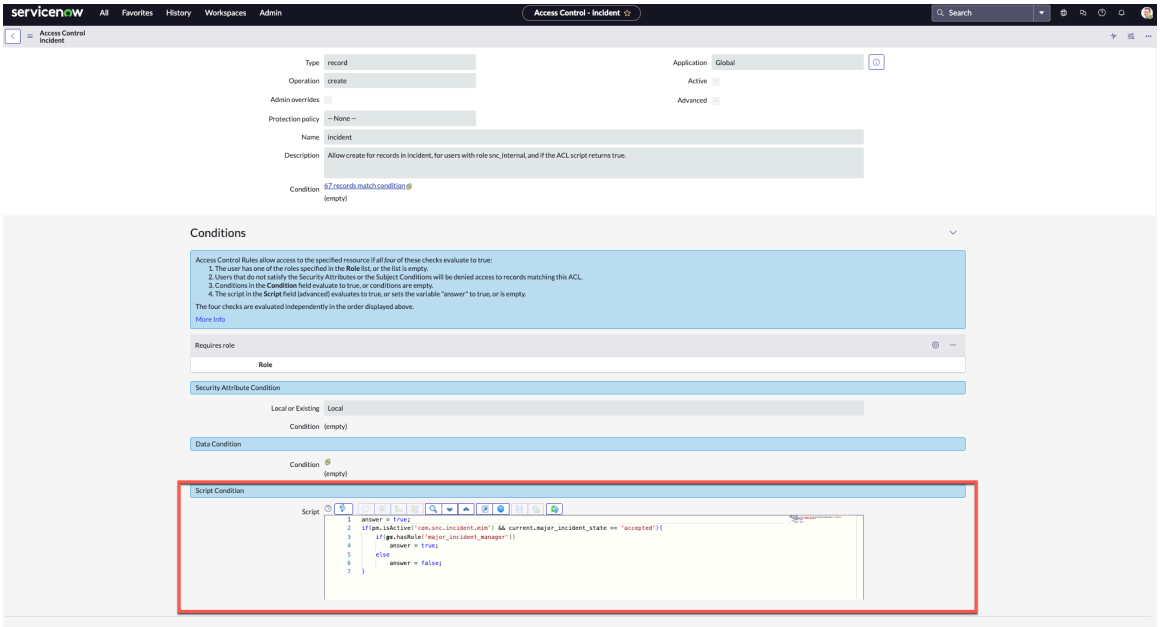
6. Selecione o Controle de acesso aprovado para saber os detalhes da ACL.



Os detalhes do Controle de acesso para a ACL selecionada serão exibidos.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para uma operação selecionada com **Aprovado** e a presença de um script. A página Controle de acesso exibe o script associado ao registro.



Permissões de visualização de uma função

Use o Acces Analyzer para visualizar as permissões de um função.

Antes de Iniciar

Função necessária: administrador

O procedimento a seguir exemplifica as etapas a serem seguidas para visualizar as permissões de uma função (**user_admin**) de ver as permissões do endpoint de REST API usando a Análise de acessos.

Nota: O Access Analyzer é um produto da loja ServiceNow®.

Procedimento

1. Navegue até **"Todos"** > **"Access Analyzer"** > **"Analisar permissões"**.
   A página inicial de inicial de Analisar acesso e permissões será exibida.
2. Selecione seus critérios da seguinte forma:

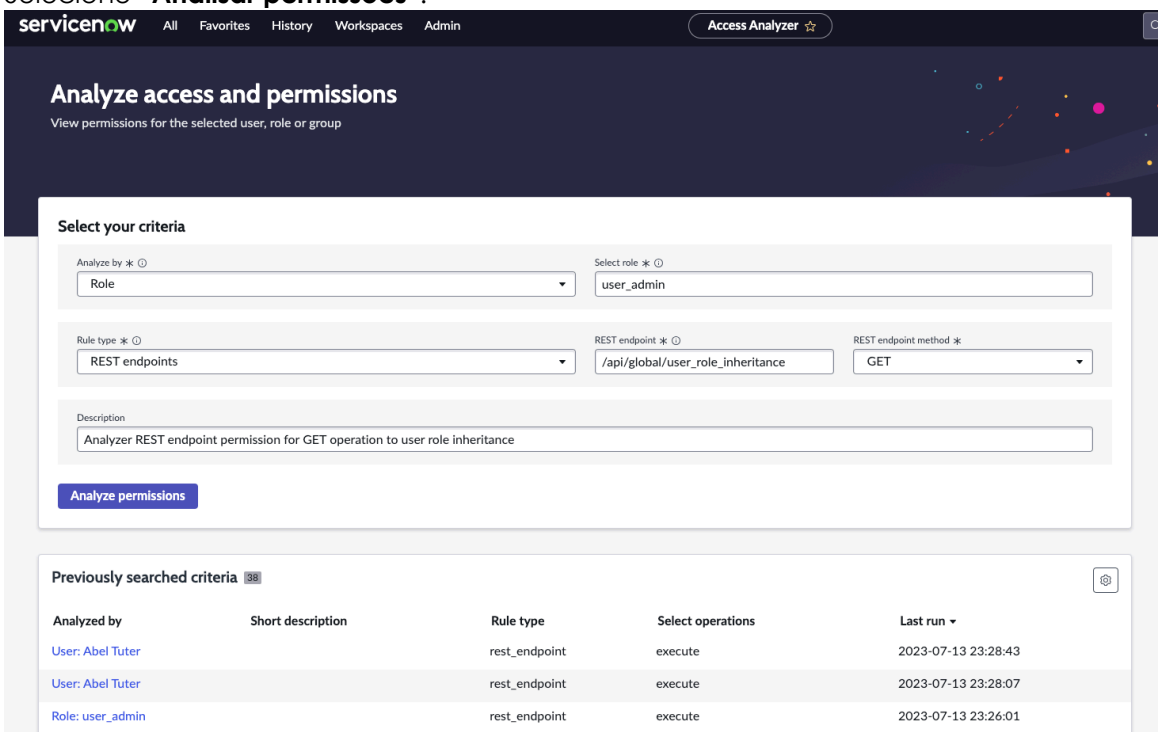
Selecione seus critérios para analisar acessos e permissões

Campo	Descrição
Analisar por *	Selecionar **Função**.
Selecionar usuário *	Especifique uma função a ser selecionada da lista. Por exemplo, **user_admin**.
Tipo de regra *	Analisar o acesso de uma tabela, uma página de IU, um Endpoint REST ou uma inclusão de script de cliente chamável. Por exemplo, **Endpoint REST**.
Endpoint REST*	Especifique um endpoint REST. Por exemplo, `/api/global/user_role_inheritance`.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: O endpoint REST completo deve ser usado ao usar o campo selecionado.
Método de endpoint REST *	Especifique um método de endpoint REST. Por exemplo, GET.

3. Especifique a descrição no campo **Descrição**.
4. Selecione **"Analisar permissões"**.



Os **Resultados de acesso** da função **user_admin** serão exibidos.

Os resultados podem ser lidos por referência às legendas, à ACL (access control list, lista de controle de acesso), ao IAccesshandler e aos filtros de dados.

O acesso geral para a função é aprovado, o que significa que a função (**user_admin**) pode acessar o **endpoint REST** para o método **GET** selecionado.

Exibir permissões para um grupo

Use o Analisador de acesso para exibir as permissões de um grupo.

Antes de Iniciar

Função necessária: administrador

O procedimento a seguir descreve as etapas de exemplo para exibir permissões de um grupo específico (**Gestão de incidentes**) para exibir as permissões de uma página de **IU de incidente** usando a avaliação de acesso na Análise de acessos.

Nota: O Access Analyzer é um produto da loja ServiceNow®.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

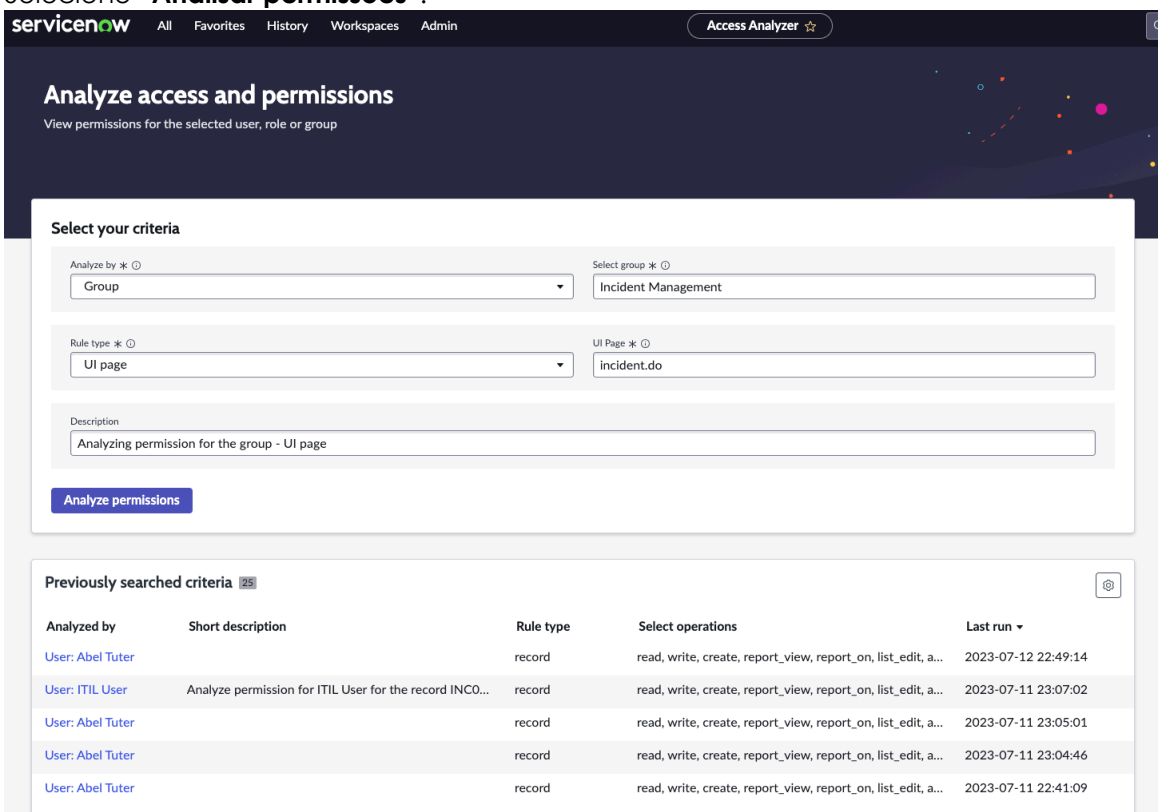
Procedimento

1. Navegue até **"Todos"** > **"Access Analyzer"** > **"Analisar permissões"**.
   A página inicial de inicial de Analisar acesso e permissões será exibida.
2. Selecione seus critérios da seguinte forma:

Selecione seus critérios para analisar acessos e permissões

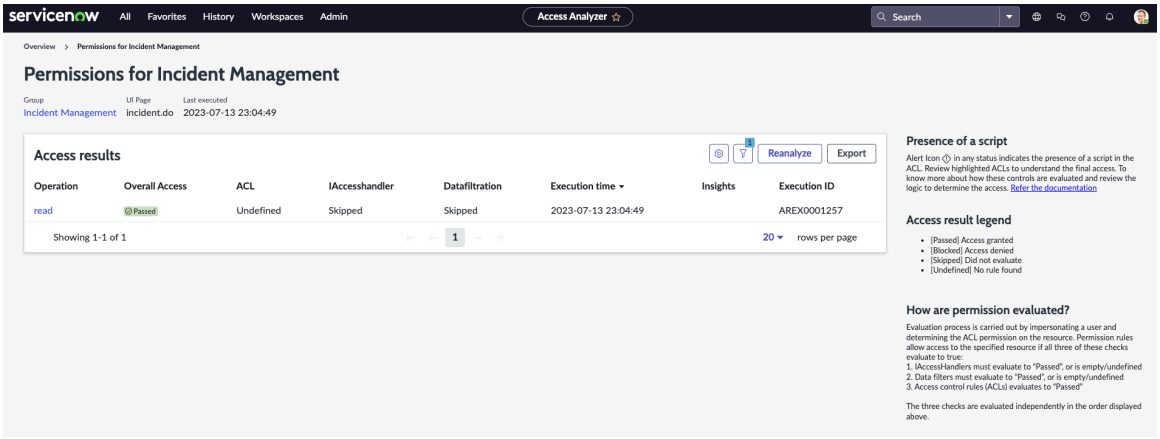
Campo	Descrição
Analisar por *	Selecionar **Grupo**
Selecionar usuário *	Especifique um nome de usuário da lista. Por exemplo, **Gestão de incidentes**.
Tipo de regra *	Analisar o acesso de uma tabela, uma página de IU, um Endpoint REST ou uma inclusão de script de cliente chamável. Por exemplo, **Página de IU**.
Página de IU *	Especifique a página de IU. Por exemplo, **incident.do**.

3. Especifique a descrição no campo **Descrição**.
4. Selecione **"Analisar permissões"**.



Os **Resultados de acesso** para o grupo **Gestão de incidentes** serão exibidos.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Os resultados podem ser lidos por referência às legendas, à ACL (access control list, lista de controle de acesso), ao IAccesshandler e aos filtros de dados.

O acesso geral do grupo é aprovado, o que significa que os usuários do grupo (**Gestão de incidentes**) podem acessar o registro de incidentes.

Exportar consultas do Access Analyzer

Exporte as consultas analisadas usando o Access Analyzer.

Antes de Iniciar

Função necessária: admin

O procedimento a seguir descreve as etapas para acessar o Access Analyzer e usar vários recursos de análise de acesso.

Nota: O Access Analyzer é um produto da loja ServiceNow®.

Procedimento

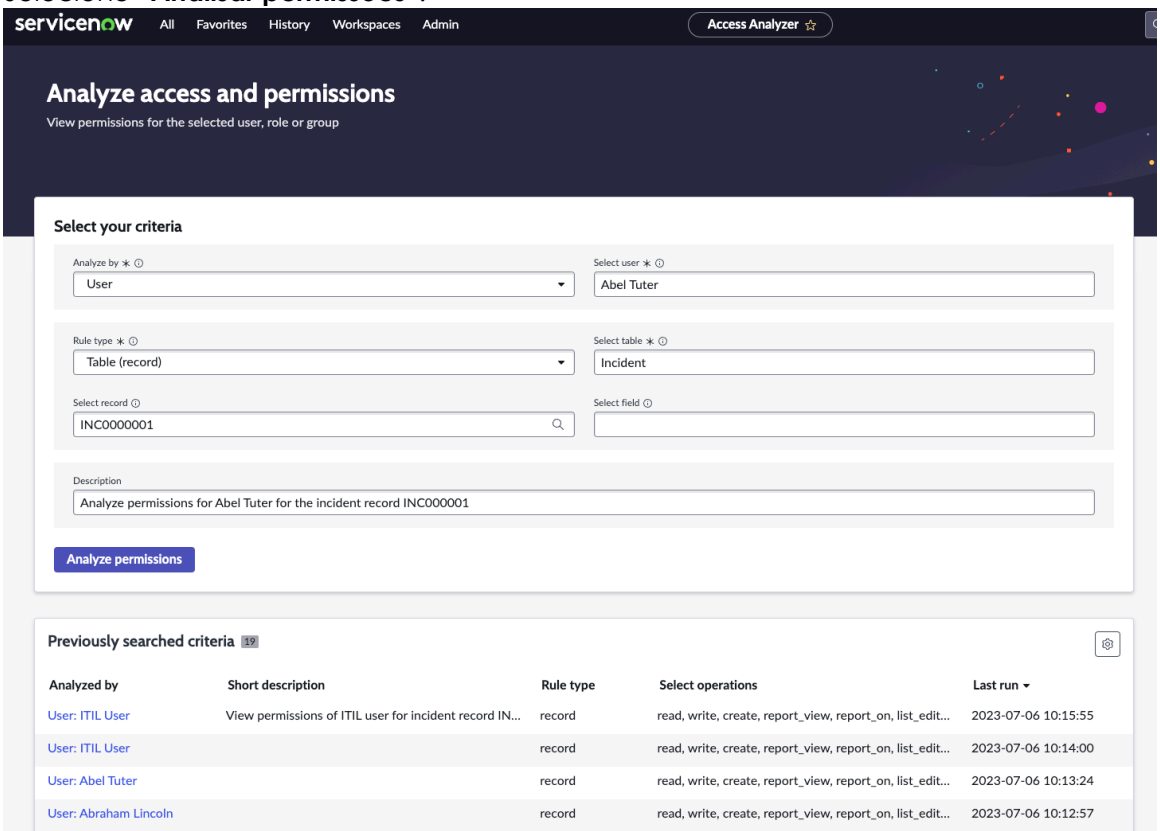
1. Navegue até **"Todos"** > **"Access Analyzer"** > **"Analisar permissões"**.
   A página inicial de inicial de Analisar acesso e permissões será exibida.
2. Selecione seus critérios da seguinte forma:

Selecione seus critérios para analisar acessos e permissões

Campo	Descrição
Analisar por *	Analisar o acesso de um usuário, uma função ou um grupo
Selecionar usuário *	Especifique um nome de usuário da lista.
Tipo de regra *	Analisar o acesso de uma tabela, uma página de IU, um REST Endpoint ou uma inclusão de script de cliente chamável.
Selecionar tabela *	Especifique um nome de tabela da lista para selecionar.
Selecione o registro	Especifique um nome de registro da lista para selecionar.
Selecionar campo	Especifique um nome de campo da lista para selecionar.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

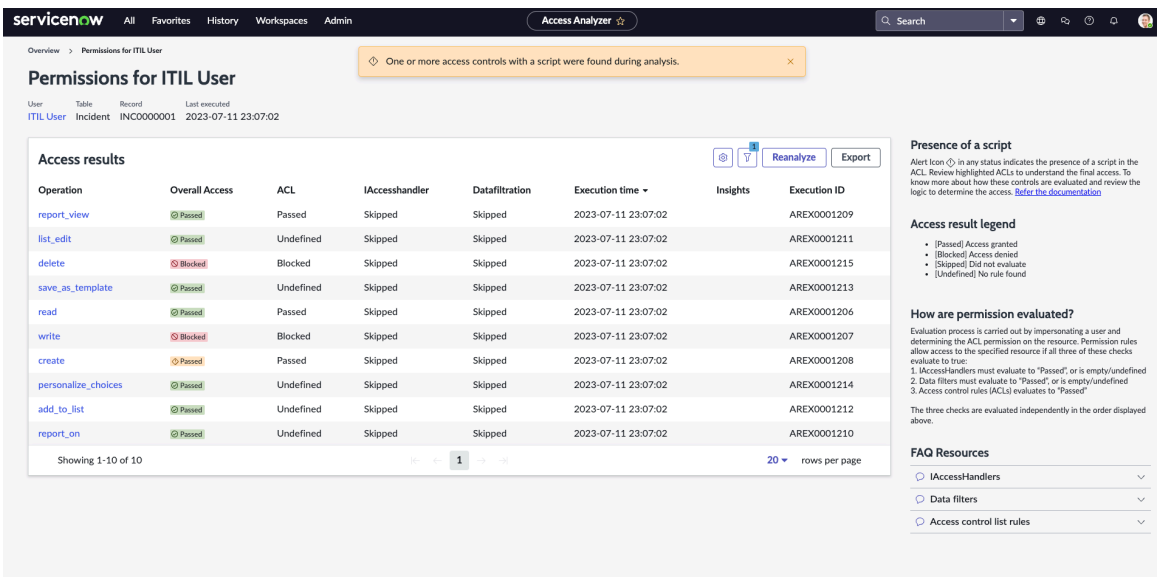
3. Especifique a descrição no campo **Descrição**.
4. Selecione **"Analisar permissões"**.



Os resultados de acesso do usuário serão exibidos. Da mesma forma, você pode analisar as permissões de um Grupo ou Função para os seguintes tipos de regra:

- Tabela (registro)
- Inclusão de script de cliente chamável
- Endpoint REST

Os **Resultados de acesso** para o tipo de regra selecionado serão exibidos.

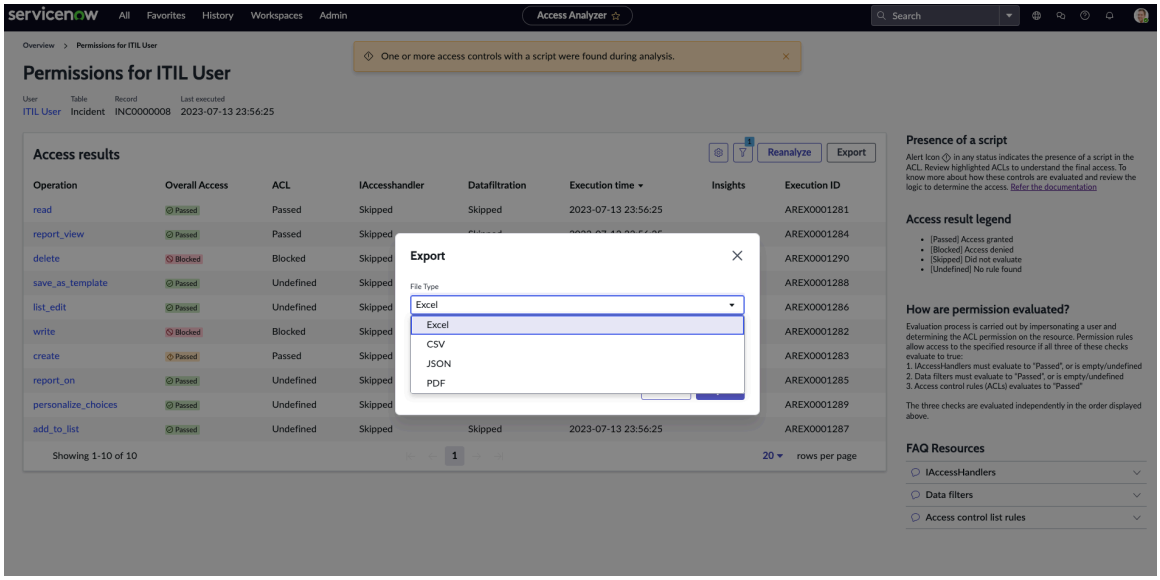


5. Clique em **Exportar**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

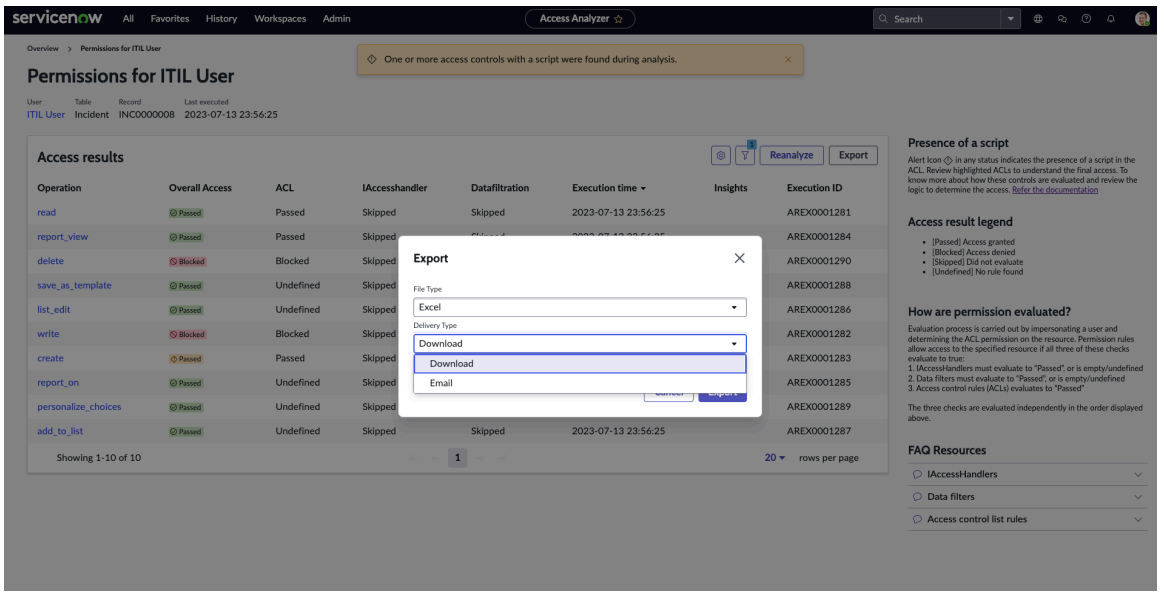
a. Escolha o Tipo de Arquivo.

Os tipos de arquivo disponíveis são Excel, CSV, JSON e PDF.



b. Escolha o Tipo de entrega.

Tipos de entrega disponíveis como Download e E-mail.



Comparar registros de usuários

Compare os registros de usuários para entender o acesso entre dois usuários.

Antes de Iniciar

Função necessária: administrador

O procedimento a seguir contém a descrição das etapas para comparar os registros de usuários usando a Análise de acessos.

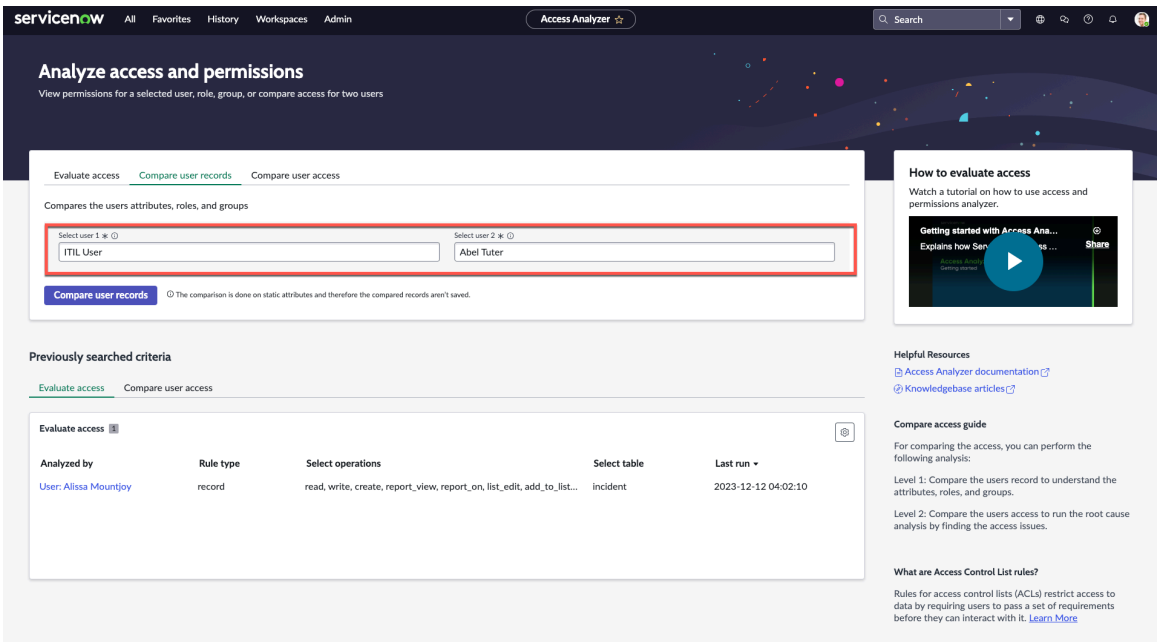
Nota: A Análise de acessos é um produto de ServiceNow® Store.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegue até **Todos** > **Análise de acessos** > **Analisar permissões**.
   A página inicial de inicial de Analisar acesso e permissões será exibida.
2. Selecione a guia **Comparar registros de usuários**.
3. Selecione o **usuário 1** e o **usuário 2** para comparação.

   Por exemplo, `Usuário ITIL` como **usuário 1** e `Abel Tuter` como **usuário 2**.

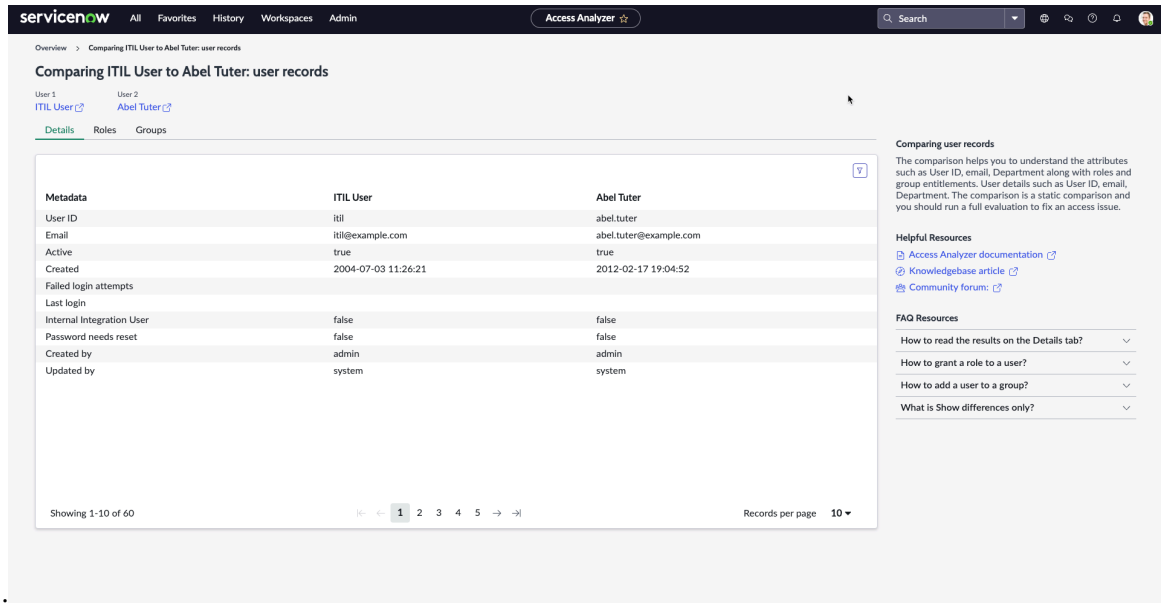


4. Selecione **Comparar registros de usuários**.

   Os resultados serão exibidos com as seguintes guias:

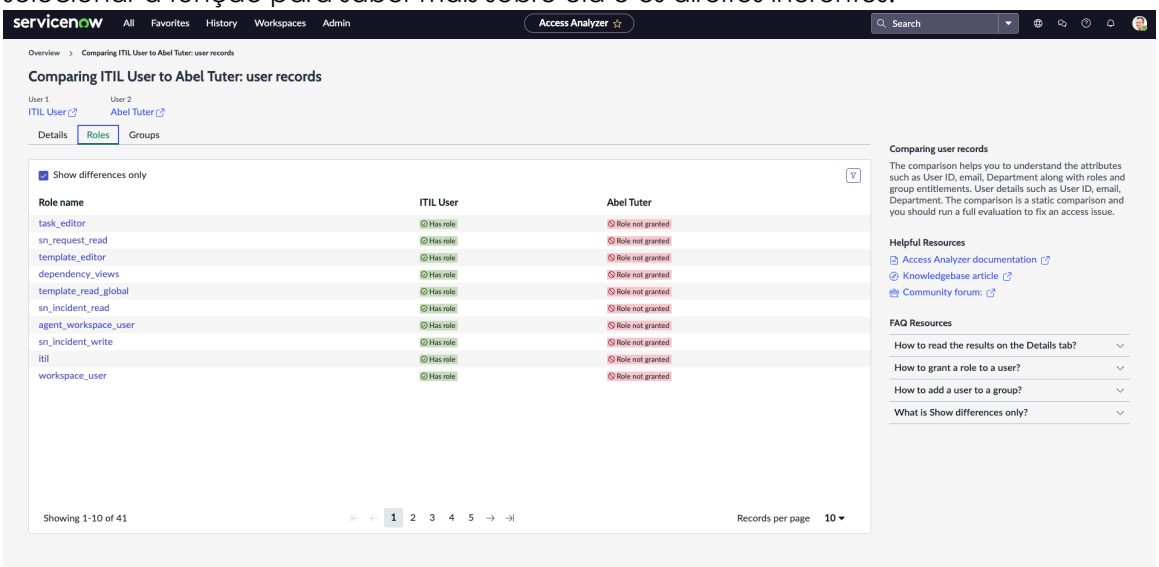
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- **Detalhes**: exibe os metadados do



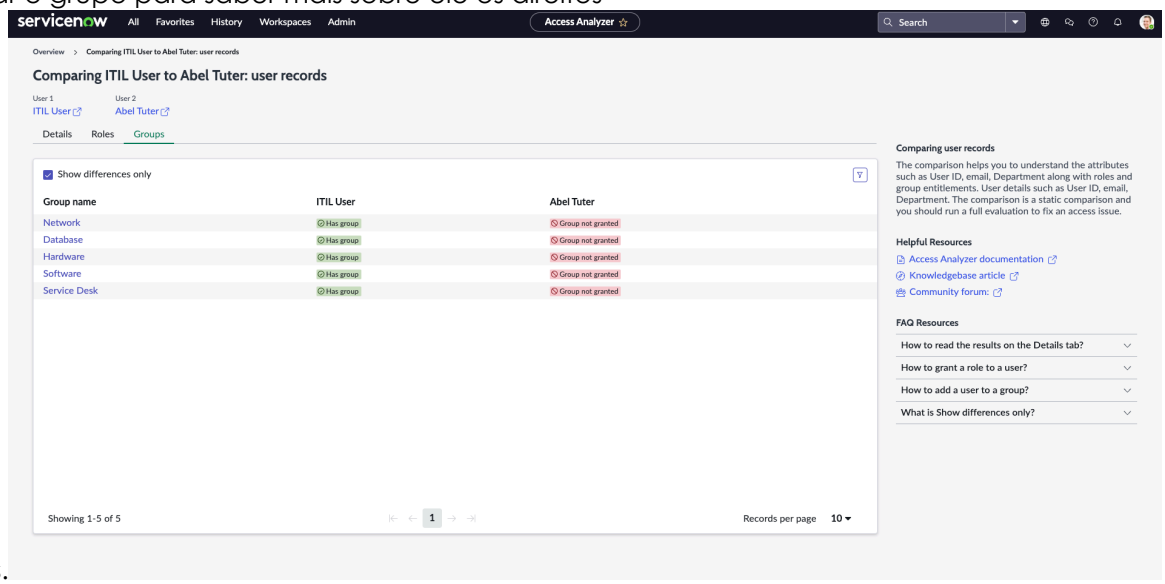
usuário.

- **Funções**: exibe as funções atribuídas ao usuário. Você pode selecionar a função para saber mais sobre ela e os direitos inerentes.



© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- **Grupos**: exibe os grupos atribuídos ao usuário. Você pode selecionar o grupo para saber mais sobre ele os direitos



inerentes.

Você também pode comparar diferentes usuários na instância ServiceNow para entender o acesso atribuído a eles.

Comparação de acessos de usuários

Compare o controle de acesso do usuário usando a Análise de acessos.

Antes de Iniciar

Função necessária: administrador

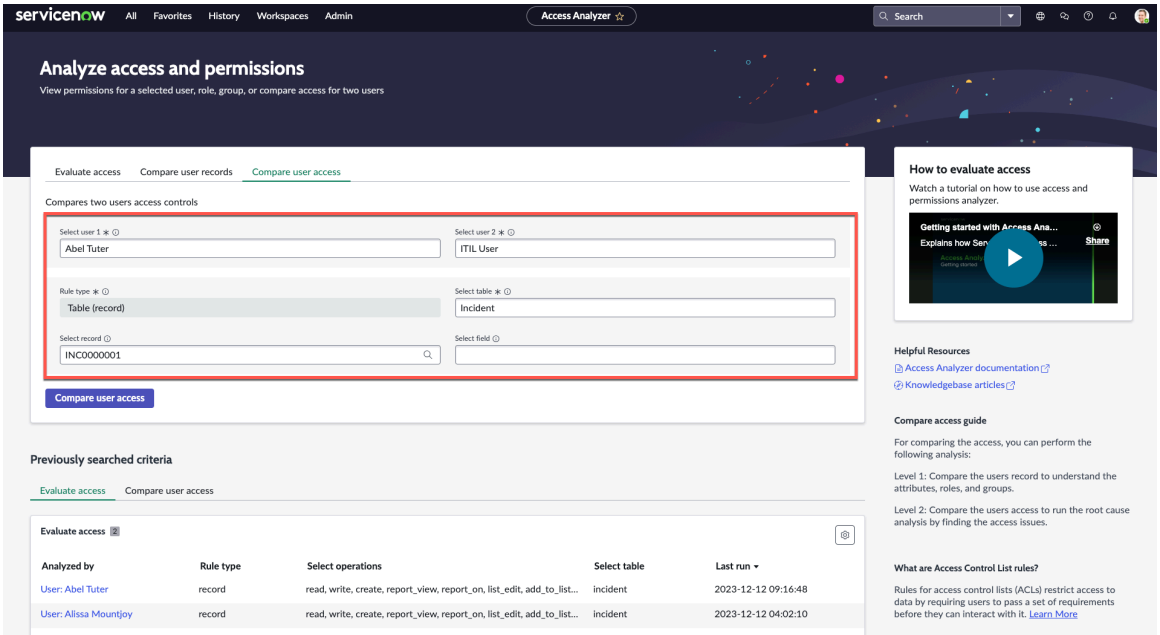
O procedimento a seguir contém a descrição das etapas para comparar o controle de acesso entre os usuários usando a Análise de acessos.

Nota: A Análise de acessos é um produto de ServiceNow® Store.

Procedimento

1. Navegue até **Todos** > **Análise de acessos** > **Analisar permissões**.
   A página inicial de inicial de Analisar acesso e permissões será exibida.
2. Selecione a guia **Comparar acesso do usuário**.
3. Preencha os seguintes campos:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Comparar acesso do usuário

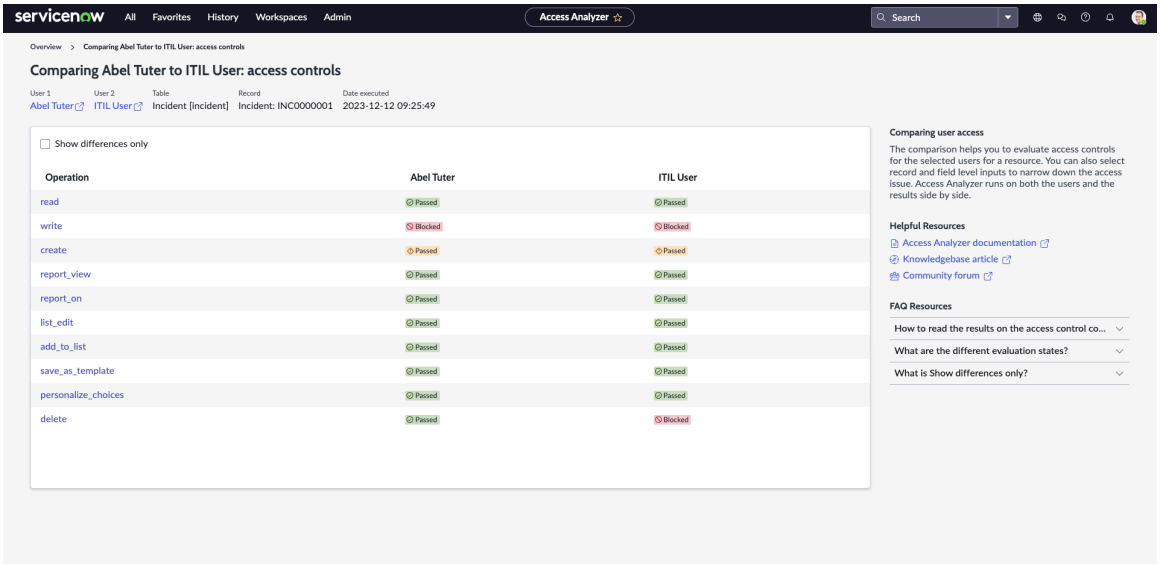
Campo	Descrição
Selecionar usuário 1*	Especifique um nome de usuário da lista para comparação.
Selecionar usuário 2*	Especifique um nome de usuário da lista para comparação com o usuário 1.
Tipo de regra*	Analise as permissões de acesso a uma tabela. **Nota:** Somente as permissões de acesso a uma tabela podem ser usadas em **Comparar acesso do usuário**.
Selecionar tabela*	Especifique um nome de tabela da lista para selecionar.
Selecione o registro	Especifique um nome de registro da lista para selecionar.
Selecionar campo	Especifique um nome de campo da lista para selecionar.

4. Selecione **Comparar acesso do usuário**.

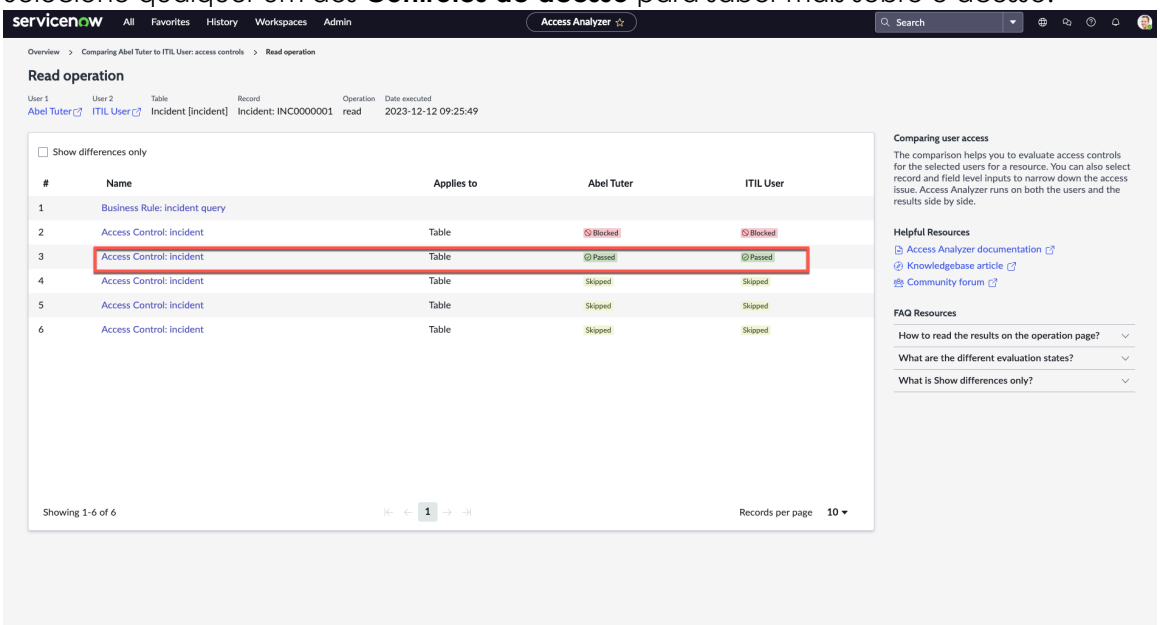
   Os resultados de **Comparar acesso do usuário** serão exibidos para os usuários selecionados.

   Os resultados da comparação de acesso do usuário exibem a operação e o status de avaliação de acesso dos usuários. Por exemplo, Abel Tuter e Usuário ITIL.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

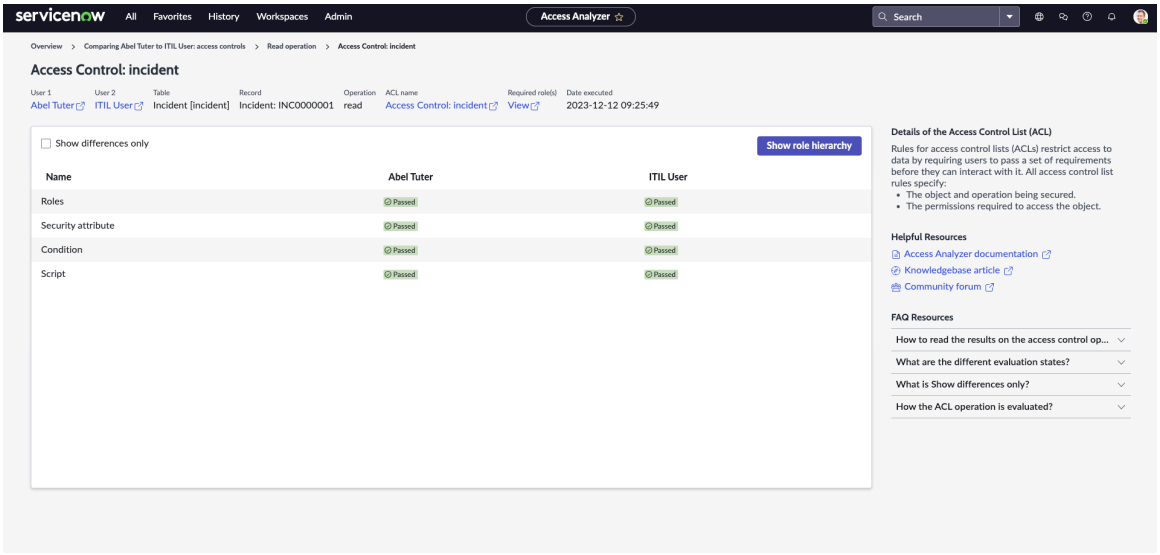


5. Selecione a Operação para saber mais sobre a avaliação de permissão e as funções às quais os usuários estão atribuídos.
   Por exemplo, operação de **leitura**.
6. Selecione qualquer um dos **Controles de acesso** para saber mais sobre o acesso.



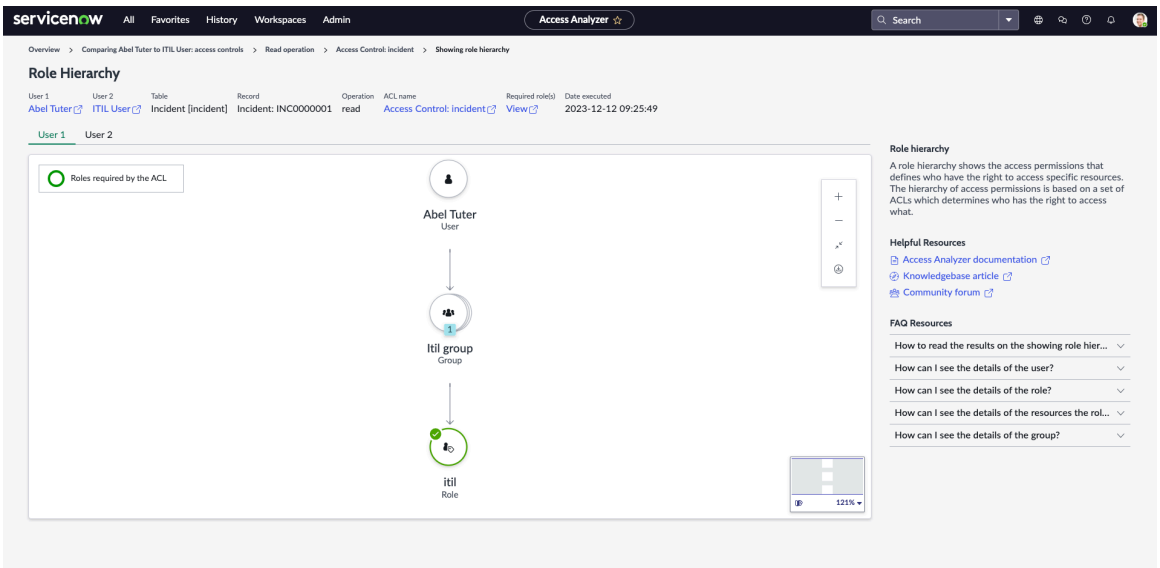
Os detalhes de Controle de acesso, como Funções, Atributo de segurança, Condição e Status de avaliação de script, serão exibidos.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



7. Selecione **Mostrar hierarquia de funções** para saber mais sobre as funções e os grupos aos quais o usuário está atribuído e compare os usuários.

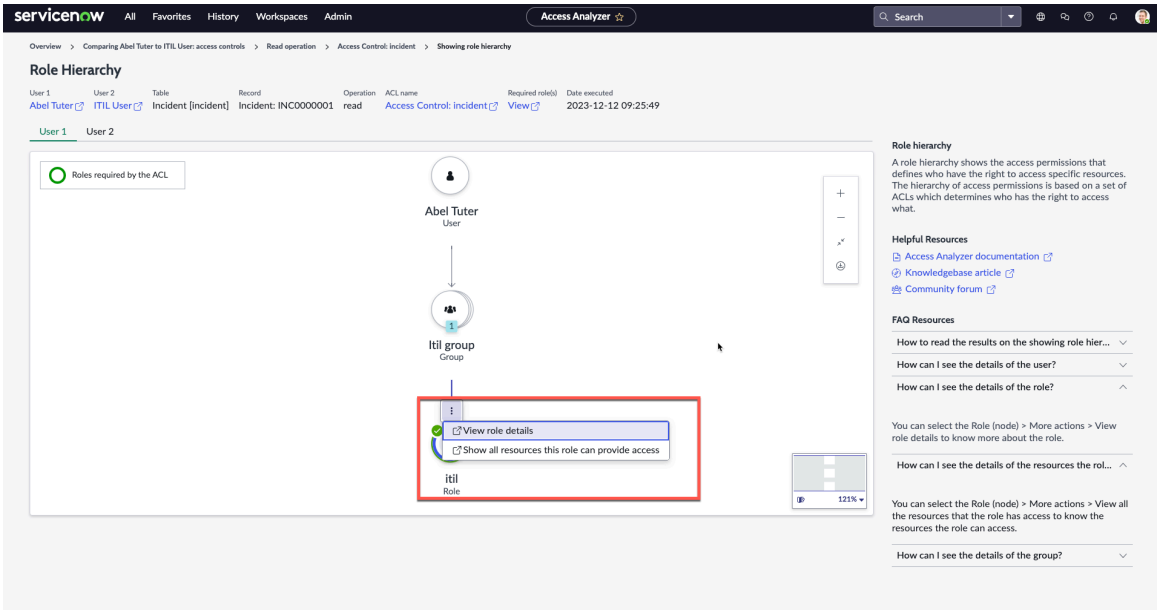
   Com base na hierarquia de funções, você pode realizar as atribuições de função e grupo necessárias ao usuário para que ele tenha acesso aos recursos (tabela).



   No exemplo, os usuários **Abel Tuter** e **ITIL** têm o usuário `itil` atribuído a eles. Dessa forma, o controle de acesso foi aprovado. Você pode determinar as atribuições de função e grupo necessárias para o usuário analisando a hierarquia de funções.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você pode selecionar o nó para saber mais sobre a função, os recursos que a função pode acessar ou o grupo.



Exibir consultas da Análise de acessos - Critérios pesquisados anteriormente

Exibir critérios do analisador de acesso pesquisados anteriormente.

Antes de Iniciar

Função necessária: administrador

Nota: A Análise de acessos é um produto de ServiceNow® Store.

Procedimento

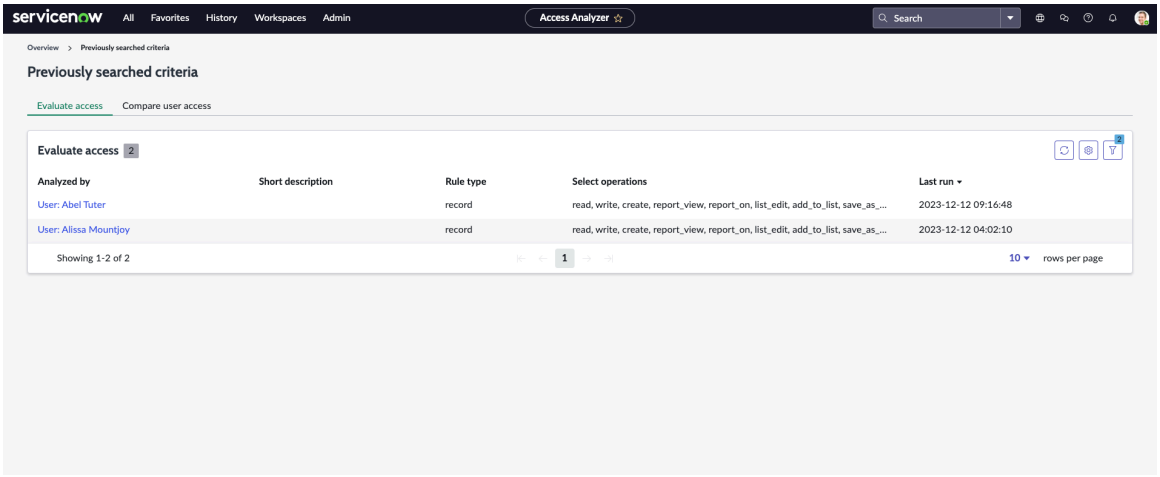
1. Navegue até **Todos** > **Analisador de acesso** > **Consultas do analisador de acesso**.

   Os critérios pesquisados anteriormente contêm as seguintes seções:

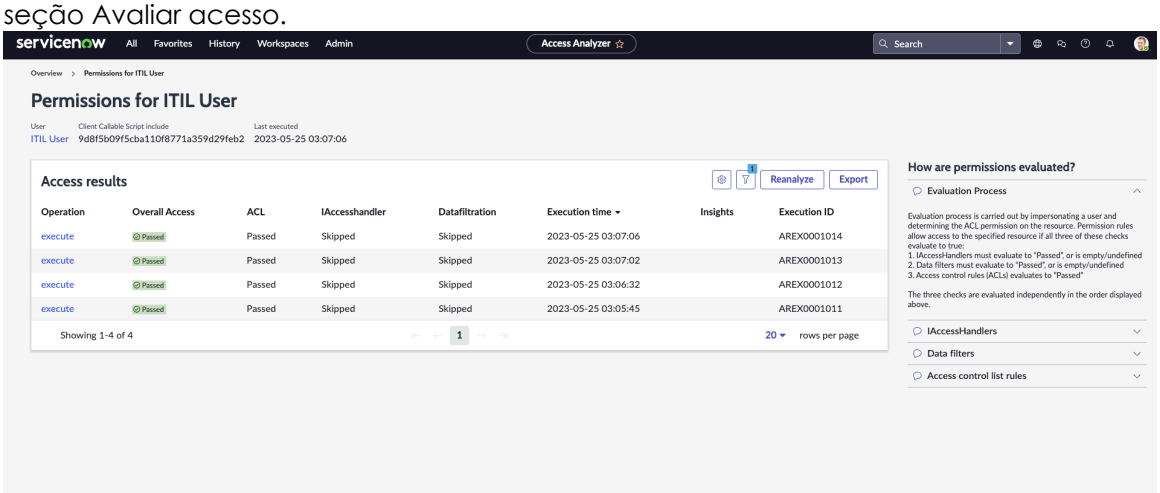
   - **Avaliar acesso**: exibe resultados com base nas consultas feitas por meio dos recursos de **Avaliar acesso**.
   - **Comparar acesso do usuário**: exibe resultados com base nas consultas feitas por meio dos recursos **Comparar acesso do usuário**.

   Nota: Os critérios pesquisados anteriormente não são armazenados ao usar o recurso de comparação de registros de usuários.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

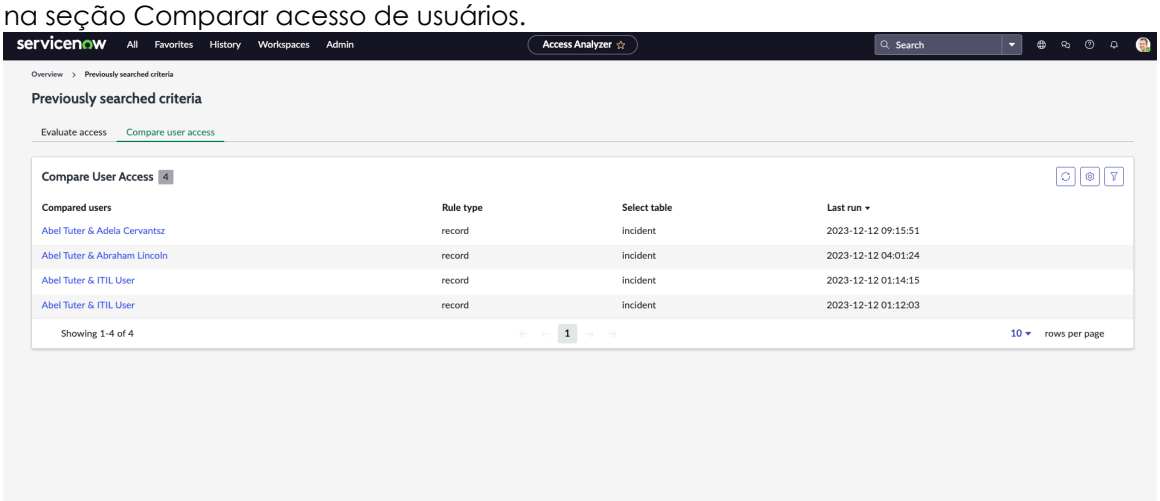


2. Selecione os links **Analisado por** a fim de exibir os critérios pesquisados anteriormente na seção Avaliar acesso.



Você pode **Analisar novamente** o acesso do usuário. Exporte os detalhes usando a opção **Exportar**.

3. Selecione os links **Usuários comparados** para exibir os critérios pesquisados anteriormente na seção Comparar acesso de usuários.



Avaliação de permissão

Critérios de avaliação de permissão ao usar o Access Analyzer.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Hierarquia de avaliação

A permissão do usuário, grupo ou função selecionada é avaliada com base na seguinte hierarquia:

- Regra de negócios: uma regra de negócios é um script relacionado ao servidor que é executado quando um registro é exibido, inserido, atualizado, excluído ou quando uma tabela é consultada.
- Manipulador de acesso: uma verificação interna do sistema que usa um código fonte oculto na plataforma.
- Data Filtration: a filtragem de dados do Data Filtration é uma forma de controle de acesso projetada para funcionar com as ACLs (Access Control rules, Regras de controle de acesso) existentes na instância. O filtro de dados só é compatível com operações de leitura.
- ACL (Lista de controle de acesso): Regras para ACLs restringem o acesso aos dados exigindo que os usuários cumpram com um conjunto de requisitos antes de poderem interagir. A seguinte hierarquia é considerada para as ACLs:
  - Função
  - Atributo de segurança
  - Condição
  - Script

Você pode analisar o acesso e as permissões de determinado usuário, função ou grupo com o Access Analyzer. As permissões são avaliadas com base nos seguintes tipos de regra:

- **Avaliação no nível de tabela**: as ACLs de função e atributo de segurança são usadas para avaliação no nível de tabela.
- **Avaliação no nível de registro ou campo**: as ACLs de nível de função, atributo de segurança, condição e script são usadas para avaliação no nível de registro ou campo.
- **Página de IU**: suporte a operações de somente leitura. Somente ACLs de nível de somente leitura são avaliadas.
- **REST Endpoint**: suporte a operações de execução. Somente ACLs de nível de somente execução são avaliadas.

Os detalhes sobre os campos importantes nos Resultados de acesso são os seguintes:

- Quando há um script disponível
- Acessar legenda do resultado
- Processo de avaliação
- IAccessHandlers
- Filtros de dados
- Regras da lista de controle de acesso

Quando há um script disponível

O ícone de alerta em qualquer status indica a presença de um script na ACL. Revise as ACLs em destaque para entender o último acesso. Para saber mais sobre como esses controles são avaliados e revisar a lógica para determinar o acesso, consulte Logs de depuração do Access Analyzer.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Legendas no Access Analyzer

Ao analisar o acesso e as permissões, as legendas são exibidas como parte do processo de avaliação. Veja as legendas a seguir:

- (Aprovado) Acesso concedido
- [Bloqueado] Acesso negado
- [Ignorado] Não avaliou
- [Indefinido] Nenhuma regra encontrada

Processo de avaliação

O processo de avaliação é realizado representando um usuário e determinando a permissão da lista de controle de acesso (ACL) no recurso. As regras de permissão habilitam o acesso ao recurso especificado se as seguintes verificações estiverem avaliadas como verdadeiras:

- IAccessHandlers deve avaliar como "Aprovado" ou estar vazio ou indefinido
- Os filtros de dados devem avaliar como "Aprovado" ou estar vazio ou indefinido
- Regras de controle de acesso (ACLs) avaliadas como "Aprovado"

IAccessHandlers

Trata-se de uma verificação interna do sistema que usa um código fonte oculto na plataforma. IAccessHandler pode conceder ou negar acesso a um recurso sem avaliar ACLs. Se IAccessHandler for ignorado, então as ACLs serão avaliadas.

Você não pode alterar as verificações do IAccessHandler. Por exemplo, uma implementação IAccessHandler é usada para verificações de acesso em recursos da aplicação, como acessos de leitura.

Filtro de dados

O filtro de dado é uma forma de controle de acesso projetada para funcionar com as ACLs existentes na instância.

Regras da lista de controle de acesso

As regras das listas de controle de acesso (ACLs) restringem o acesso aos dados exigindo que os usuários passem por um conjunto de requisitos antes de interagir com eles.

Perguntas frequentes

Perguntas frequentes ao usar a Análise de acessos.

Avaliar acesso

A seguir você encontra algumas das perguntas mais frequentes ao usar recurso Avaliar acesso da Análise de acessos:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Perguntas frequentes

Perguntas	Explicação
Como ler os resultados da avaliação exibidos pelo Access Analyzer?	Cada linha representa uma lista de controle de acesso (ACL) individual. A sequência (nº) nos resultados representa a ordem na qual as ACLs são avaliadas. O status mostra se o acesso geral foi concedido (aprovado) ou negado (bloqueado).
Como as ACLs são avaliadas?	No nível de tabela, as ACLs são avaliadas somente para funções e atributos de segurança. Condições e scripts não são avaliados. As funções são avaliadas primeiro. Se as funções estiverem bloqueadas, as condições e os scripts serão ignorados. Para obter mais informações, consulte Configuração de uma regra de ACL.
Quais são as legendas do Access Analyzer?	Ao analisar o acesso e as permissões, as legendas são exibidas como parte do processo de avaliação. Veja as legendas a seguir: • [Passado] Acesso concedido • [Bloqueado] Acesso negado • [Ignorado] Não foi avaliado • [Indefinido] Nenhuma regra encontrada
O que significa o ícone de Alerta nos resultados do Access?	O ícone de alerta em qualquer status indica a presença de um script na ACL. Revise as ACLs em destaque para entender o último acesso. Para saber mais sobre como esses controles são avaliados e revisar a lógica para determinar o acesso, consulte Logs de depuração do Access Analyzer.
O que é **IAccesshandler**?	Trata-se de uma verificação interna do sistema que usa um código fonte oculto na plataforma. É uma verificação de segurança do sistema que você não pode modificar. **IAccessHandler** pode conceder ou negar acesso a um recurso sem avaliar ACLs. Se este **IAccessHandler** for ignorado, então as ACLs serão avaliadas. Não é possível modificar as verificações do **IAccessHandler**

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Perguntas frequentes

Perguntas	Explicação
	de forma alguma. Por exemplo, uma implementação **IAccessHandler** é usada para verificações de acesso em recursos da aplicação, como acessos de somente leitura.
O que são filtros de dados?	Os filtros de dados são uma forma de controle de acesso projetada para funcionar com as ACLs (Access Control rules, Regras de controle de acesso) existentes na instância.
O que é uma regra de ACL?	As regras para listas de controle de acesso (ACLs) restringem o acesso aos dados exigindo que os usuários passem por um conjunto de requisitos antes que possam interagir com eles.

Atribuições de função com limite de tempo encontradas para o usuário que podem afetar os resultados. Aqui você pode verificar as funções com limite de tempo atribuídas ao usuário.

Comparar registros de usuários

A seguir você encontra algumas das perguntas mais frequentes ao usar recurso Comparar registros de usuários da Análise de acessos:

Perguntas frequentes

Perguntas	Explicação
Como ler os resultados na guia Detalhes?	A guia Detalhes exibe os metadados associados ao usuário 1 e ao usuário 2
Como conceder uma função a um usuário?	Na guia Usuários, você pode verificar a função que deve ser concedida ao usuário e atribuí-la.
Como adicionar um usuário a um grupo?	Na guia Grupos, você pode verificar o grupo ao qual o usuário deve ser adicionado e adicioná-lo.
O que é Somente mostrar a diferença?	Quando você habilita a caixa de seleção Somente mostrar a diferença, apenas as funções ou o grupo que são diferentes entre o usuário 1 e o usuário 2 são exibidos.

Comparar acesso do usuário

A seguir você encontra algumas das perguntas mais frequentes ao usar recurso Comparar acessos de usuários da Análise de acessos:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Perguntas frequentes

Perguntas	Explicação
Como ler os resultados na página de comparação de controle de acesso?	A página de comparação de controle de acesso exibe os estados de avaliação para diferentes operações de ACL.
Quais são os diferentes estados de avaliação?	Ao comparar os controles de acesso entre os usuários, os diferentes estados de avaliação são: • Aprovado • Bloqueado
O que é Somente mostrar as diferença?	Quando você habilita a caixa de seleção Somente mostrar a diferença, apenas os estados da avaliação da operação que são diferentes entre o usuário 1 e o usuário 2 são exibidos.
Como a operação das ACLs é avaliada?	A ACL (Lista de controle de acesso) é a regras para ACLs que restringe o acesso aos dados exigindo que os usuários cumpram com um conjunto de requisitos antes de poderem interagir. A seguinte hierarquia é considerada para as ACLs: • Função • Atributo de segurança • Condição • Script
Como ler os resultados na página de hierarquia de funções?	A página de hierarquia de funções exibe a função atribuída ao usuário 1 e ao usuário 2. Você pode entender a função exigida para o usuário para uma operação da ACL específica.
Como posso ver os detalhes do usuário?	Você pode selecionar **Usuário (nó)** > **Mais ações** > **Exibir detalhes do usuário** para saber mais sobre o usuário.
Como posso ver os detalhes da função?	Você pode selecionar **Função (nó)** > **Mais ações** > **Exibir detalhes da função** para saber mais sobre a função.
Como posso ver os detalhes dos recursos que a função pode acessar?	Você pode selecionar **Função (nó)** > **Mais ações** > **Exibir todos os recursos aos quais a função tem acesso** para saber os recursos que a função pode acessar.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Perguntas frequentes

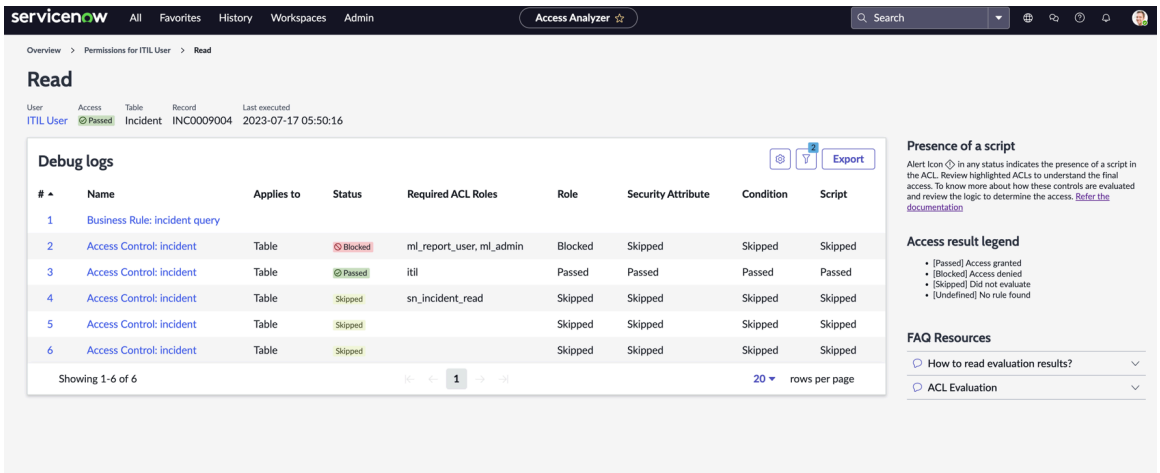
Perguntas	Explicação
Como posso ver os detalhes do grupo?	Você pode selecionar **Grupo (nó)** > **Mais ações** > **Exibir detalhes do grupo** para saber mais sobre o grupo.

Logs de depuração do Access Analyzer

Os logs de depuração exibem os detalhes da operação resultante do acesso de seleção.

Campos nos logs de depuração

Os logs de depuração no Access Analyzer exibem informações sobre a operação selecionada para entender as permissões, regras de negócios e ACLs associadas à operação.



A seguir estão os campos e suas descrições nos logs de depuração:

Logs de depuração

Campos	Descrição
Nome	Detalhes sobre a regra de negócios ou ACL. Selecione a regra de negócios da ACL para obter mais informações.
Aplica-se a	Detalhes sobre a aplicação da ACL em nível de campo, registro ou tabela.
Status	Status da ACL para a função e permissão associadas.
ACL obrigatório	A função necessária para acessar o campo, registro ou tabela.
Função	Detalhes sobre a função que está sendo bloqueada, aprovada ou ignorada para o Controle de acesso.
Atributo de segurança	Detalhes sobre o atributo de segurança que está sendo bloqueado, aprovado ou ignorado para o Controle de acesso.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Logs de depuração

Campos	Descrição
Condição	Detalhes sobre a condição que está sendo bloqueada, aprovada ou ignorada para o controle de acesso.
Script	Detalhes sobre o script que está sendo bloqueado, aprovado ou ignorado para o controle de acesso.
Personalizado	Detalhes sobre a ACL personalizada, se houver, para o Controle de acesso.
Aplicação	Status da aplicação Global ou Store.

Hierarquia de avaliação

A permissão do usuário, grupo ou função selecionada é avaliada com base na seguinte hierarquia:

- Regra de negócios: uma regra de negócios é um script relacionado ao servidor que é executado quando um registro é exibido, inserido, atualizado, excluído ou quando uma tabela é consultada.
- Manipulador de acesso: uma verificação interna do sistema que usa um código fonte oculto na plataforma.
- Filtragem de dados: a filtragem de dados é uma forma de controle de acesso projetada para funcionar com as ACLs (Access Control rules, Regras de controle de acesso) existentes na instância. Os filtros de dados só são compatíveis com operações de leitura.
- ACL (Lista de controle de acesso): Regras para ACLs restringem o acesso aos dados exigindo que os usuários cumpram com um conjunto de requisitos antes de poderem interagir. A seguinte hierarquia é considerada para as ACLs:
  - Função
  - Atributo de segurança
  - Condição
  - Script

Avaliação da lista de controle de acesso

As ACLs para operações são avaliadas da seguinte forma:

- Função
- Atributo de segurança
- Condição
- Script

Quando há um script disponível

O ícone de alerta em qualquer status indica a presença de um script na ACL. Revise as ACLs em destaque para entender o último acesso.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Durante uma consulta do analisador de acesso, as regras de negócios são executadas primeiro, seguidas da lista de controle de acesso.

Sequência de execução

A sequência de execução do resultado de acesso em diferentes cenários é a seguinte:

- **Quando há uma ACL herdada ou curinga**: durante a sequência de execução, as ACLs herdadas são avaliadas primeiro e, em seguida, as ACLs curingas.
- **Quando uma ACL é aprovada, as outras são ignoradas**: durante a execução e a avaliação da permissão, se uma ACL for aprovada, outras execuções e avaliações de ACL serão ignoradas. Isso acontece porque a permissão geral da operação selecionada requer uma ACL para acessar um campo, registro ou tabela de uma identidade.
- **Quando há a execução de ACLs de nível de campo e ACLs de nível de tabela**: durante a execução, as ACLs de nível de campo são executadas primeiro, seguidas pelas ACLs de nível de tabela para fornecer resultados mais granulares ao analisar o acesso de uma identidade.
- **Quando é feita avaliação na presença de ACLs com script**: na presença de um script, o acesso geral da operação é aprovado com um ícone de alerta para indicar que há um Script na ACL.

Simulador de acesso

O Simulador de acesso ajuda a simular as alterações do acesso à tabela quando uma função ou grupo fosse atribuído ou removido do usuário.

Explorar

Conheça os recursos e o valor comercial do Simulador de acesso.

Usar

Entenda como usar o Simulador de acesso.

Configurar

Perguntas frequentes

Veja os detalhes sobre as perguntas mais comuns sobre o Simulador de acesso.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Saiba como configurar o Simulador de acesso.

Exploração do Simulador de acesso

O Simulador de acesso simula como o acesso à tabela especificada mudaria quando uma função ou um grupo fosse atribuído ou removido do usuário.

Os administradores podem usar o Simulador de acesso para simular os requisitos de acesso de seus usuários em uma tabela especificada e entender como os controles de acesso mudam para um usuário. Isso ajuda a entender rapidamente o acesso atual dos usuários e os impactos de designar ou remover funções dos usuários.

https://player.vimeo.com/video/988627830?badge=0&autopause=0&player_id=0&app_id=58479

É possível usar o Simulador de acesso para simular o acesso de um usuário nos seguintes cenários:

- Como adicionar uma função ao usuário
- Como remover uma função do usuário
- Como adicionar o usuário a um grupo
- Como remover o usuário de um grupo

Para saber mais sobre as configurações do Simulador de acesso e ativar a execução de ações, consulte Configuração do Simulador de acesso (Executar ações).

Configuração do Simulador de acesso (Executar ações)

Configure as opções de execução de ações para concluir as atribuições de função e grupo que você deseja adicionar após a simulação.

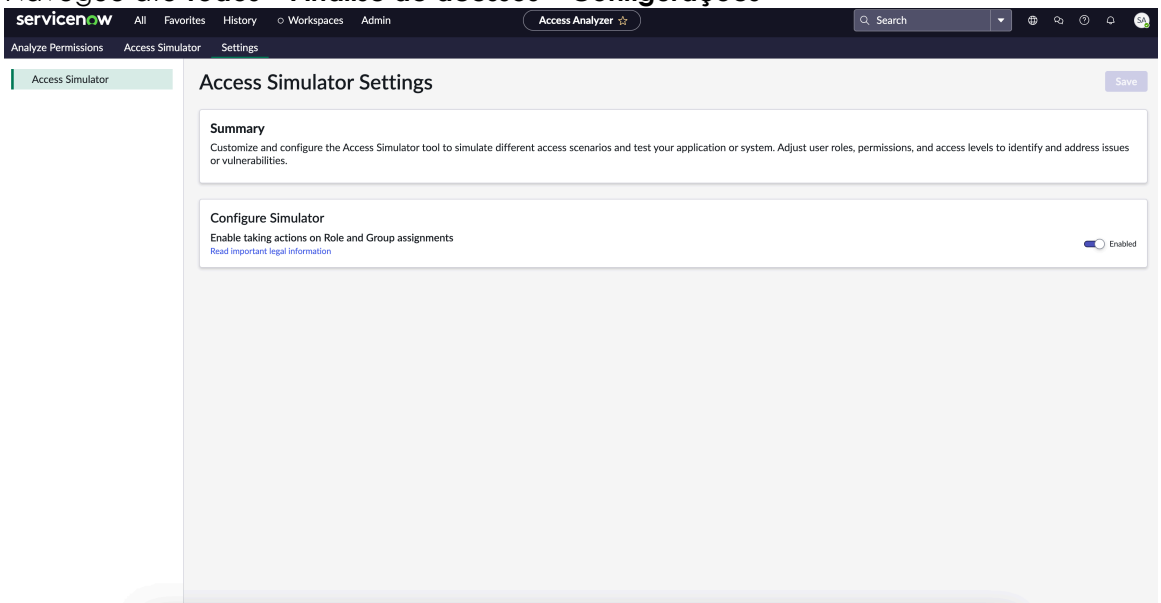
Antes de Iniciar

Função necessária: administrador

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegue até **Todos** > **Análise de acessos** > **Configurações**



2. Selecione o botão de alternância para ativar.
   Leia as informações jurídicas antes de ativar o Simulador de acesso (Executar ações).
3. Selecione **Aceitar**.
4. Selecione **Salvar** para salvar a configuração.

Como usar o Simulador de acesso

Use o Simulador de acesso para simular como o acesso do usuário à tabela especificada mudaria quando uma função ou um grupo fosse atribuído ou removido.

Antes de Iniciar

Função necessária: administrador

Ative a execução de ações. Para obter mais informações, consulte Configuração do Simulador de acesso (Executar ações).

Procedimento

1. Navegue até **Todos** > **Análise de acessos** > **Simulador de acesso**.
2. Selecione a opção **Simular** em cada seção com base nos seguintes cenários:
   - Como adicionar uma função ao usuário
   - Como remover uma função do usuário
   - Como adicionar o usuário a um grupo
   - Como remover o usuário de um grupo

Como adicionar uma função ao usuário

Use **Simular adição de função** para simular as mudanças de acesso do usuário a um recurso (tabelas).

Antes de Iniciar

Função necessária: administrador

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

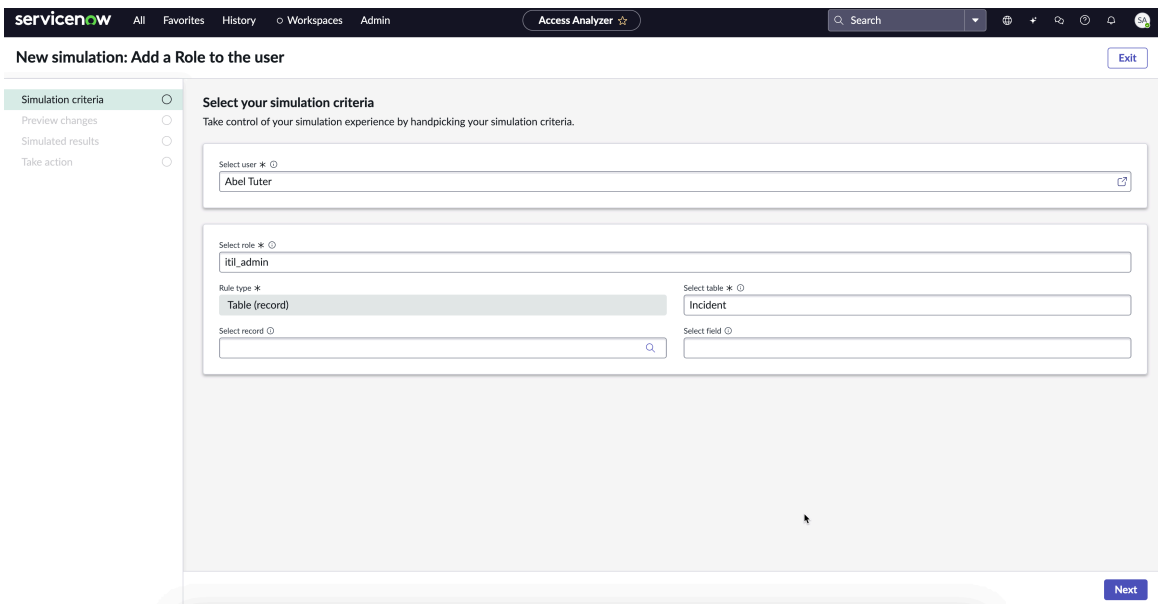
Ative a execução de ações. Para obter mais informações, consulte Configuração do Simulador de acesso (Executar ações).

Procedimento

1. Navegue até **Todos** > **Análise de acessos** > **Simulador de acesso**.
2. Selecione **Simular** na seção "Adicionar uma função ao usuário".
3. Especifique os seguintes campos para seus critérios de simulação:

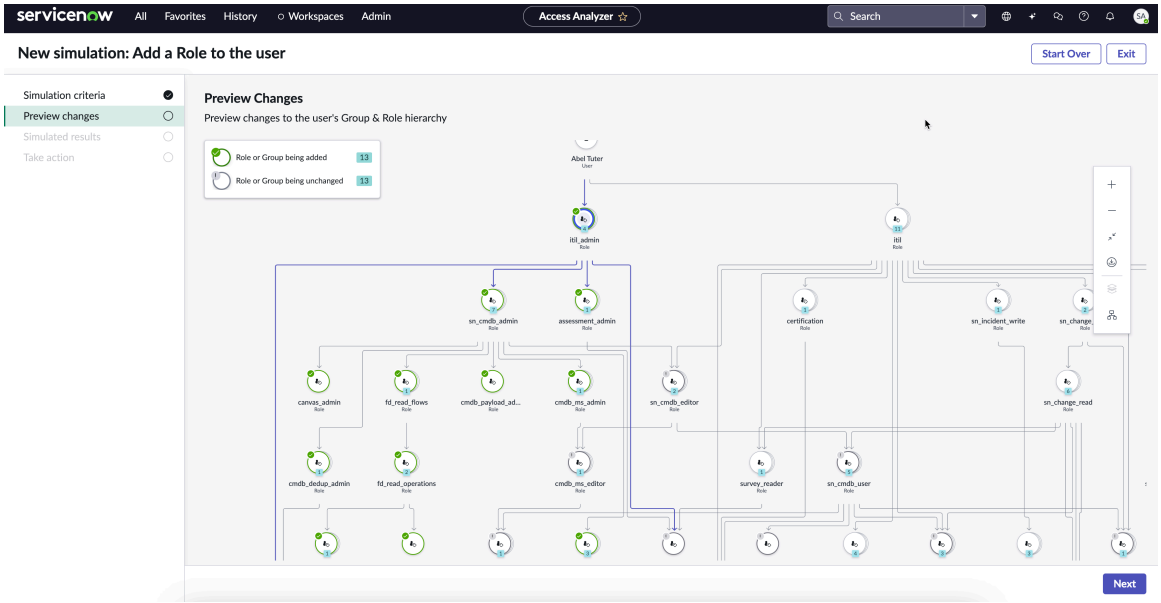
Adicionar uma função ao usuário

Campo	Descrição
Selecionar usuário *	Especifique um nome de usuário da lista. Neste exemplo, **Abel Tuter**.
Selecionar função *	Especifique uma função a ser selecionada da lista. Neste exemplo, **itil_admin**.
Tipo de regra *	Há o preenchimento automático do tipo de regra e não é possível mudá-lo.
Selecionar tabela *	Especifique um nome de tabela da lista para selecionar. Neste exemplo, **Incidente**.
Selecionar registro	Especifique um nome de registro para selecionar na lista (opcional).
Selecionar campo	Especifique um nome de campo da lista para selecionar. Este campo pode ser usado para analisar permissão mesmo no nível de campo. Por exemplo, "ativo", "criado por" e assim por diante.



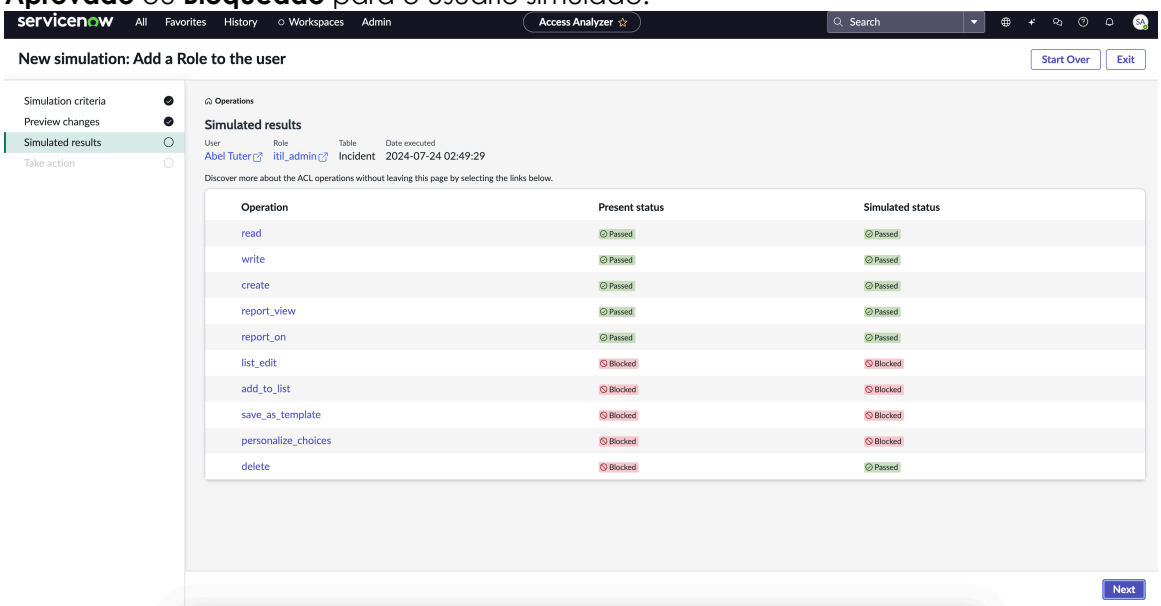
4. Selecione **Avançar**.
5. Visualize as mudanças.
   Em "Visualizar mudanças", há a simulação das funções recém-atribuídas. Antes de avançar para a próxima etapa, é possível validar as funções e as funções secundárias que estão sendo adicionadas ao usuário.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



É possível ver as novas funções que estão sendo adicionadas como parte da função **itil_admin** junto com as funções existentes do usuário.

6. Selecione **Avançar**.
7. Valide o **Status presente** e o **Status simulado** para verificar o acesso que está sendo **Aprovado** ou **Bloqueado** para o usuário simulado.



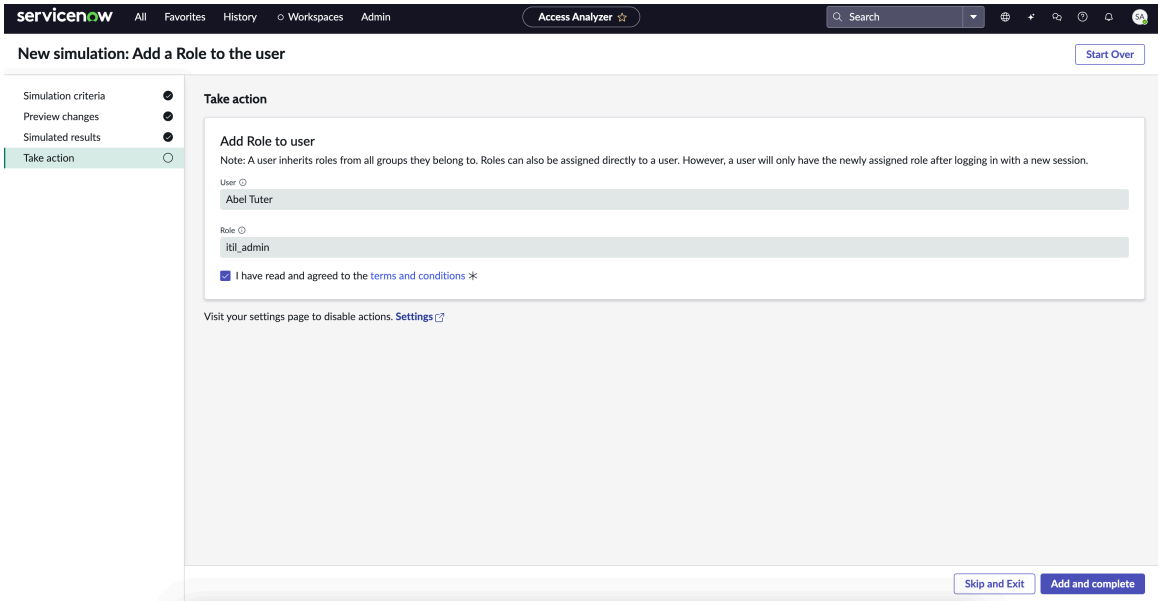
Adicionar **itil_admin** permite que o usuário realize a operação de exclusão na tabela ("Incidente").

Nota:

- Se você quiser saber mais sobre a ACL (operações), selecione os links de operação para cada registro.
- Se você quiser reiniciar a simulação para uma função diferente, selecione **Começar**.
- Se você quiser sair da simulação, selecione **Sair**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

8. Selecione **Avançar**.
9. Selecione **Adicionar e concluir**.



Nota:

- Se o Simulador de acesso não estiver ativado, não será possível concluir a simulação. Para ativá-lo, selecione **Ativar ações** e aceite as informações jurídicas.
- Se você quiser ocultar a simulação, selecione **Ocultar ações**. Para exibir e ativar ações, acesse as configurações. Para obter mais informações, consulte Configuração do Simulador de acesso (Executar ações).
- Se você quiser sair da simulação, selecione **Ignorar e sair**.

As funções são adicionadas ao usuário com sucesso. É possível verificar o acesso usando a Análise de acessos. Para obter mais informações sobre como verificar o acesso de um usuário, consulte Análise de acessos.

Como remover uma função do usuário

Use **Simular remoção de função** para simular as mudanças de acesso do usuário a um recurso (tabelas).

Antes de Iniciar

Função necessária: administrador

Ative a execução de ações. Para obter mais informações, consulte Configuração do Simulador de acesso (Executar ações).

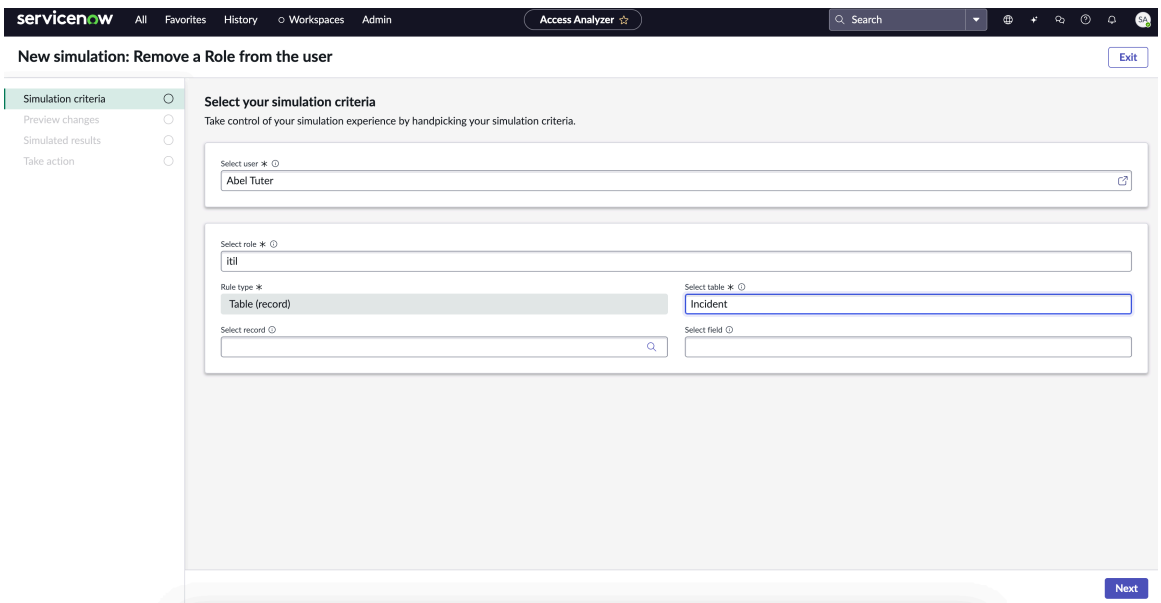
Procedimento

1. Navegue até **Todos** > **Análise de acessos** > **Simulador de acesso**.
2. Selecione **Simular** na seção "Remover uma função do usuário".
3. Especifique os seguintes campos para seus critérios de simulação:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

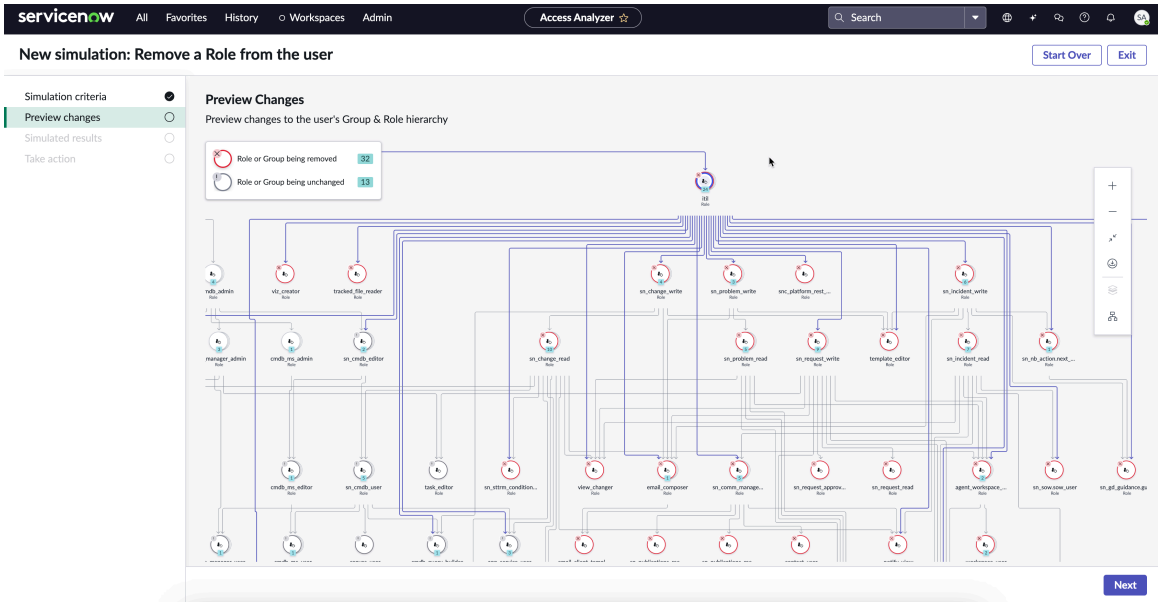
Remover uma função do usuário

Campo	Descrição
Selecionar usuário *	Especifique um nome de usuário da lista. Neste exemplo, **Abel Tuter**.
Selecionar função *	Especifique uma função a ser selecionada da lista. Neste exemplo, **itil**.
Tipo de regra *	Há o preenchimento automático do tipo de regra e não é possível mudá-lo.
Selecionar tabela *	Especifique um nome de tabela da lista para selecionar. Neste exemplo, **Incidente**.
Selecione o registro	Especifique um nome de registro da lista para selecionar.
Selecionar campo	Especifique um nome de campo da lista para selecionar. Este campo pode ser usado para analisar permissão mesmo no nível de campo. Por exemplo, "ativo", "criado por" e assim por diante.

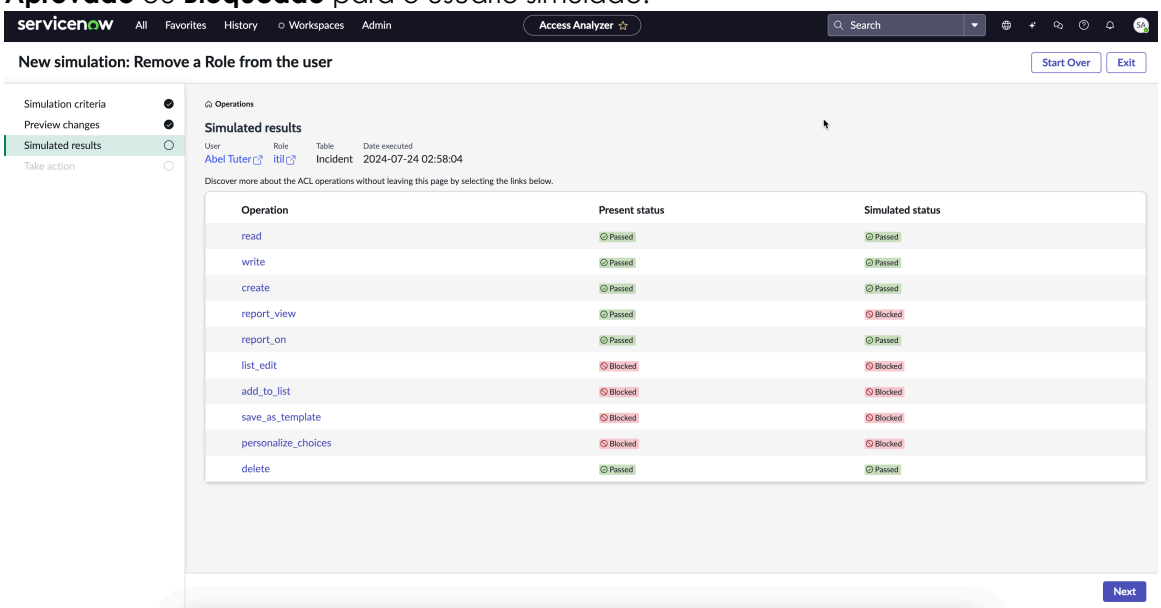


4. Selecione **Avançar**.
5. Visualize as mudanças.
   Em "Visualizar mudanças", há a simulação das funções removidas. Antes de avançar para a próxima etapa, é possível validar as funções e as funções secundárias que estão sendo removidas do usuário.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



6. Selecione **Avançar**.
7. Valide o **Status presente** e o **Status simulado** para verificar o acesso que está sendo **Aprovado** ou **Bloqueado** para o usuário simulado.



Nota:

- Se você quiser saber mais sobre a ACL (operações), selecione os links de operação para cada registro.
- Se você quiser reiniciar a simulação para uma função diferente, selecione **Começar**.
- Se você quiser sair da simulação, selecione **Sair**.

8. Selecione **Avançar**
9. Selecione **Remover e concluir**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

- Se o Simulador de acesso não estiver ativado, não será possível concluir a simulação. Para ativá-lo, selecione **Ativar ações** e aceite as informações jurídicas.
- Se você quiser ocultar a simulação, selecione **Ocultar ações**. Para exibir e ativar ações, acesse as configurações. Para obter mais informações, consulte Configuração do Simulador de acesso (Executar ações).
- Se você quiser sair da simulação, selecione **Ignorar e sair**.

As funções são removidas do usuário com sucesso. É possível verificar o acesso usando a Análise de acessos. Para obter mais informações sobre como verificar o acesso de um usuário, consulte Análise de acessos.

Como adicionar o usuário a um grupo

Use **Simular adição ao grupo** para simular as mudanças de acesso do usuário a um recurso (tabelas) após a adição de um usuário a um grupo.

Antes de Iniciar

Função necessária: administrador

Ative a execução de ações. Para obter mais informações, consulte Configuração do Simulador de acesso (Executar ações).

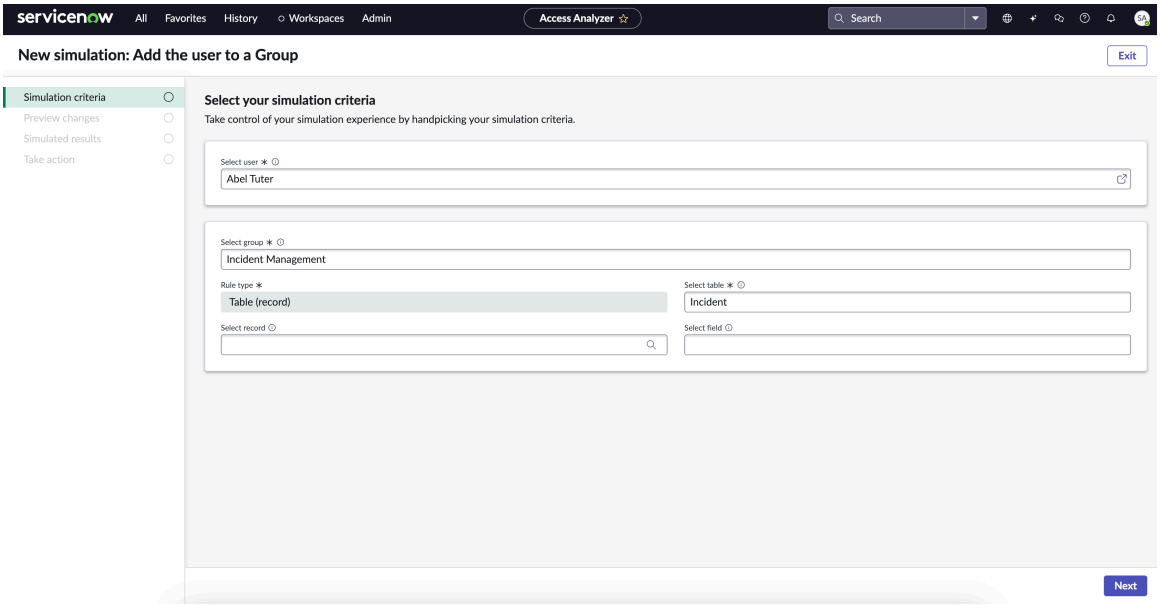
Procedimento

1. Navegue até **Todos** > **Análise de acessos** > **Simulador de acesso**.
2. Selecione **Simular** na seção "Adicionar o usuário a um grupo".
3. Especifique os seguintes campos para seus critérios de simulação:

Adicionar o usuário a um grupo

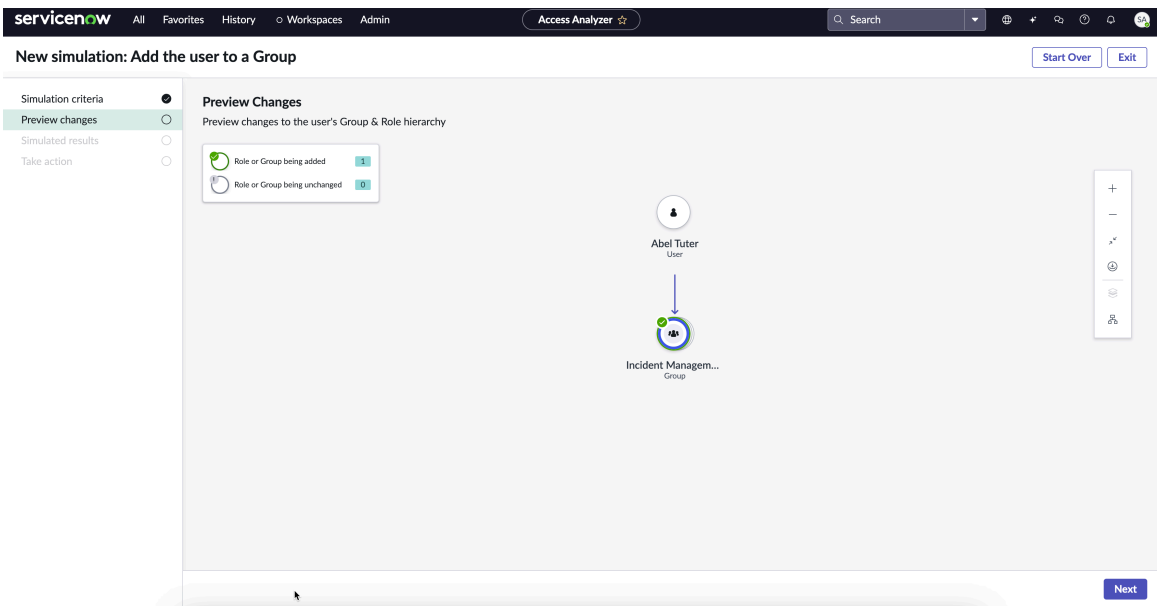
Campo	Descrição
Selecionar usuário *	Especifique um nome de usuário da lista. Neste exemplo, **Abel Tuter**.
Selecionar grupo *	Especifique um grupo para seleção na lista. Neste exemplo, **Gestão de incidentes**.
Tipo de regra *	Há o preenchimento automático do tipo de regra e não é possível mudá-lo.
Selecionar tabela *	Especifique um nome de tabela da lista para selecionar. Neste exemplo, **Incidente**.
Selecione o registro	Especifique um nome de registro da lista para selecionar.
Selecionar campo	Especifique um nome de campo da lista para selecionar. Este campo pode ser usado para analisar permissão mesmo no nível de campo. Por exemplo, "ativo", "criado por" e assim por diante.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



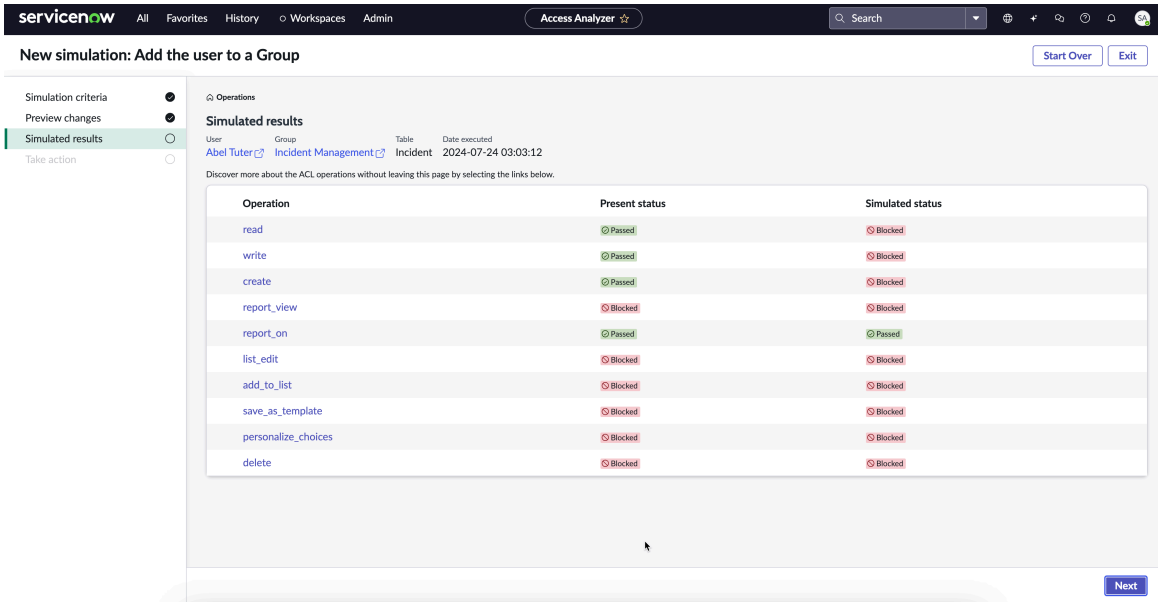
4. Selecione **Avançar**.
5. Visualize as mudanças.

   O grupo ao qual o usuário está atribuído é simulado em "Visualizar mudanças". É possível validar as mudanças antes de avançar para a próxima etapa.



6. Selecione **Avançar**.
7. Valide o **Status presente** e o **Status simulado** para verificar o acesso que está sendo **Aprovado** ou **Bloqueado** para o usuário simulado.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Nota:

- Se você quiser saber mais sobre a ACL (operações), selecione os links de operação para cada registro.
- Se você quiser reiniciar a simulação para uma função diferente, selecione **Começar**.
- Se você quiser sair da simulação, selecione **Sair**.

8. Selecione **Avançar**.
9. Selecione **Adicionar e concluir**.

Nota:

- Se o Simulador de acesso não estiver ativado, não será possível concluir a simulação. Para ativá-lo, selecione **Ativar ações** e aceite as informações jurídicas.
- Se você quiser ocultar a simulação, selecione **Ocultar ações**. Para exibir e ativar ações, acesse as configurações. Para obter mais informações, consulte Configuração do Simulador de acesso (Executar ações).
- Se você quiser sair da simulação, selecione **Ignorar e sair**.

O usuário é adicionado ao grupo com sucesso.

Como remover o usuário de um grupo

Use **Simular remoção do grupo** para simular as mudanças de acesso do usuário a um recurso (tabelas) quando ele é removido de um grupo.

Antes de Iniciar

Função necessária: administrador

Ative a execução de ações. Para obter mais informações, consulte Configuração do Simulador de acesso (Executar ações).

Procedimento

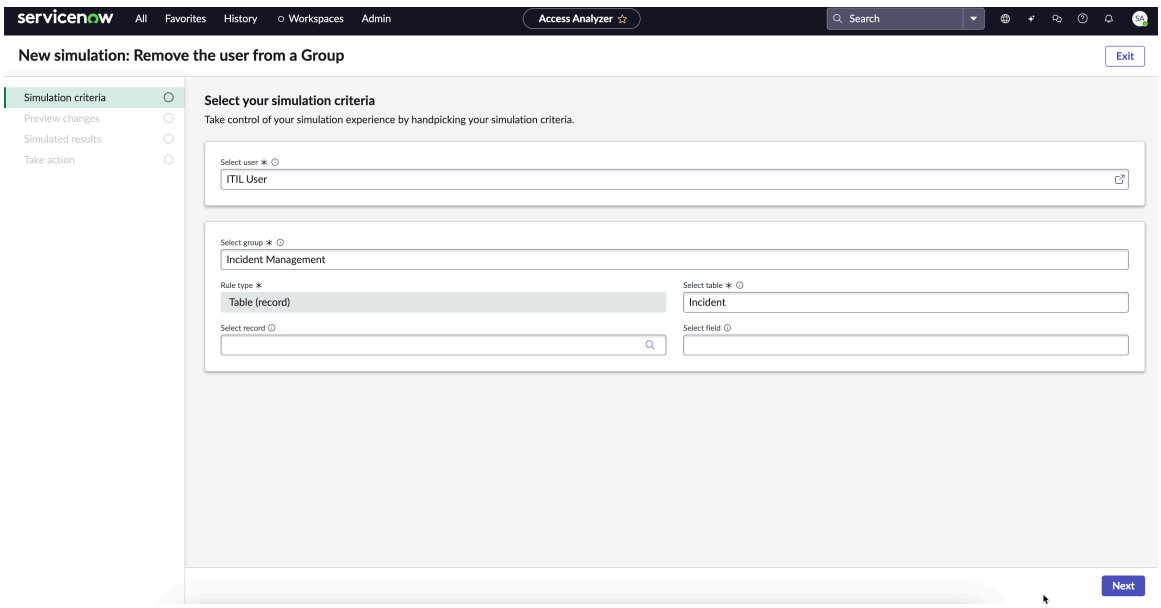
1. Navegue até **Todos** > **Análise de acessos** > **Simulador de acesso**.
2. Selecione **Simular** na seção "Remover o usuário de um grupo".

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Especifique os seguintes campos para seus critérios de simulação:

Remover o usuário de um grupo

Campo	Descrição
Selecionar usuário *	Especifique um nome de usuário da lista. Neste exemplo, **Usuário ITIL**.
Selecionar grupo *	Especifique um grupo para seleção na lista. Neste exemplo, **Gestão de incidentes**.
Tipo de regra *	Há o preenchimento automático do tipo de regra e não é possível mudá-lo.
Selecionar tabela *	Especifique um nome de tabela da lista para selecionar. Neste exemplo, **Incidente**.
Selecione o registro	Especifique um nome de registro da lista para selecionar.
Selecionar campo	Especifique um nome de campo da lista para selecionar. Este campo pode ser usado para analisar permissão mesmo no nível de campo. Por exemplo, "ativo", "criado por" e assim por diante.

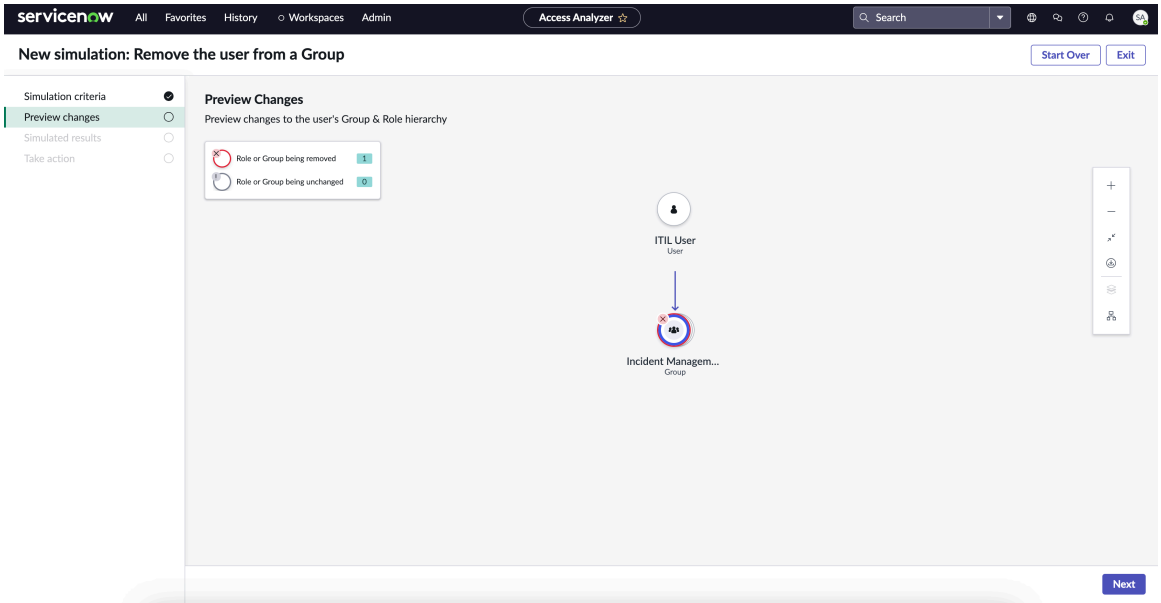


4. Selecione **Avançar**

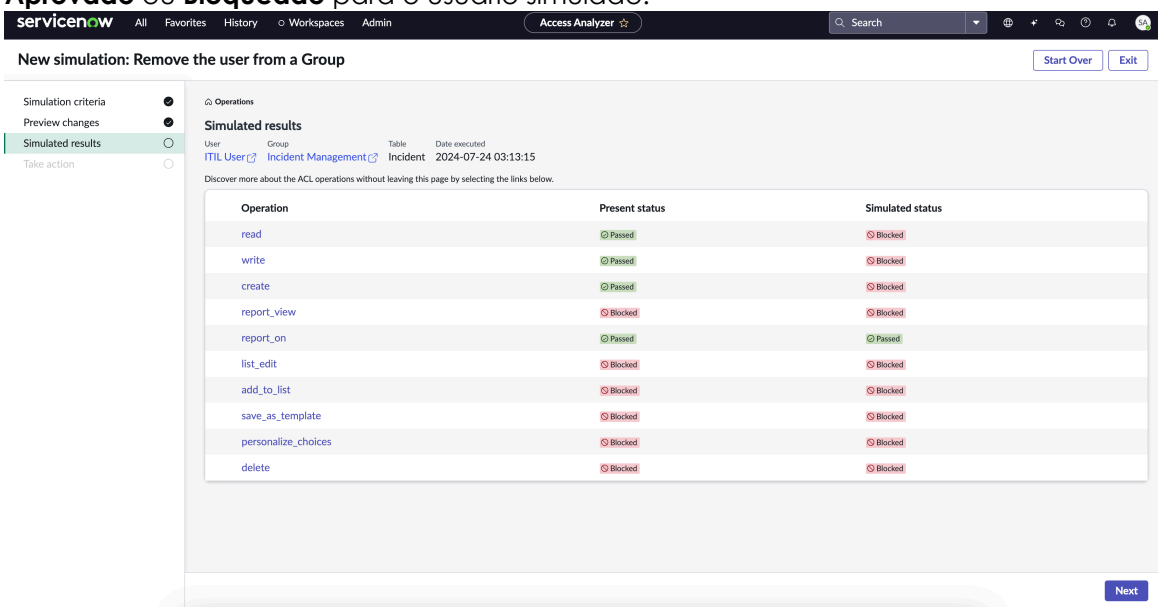
5. Visualize as mudanças.

Em "Visualizar mudanças", há a simulação do grupo do qual o usuário é removido. É possível validar as mudanças antes de avançar para a próxima etapa.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



6. Selecione **Avançar**
7. Valide o **Status presente** e o **Status simulado** para verificar o acesso que está sendo **Aprovado** ou **Bloqueado** para o usuário simulado.



Nota:

- Se você quiser saber mais sobre a ACL (operações), selecione os links de operação para cada registro.
- Se você quiser reiniciar a simulação para uma função diferente, selecione **Começar**.
- Se você quiser sair da simulação, selecione **Sair**.

8. Selecione **Avançar**
9. Selecione **Remover e concluir**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

- Se o Simulador de acesso não estiver ativado, não será possível concluir a simulação. Para ativá-lo, selecione **Ativar ações** e aceite as informações jurídicas.
- Se você quiser ocultar a simulação, selecione **Ocultar ações**. Para exibir e ativar ações, acesse as configurações. Para obter mais informações, consulte Configuração do Simulador de acesso (Executar ações).
- Se você quiser sair da simulação, selecione **Ignorar e sair**.

O usuário é removido do grupo com sucesso.

Perguntas frequentes

Perguntas frequentes sobre como usar o Simulador de acesso.

Perguntas frequentes

Perguntas	Explicação
Como posso começar a usar o simulador?	Você pode selecionar a opção Simular para o cenário diferente que deseja simular para os usuários e seguir as etapas.
Como o Simulador funciona?	O Simulador de acesso simula o acesso do usuário selecionado à tabela especificada e permite visualizar as mudanças de acesso para você tomar decisões sobre o provisionamento de acesso.
Como ativar ou desativar ações no Simulador?	Para ativar ou desativar ações no Simulador de acesso, acesse as Configurações ou durante as etapas de "Executar ações" no processo de simulação.

Identidade global

A Identidade global é um produto da ServiceNow® que permite identificar usuários exclusivos em várias instâncias.

A Identidade Global ajuda com várias instâncias da ServiceNow® para gerenciar usuários, os atributos deles e outros dados básicos em várias instâncias da ServiceNow®.

Explorar ID federado

Conheça os principais recursos e o valor comercial do ID federado.

Acessando o ID federado

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

	Acesse o ID federado.
Atualizando campos de ID Atualize e configure o ID federado.	

Explorando ID federado

Determine os usuários em várias instâncias com base no nome de usuário e e-mail e forneça um ID exclusivo (ID federado) ao usuário em todas as instâncias.

O ID federado é usado para identificar usuários nas diferentes instâncias da ServiceNow®. Com base no ID federado, o usuário pode ser identificado e o número preciso de usuários em várias instâncias pode ser determinado. Para mais informações, consulte ID federado.

Nota: O nome de usuário é necessário para gerar IDs federados

O ID federado é um identificador exclusivo para uma identidade que usa uma função de hash nas instâncias da ServiceNow®.

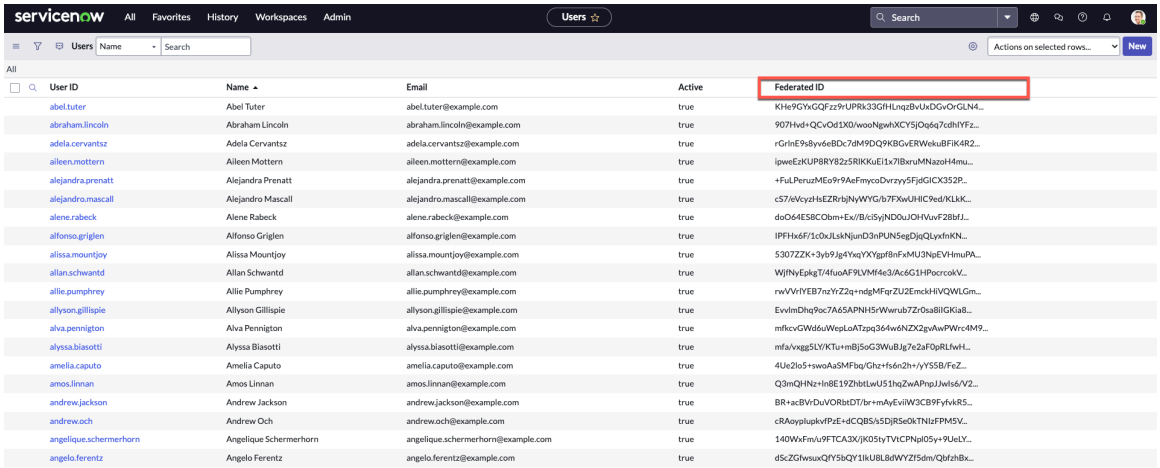
Ao usar o **ID do usuário** e o **E-mail** do usuário nas instâncias, o ID federado é criado e exibido na tabela sys_user.

Após a atualização para a versão Xanadu, o plug-in de Geração do ID federado (`com.glide.identity.globalid`) é instalado automaticamente em todas as instâncias.

Nota:

- O nome de usuário é necessário para gerar IDs federados
- O nome de usuário e o e-mail são usados para gerar IDs federados por padrão. Para atualizar os campos a fim de gerar IDs federados com base em seu requisito, consulte Atualização de campos de ID.
- A função **Iamsync_admin** é necessária para atualizar a configuração.
- Se houver usuários com e-mail e nomes de usuários duplicados, o ID federado será gerado apenas para um usuário. Se o nome de usuário for nulo ou estiver vazio, o ID federado será nulo.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



As mudanças de esquema após a instalação do plug-in são as seguintes:

- Uma nova coluna federated_id é criada na tabela `sys_user`.
- Nova tabela: `iamsync_type` é preenchido automaticamente com a configuração padrão da tabela `sys_user`.

O ID federado só é compatível com a tabela `sys_user` e todas as tabelas que estendem a tabela sys_user.

Após a atualização para a versão Xanadu, o plug-in de Geração do ID federado (`com.glide.identity.globalid`) é instalado automaticamente em todas as instâncias.

Acessando critérios de ID federado

Acesse os critérios de ID federado para saber mais sobre os campos de ID usados para o ID federado gerado.

Antes de Iniciar

Função necessária: iamsync_admin

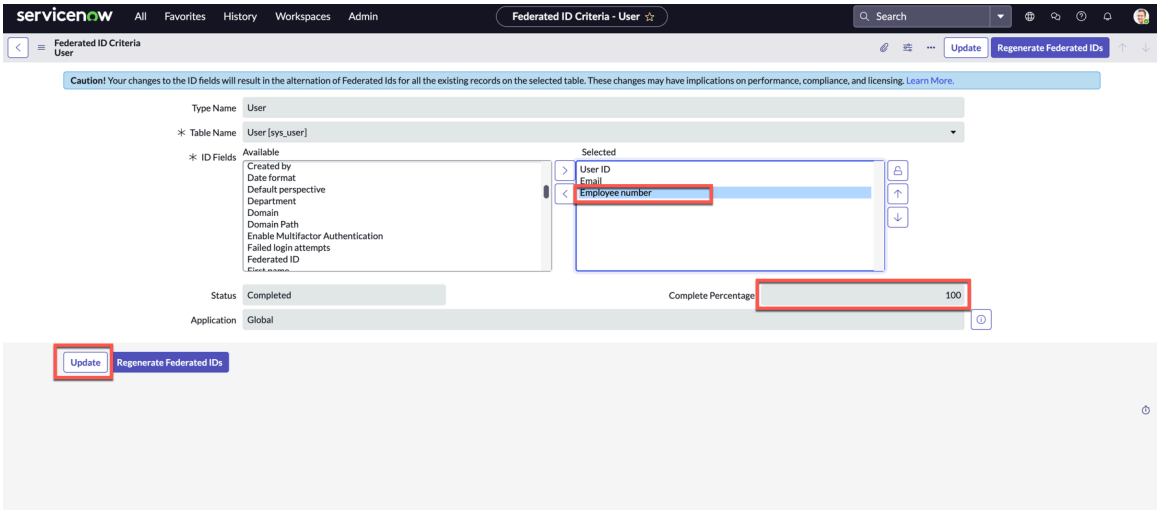
Procedimento

1. Navegue até **Tudo** > **Gerenciar ID federado** > **Critérios de IDs federados**.
2. A página Critérios de ID federado exibe o registro com os seguintes detalhes:
   - Nome do tipo: **usuário**
   - Nome da tabela: **Usuário [sys_user]**
   - Campos de ID: **user_name (ID do usuário), e-mail** (campos padrão que são usados para geração de ID federado).
   - Status: **concluído** (status de geração de ID federado). Status disponível: **Pronto**, **Em execução**, **Concluído**, **Erro**.

Nota:

- O nome de usuário é necessário para gerar IDs federados
- O nome de usuário e o e-mail são usados para gerar IDs federados por padrão.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Nota: Somente os campos de ID podem ser atualizados para gerar um novo ID federado para os registros existentes. Para saber mais, consulte Atualização de campos de ID.

Atualização de campos de ID

Atualize os campos de ID para gerar novamente os IDs federados com base nos campos atualizados.

Antes de Iniciar

Função necessária: iamsync_admin

Nota: Quaisquer mudanças nos campos de ID resultam na alteração dos IDs federados para todos os registros existentes na tabela selecionada. Essas mudanças podem afetar o desempenho, a conformidade e o licenciamento.

Procedimento

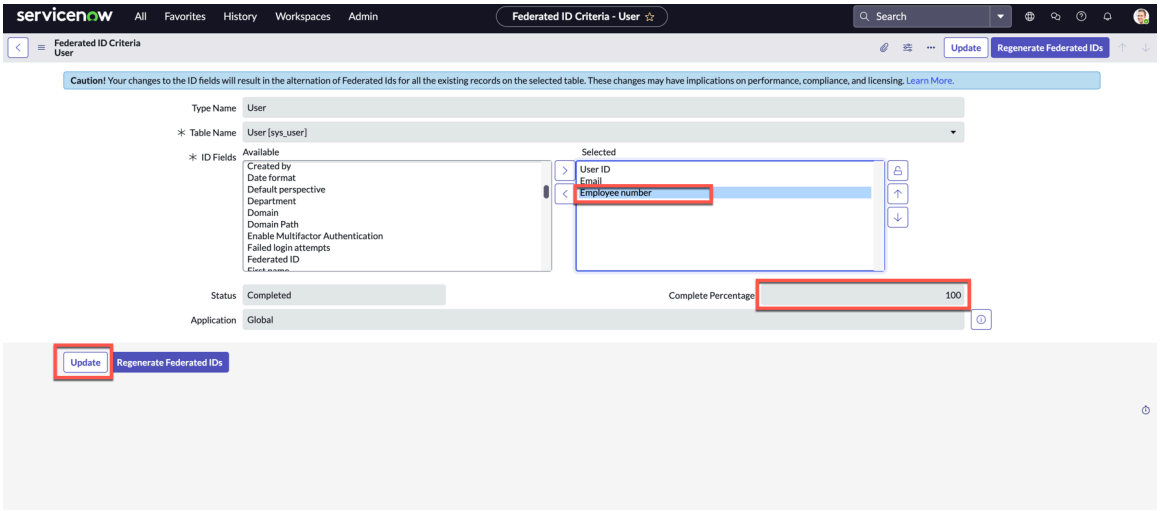
1. Navegue até **Tudo** > **Gerenciar ID federado** > **Critérios de IDs federados**.
2. Selecione o Nome do tipo (**Usuário**).
3. Selecione os novos campos de ID na página Usuário de critérios de ID federado que você deseja adicionar de Disponível a Selecionado usando as setas.

   Por exemplo, **Número do funcionário**.

   Nota:

   - O nome de usuário é necessário para gerar IDs federados
   - O nome de usuário e o e-mail são usados para gerar IDs federados por padrão.
   - Se houver usuários com e-mail e nomes de usuários duplicados, o ID federado será gerado apenas para um usuário. Se o nome de usuário for nulo ou estiver vazio, o ID federado será nulo.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Agora, o **Número do funcionário** selecionado se torna outro atributo para gerar o ID federado.

4. Selecione **"Atualizar"** para gerar IDs federados.

   Nota: Selecione **"Atualizar"** primeiro e verifique a porcentagem de conclusão (100) antes de iniciar outra atualização

   A porcentagem do status indica a geração do ID federado para todas as identidades nas instâncias.

   Nota:

   - Até que o trabalho de atualização anterior seja concluído, não faça alterações no campo.
   - Os campos atualizados devem ser do tipo cadeia de caracteres.
   - Os campos que não podem ser selecionados como campos de ID são os seguintes:
     - Campos de nível do sistema
     - Campos de Edge Encryption
     - Campos de senhas.

5. Navegue até a tabela sys_user para exibir os novos IDs federados que são gerados com a atualização dos campos de ID.

   Nota: Selecione **Gerar IDs federados novamente** se um usuário for criado ou atualizado por meio de importações de XML, atualizações de banco de dados de baixo nível ou a instância não estiver funcionando corretamente. Selecionar **Gerar IDs federados novamente**, os IDs de todos os usuários serão gerados novamente usando o critério de campo de ID atual.

Central de identidade

Permite monitorar, gerenciar e minimizar o risco com base na identidade e lacunas de segurança.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Explorar

Conheça os recursos e o valor comercial da Central de identidade.

Ativar

Entenda como ativar a Central de identidade.

Métricas de identidade para administradores

Saiba como as permissões são avaliadas.

Central de identidade para usuários

Veja os detalhes sobre as perguntas mais comuns sobre o Analisador de Acesso.

Explorando o Identity Center

O Identity Center é uma coleção de atributos do usuário, acessos, dispositivos, histórico de login, atividade de segurança e muito mais.

O Identity Center oferece recursos para monitorar, gerenciar e minimizar riscos baseados na identidade e lacunas de segurança.

A Central de identidade é uma etapa para monitorar, gerenciar e minimizar riscos com base na identidade e lacunas na segurança em ServiceNow.

Para ativar a Central de identidade, instale o plug-in Identity Center (`com.snc.identity_center`). O Identity Center está disponível para o usuário final, exibindo os detalhes sobre as sessões ativas, o histórico de login e os dispositivos confiáveis com o Identity Center. Para obter mais informações, consulte Central de identidade para usuários.

Ativando a Central de identidade

Para usar a Central de identidade, instale o plug-in Identity Center (`com.snc.identity_center`).

Antes de Iniciar
Função necessária: administrador

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegue até **Todos** > **Aplicações do sistema** > **Todas as aplicações disponíveis** > **Todas**.
2. Encontre o plug-in Identity Center (`com.snc.identity_center`) usando os critérios de filtro e a barra de pesquisa.

   Pesquise o plug-in pelo nome ou ID. Se não conseguir encontrar um plug-in, talvez seja necessário solicitá-lo ao pessoal ServiceNow.

3. Selecione **Instalar** para iniciar o processo de instalação.

   Nota: Quando a separação de domínio e o administrador delegado estão habilitados em uma instância, o usuário administrativo deve estar no domínio **global.** Caso contrário, será exibido o seguinte erro: `A instalação da aplicação não está disponível porque há outra operação em execução: ativação de plug-in para <plugin name>.`

   Você verá uma mensagem após a conclusão da instalação.

Central de identidade para usuários

Exiba os detalhes sobre as sessões ativas, o histórico de login e os dispositivos confiáveis com a Central de identidade.

A central de identidade é uma coleção de atributos do usuário, dispositivos, histórico de login, atividade de segurança e muito mais. Ela fornece uma exibição em painel único de todos os dados com controles de segurança adicionais e recursos de notificação.

Com a Central de identidade, é possível visualizar os detalhes sobre suas sessões ativas, histórico de login e dispositivos confiáveis.

Para acessar a Central de identidade dos usuários, navegue até um dos seguintes:

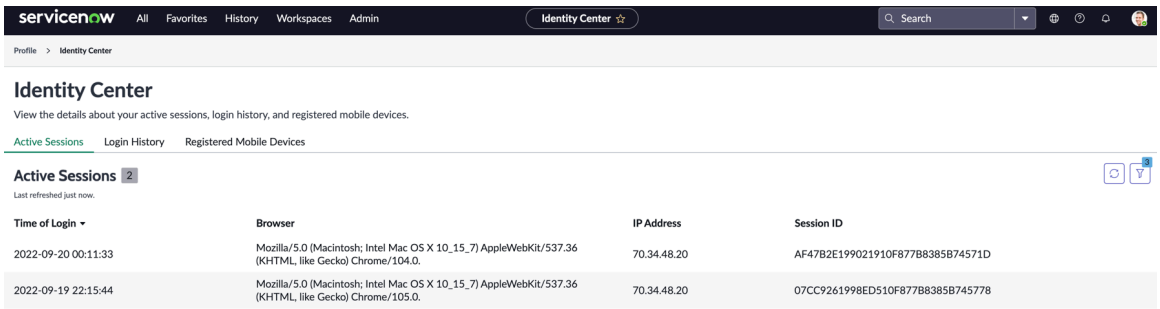
- Em Now Platform, navegue até **Todos** > **Autoatendimento** > **Meu perfil** e selecione **Exibir Central de identidade** na seção Links relacionados.

  Nota: Você também pode acessar seu perfil selecionando o nome de usuário no cabeçalho da instância.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Em Now Support, selecione o perfil, escolha **Exibir Central de identidade** na parte inferior da página.

A página Central de identidade é exibida da seguinte forma:



A Central de identidade tem as seguintes guias:

- Sessões ativas
- Histórico de login
- Dispositivos móveis registrados

Você pode selecionar essas guias para exibir detalhes, como navegador, endereços de IP, informações de relação de sessão, informações de login e seus dispositivos móveis registrados.

Exibir sessões ativas

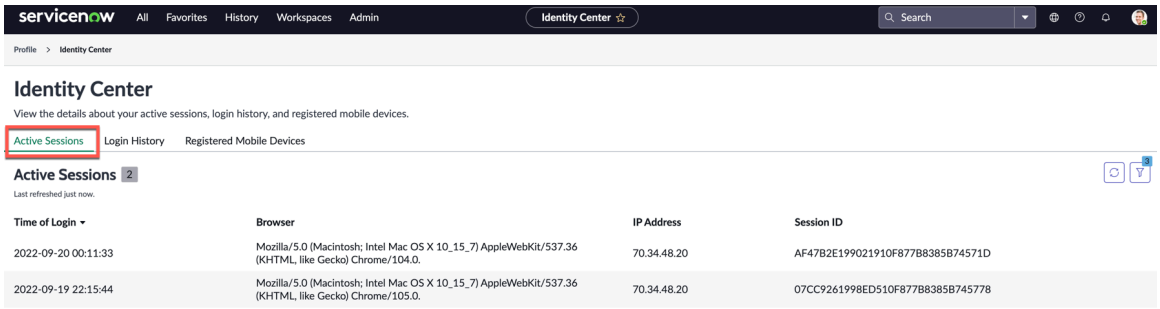
Exibe as informações sobre as sessões do usuário.

Sessões ativas são as sessões abertas na instância ServiceNow® atual com diferentes navegadores ou dispositivos.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A guia Sessões ativas na Central de identidade ajuda a identificar suas sessões com base no Navegador, Endereço IP e ID de sessões. Usando essas informações, é possível executar as ações necessárias, como estender ou encerrar a sessão.

O uso dessas informações pode ajudar a determinar se as sessões são legítimas e não representam uma preocupação de segurança.



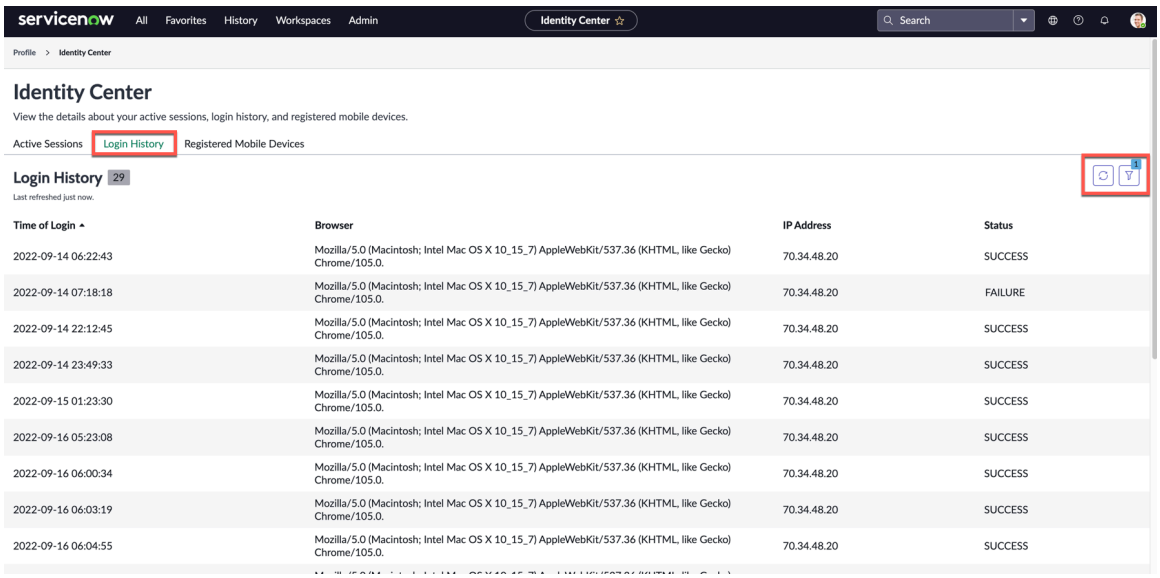
Exibir histórico de login

Fornece detalhes sobre seu histórico de login.

A guia Histórico de login na Central de identidade ajuda você com suas informações e o status do seu login.

É possível usar os filtros para especificar ações de login a fim de ajudar nas investigações de segurança. O filtro pode ajudar a determinar se a atividade foi real ou suspeita e relatar as informações ao seu administrador.

A paginação no histórico de login é 20 por padrão e pode ser definida como até 100, no máximo.



A seguir estão alguns dos outros detalhes do histórico de login:

- A Hora de login é a hora atualizada em que os dispositivos móveis são usados para acessar a instância.
- Os registros ficam armazenados na Central de identidade por 30 dias.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exibir dispositivos móveis registrados

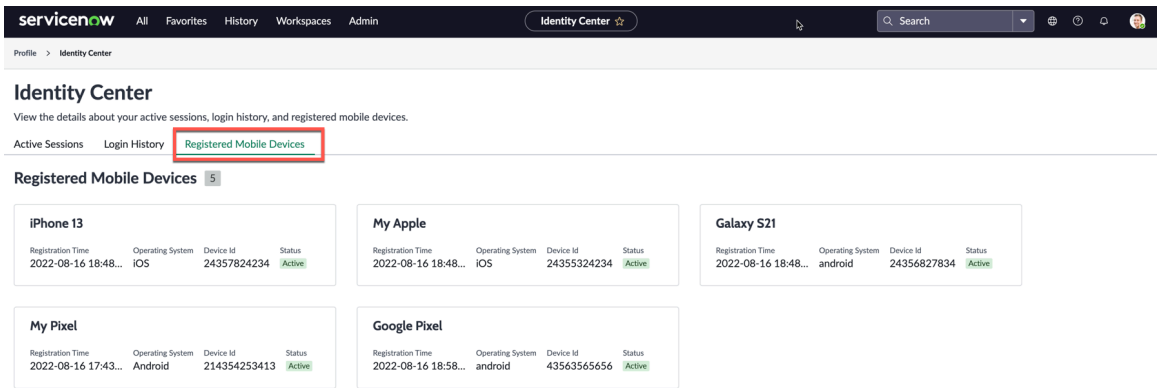
Forneça detalhes sobre seu dispositivo móvel registrado na instância ServiceNow.

A guia Dispositivos móveis registrados na Central de identidade exibe os detalhes sobre os dispositivos registrados que foram usados para acessar a instância ServiceNow.

Se o módulo de Autenticação adaptável estiver ativado e um dispositivo móvel registrado estiver inscrito, a Central de identidade exibirá os detalhes sobre seus dispositivos registrados.

Além disso, ele também exibe detalhes dos dispositivos, como sistema operacional, ID do dispositivo e status do dispositivo com a hora de registro do dispositivo.

Para registrar seu dispositivo móvel, você deve verificar se o plug-in de Autenticação adaptável (*com.snc.adaptive_authentication*) está instalado e se você ativou o recurso Aplicativo para celular confiável. Para obter mais informações, consulte Como ativar o aplicativo Trusted Mobile.



Métricas de identidade para administradores

Exiba as tendências dos usuários, usuários privilegiados, sessões ativas e conta integrada na sua instância da ServiceNow.

As métricas de identidade para administradores têm as tendências para o seguinte:

- Usuários
- Usuários privilegiados
- Integração ou contas não humanas
- Sessões ativas
- Sessões inativas

Para saber mais, consulte as Métricas da Central de Segurança.

Sistema de gerenciamento de usuários entre domínios (SCIM)

A API do Sistema de gerenciamento de usuários entre domínios (SCIM) fornece endpoints para criar, ler, atualizar e excluir operações em usuários e grupos usando o protocolo SCIM.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Provedor de SCIM

O provedor de SCIM sincroniza as mudanças feitas nas identidades no IdP, incluindo a criação, atualização ou exclusão de registros.

Cliente de SCIM

O Cliente do SCIM é usado para criar, atualizar e excluir recursos de identidade em um sistema que é compatível com solicitações REST em conformidade com SCIM.

O protocolo do SCIM é um protocolo baseado em HTTP de nível de aplicação baseada no padrão HTTP (RFC7230). Use esta API para provisionar e gerenciar dados de identidade, como usuários e grupos. Use a API na Web e em ambientes de domínio cruzado, como provedores de serviços de empresa para nuvem ou cenários entre nuvens.

Para acessar esta API, você deve ativar o plug-in SCIM v2 - ServiceNow®Cross-domain Identity Management (com.snc.integration.scim2).

Para saber mais sobre a API SCIM, consulte Sistema para API de gestão de identidade entre domínios (SCIM) .

Provedor de SCIM

O Provedor de serviço provisiona usuários e grupos usando a API do SCIM

Explorar

Saiba mais sobre o provedor de SCIM.

Ativar

Ativar SCIM.

Personalização do SCIM

Definição da origem

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Veja os detalhes sobre como personalizar o SCIM.

Saiba mais sobre a definição de origem para SCIM.

Explorando o Provedor de SCIM

O Provedor de serviço provisiona usuários e grupos usando a API do SCIM

Como um provedor de SCIM, os esquemas da ServiceNow oferecem suporte a APIs SCIM para provisionar usuários e grupos.

O provedor de SCIM sincroniza as mudanças feitas nas identidades no IdP, incluindo a criação, atualização ou exclusão de registros. Essas mudanças são sincronizadas automaticamente com o provedor de acordo com o protocolo do SCIM. Além disso, o IdP pode ler identidades do provedor para adicionar ao diretório IdP. O IdP pode então detectar valores incorretos no provedor que podem criar vulnerabilidades de segurança. A sincronização permite que os usuários finais tenham acesso contínuo às aplicações para as quais foram atribuídos, com perfis e permissões atualizados.

Configurações para o Provedor de SCIM

Para configurar o Provedor de SCIM, execute as seguintes tarefas:

- Ative o plug-in **SCIM v2 - ServiceNow Cross-domain Identity Management**. Para saber mais, consulte Ativando o plug-in do SCIM.
- Ative os outros plug-ins necessários para o SCIM:
  - OAuth 2.0
  - REST API Provider
  - Políticas de acesso de API REST
- Adicione a função scim_admin como parte do serviço de SCIM.

⚠ **Aviso:** Conceda esta função com cuidado. A função scim_admin é equivalente a conceder ao usuário a função de administrador, porque a função scmin_admin pode adicionar ou atualizar Informações de identificação pessoal (PII).

Tabelas

Duas tabelas, sys_user e sys_group, contêm os atributos de SCIM que não são mapeados para as tabelas da ServiceNow existentes. Para saber mais sobre as tabelas, consulte as Tabelas específicas do SCIM.

Ativando o plug-in do SCIM

Para ativação do SCIM, instale o plug-in SCIM v2 - ServiceNow Cross-domain Identity Management (com.snc.integration.scim2).

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Navegue até **Todos** > **Aplicações do sistema** > **Todas as aplicações disponíveis** > **Todas**.
2. Encontre o plug-in SCIM v2 - ServiceNow Cross-domain Identity Management (com.snc.integration.scim2) usando os critérios de filtro e a barra de pesquisa.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Pesquise o plug-in pelo nome ou ID. Se não conseguir encontrar um plug-in, talvez seja necessário solicitá-lo ao pessoal ServiceNow.

3. Selecione **Instalar** para iniciar o processo de instalação.

> **Nota:** Quando a separação de domínio e o administrador delegado estão habilitados em uma instância, o usuário administrativo deve estar no domínio **global.** Caso contrário, será exibido o seguinte erro: `A instalação da aplicação não está disponível porque há outra operação em execução: ativação de plug-in para <plugin name>.`

Você verá uma mensagem após a conclusão da instalação.

Tutorial: como configurar o SCIM para provisionamento de usuários com um provedor

A configuração do SCIM provisiona e desprovisiona usuários e grupos automaticamente na ServiceNow usando o serviço de provisionamento dos provedores.

Antes de Iniciar

Instale o plug-in do SCIM.

Função necessária: scim_admin

> **Aviso:** Conceda esta função com cuidado. A função scim_admin é equivalente a conceder ao usuário a função de administrador, porque a função scmin_admin pode adicionar ou atualizar Informações de identificação pessoal (PII).

Por Que e Quando Desempenhar Esta Tarefa

Você pode provisionar usuários usando o SCIM pelos seguintes métodos de autenticação:

- Provisionamento do usuário usando a autenticação básica
- Provisionando usuário usando OAuth

Provisionamento do usuário usando a autenticação básica

A configuração do SCIM provisiona e desprovisiona usuários e grupos automaticamente na ServiceNow usando o serviço de provisionamento dos provedores com a Autenticação básica.

Antes de Iniciar

Função necessária: scim_admin

> **Aviso:** Conceda esta função com cuidado. A função scim_admin é equivalente a conceder ao usuário a função de administrador, porque a função scmin_admin pode adicionar ou atualizar Informações de identificação pessoal (PII).

É necessário ativar o plug-in SCIM.

Procedimento

1. Navegue até **Todas** > **Serviços Web do Sistema** > **Políticas de Acesso à REST API** para verificar os detalhes das Políticas de Acesso à REST API.
2. Na página Política de acesso à API, clique no registro **Política de API do SCIM**.
3. Verifique se o registro de **Autenticação básica da SCIM API** está disponível nas seções Perfis de autenticação.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Verifique se o campo **Autenticação básica** está especificado com o registro de **SCIM API** que foi configurado ou verificado anteriormente como registro de aplicação.
5. Crie as configurações necessárias no sistema do provedor.
6. Teste a conexão para garantir que o provedor possa se conectar à ServiceNow.

> **Nota:** Se a conexão falhar, certifique-se de que sua conta da ServiceNow tenha permissões de administrador e tente novamente.

Provisionando usuário usando OAuth

Configure o provedor de SCIM para provisionar e desprovisionar usuários e grupos da ServiceNow usando o serviço de provisionamento de provedores com OAuth.

Antes de Iniciar

Função necessária: scim_admin

> **Aviso:** Conceda esta função com cuidado. A função scim_admin é equivalente a conceder ao usuário a função de administrador, porque a função scmin_admin pode adicionar ou atualizar Informações de identificação pessoal (PII).

É necessário ativar o plug-in SCIM.

Procedimento

1. Navegue até **Todos** > **OAuth de Sistema** > **Registro de aplicações**.
2. Na página Registros de aplicação, clique no registro da **SCIM API**.
3. Verifique os detalhes do registro da **SCIM API**.

   Esses detalhes devem ser fornecidos ao configurar a aplicação da ServiceNow no Azure AD.

4. Navegue até **Todas** > **Serviços Web do Sistema** > **Políticas de Acesso à REST API** para verificar os detalhes das Políticas de Acesso à REST API.
5. Na página Política de acesso à API, clique no registro **Política de API do SCIM**.
6. Verifique se o registro **SCIMAPIOAuthOnly** está disponível nas seções de Perfis de autenticação.
7. Verifique se o campo **Entidade OAuth** está especificado com o registro **SCIM API** que foi configurado ou verificado anteriormente como registro de aplicação.
8. Crie as configurações necessárias no sistema do provedor.
9. Teste a conexão para garantir que o provedor possa se conectar à ServiceNow.

> **Nota:** Se a conexão falhar, certifique-se de que sua conta da ServiceNow tenha permissões de administrador e tente novamente.

Solução de problemas de SCIM

Cenários de erros comuns de integração com SCIM.

URL da REST API inválido

Ação: Insira um URL de API válido. Deve ser capaz de fazer a verificação cruzada do URL do REST API no **Explorador de REST API**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nenhum URL de redirecionamento está definido na instância ServiceNow

Ação: Insira um URL de redirecionamento válido para a entidade OAuth de SCIM em ServiceNow. Insira o URL de redirecionamento ao configurar a entidade OAuth em ServiceNow.

Quando o URL de redirecionamento for diferente da solicitação

Ação: "**redirecionamento_url**" fornecido em "**Endpoint de autorização"** deve ser igual à entidade OAuth configurada em ServiceNow.

Nota:

Este erro ocorre quando há uma incompatibilidade entre o "endpoint de autorização" do Azure e o "URL de redirecionamento" do ServiceNow.

Quando um segredo de cliente inválido é aprovado

Ação: o valor inserido em "Segredo do cliente" deve ser igual ao da entidade OAuth configurada em ServiceNow.

Quando um "ClientId" inválido é aprovado no "EndPoint de autorização" do Azure.

Ação: o valor inserido para o parâmetro "client_id" em "Endpoint de autorização" deve ser igual ao da entidade OAuth configurada em ServiceNow.

Personalização do SCIM

Personalize os protocolos do SCIM para o gerenciamento de identidade.

A personalização do SCIM permite que você faça o seguinte:

- Ofereça suporte a campos personalizados nas tabelas sys_user e sys_user_group por meio da geração de esquema de extensão dinâmica.
- Forneça uma capacidade para substituir os mapeamentos de SCIM padrão.

Um administrador do SCIM pode definir esquemas de extensão personalizados para recursos de usuário e grupo. Os atributos definidos no esquema de extensão personalizado podem ser mapeados para campos nas tabelas sys_user ou sys_user_group.

Configurações para personalização do SCIM

Para personalização do SCIM, você deve executar as seguintes tarefas:

- Defina um esquema de extensão personalizado para usuários e grupos na tabela Esquema de extensão do SCIM. Para obter mais informações, consulte Criar um esquema de extensão de SCIM.
- Crie entidades em uma definição de ETL para atributos de esquema personalizados. As entidades são criadas para a tabela de destino mapeada com os atributos sys_user ou sys_user_group. Para obter mais informações, consulte Criar uma definição de ETL de SCIM.
- Crie um mapeamento de RTE entre essas duas entidades. Para obter mais informações, consulte a etapa 5 no Criar uma definição de ETL de SCIM.
- Envie atributos de esquema personalizado com dados na carga da solicitação de API do SCIM.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A API do SCIM chama o mecanismo de RTE com o mapeamento definido. Os dados são armazenados nos respectivos campos na tabela de destino, conforme definido no mapeamento.

Propriedades e esquemas de personalização do SCIM

A personalização do SCIM inclui as seguintes propriedades, esquemas compatíveis e esquemas não compatíveis.

Propriedades

A personalização do SCIM adiciona as seguintes propriedades do sistema.

Propriedades

Nome	Descrição
com.snc.integration.scim2.max.member.count	A contagem máxima de membros do SCIM.
com.snc.integration.scim2.resolve.extensionAttributes	Resolva recursos de SCIM com base na definição de origem do cliente solicitante se vários recursos forem localizados com um filtro de SCIM de ID externo. **Nota:** Como pré-requisito, se o provisionamento for feito de várias origens, as origens deverão ser definidas na tabela Definição de origem do SCIM. Se as origens não estiverem definidas ou se esta propriedade estiver inativa, todos os recursos correspondentes serão retornados com uma resposta de filtro de ID externo.
com.snc.integration.scim2.user.etl.definition	O ID de definição de ETL do usuário de SCIM.
com.snc.integration.scim2.group.etl.definition	ID de definição de ETL do grupo de SCIM
com.snc.integration.scim2.rte.verbose.logging.enabled	Habilite registro em log detalhado nas definições de RTE do grupo e do usuário de SCIM
com.snc.integration.scim2.string.field.validation.enabled	A validação de comprimento dos campos. Esta propriedade permite a validação em vez de truncar e salvar o campo.
com.snc.integration.scim2.provider.customization.script	O ID da inclusão de script para personalizar as respostas do SCIM.

Esquemas compatíveis

A personalização do SCIM adiciona os seguintes esquemas compatíveis.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Esquemas compatíveis

Esquemas	Descrição	Prefixo	Exemplo
urn:ietf:params:scim:schemas:core:2.0:User	Inclui atributos principais para os recursos.	nenhum	name.middleName
urn:ietf:params:scim:schemas:extension:servicenow:2.0:User	Inclui atributos relacionados a ServiceNow.	servicenow	servicenow.manager.value
urn:ietf:params:scim:schemas:extension:customized:2.0:User	Inclui atributos personalizados que não são mapeados como parte da extensão principal ou do esquema de extensão da ServiceNow.	Personalizado	custom.sscialId

Esquemas não compatíveis

urn:ietf:params:scim:schemas:extension:enterprise:2.0:User: inclui atributos comumente usados na representação de usuários que pertencem ou atuam em nome de um negócio ou uma empresa.

Nota: O esquema corporativo é um esquema válido, mas seus atributos são mapeados para qualquer tabela. Como não há suporte para a persistência do banco de dados, nenhum erro será exibido se um esquema corporativo for incluído no corpo da solicitação.

Criar um esquema de extensão de SCIM

Crie atributos personalizados para mapear para campos que não são mapeados como parte do esquema principal ou do esquema de extensão da ServiceNow.

Antes de Iniciar

Função necessária: scim_admin

Aviso: Conceda esta função com cuidado. A função scim_admin é equivalente a conceder a função de administrador ao usuário, porque a função scmin_admin pode incluir novos registros nas tabelas que podem ignorar lógicas de negócios ou proteções de ACL.

Procedimento

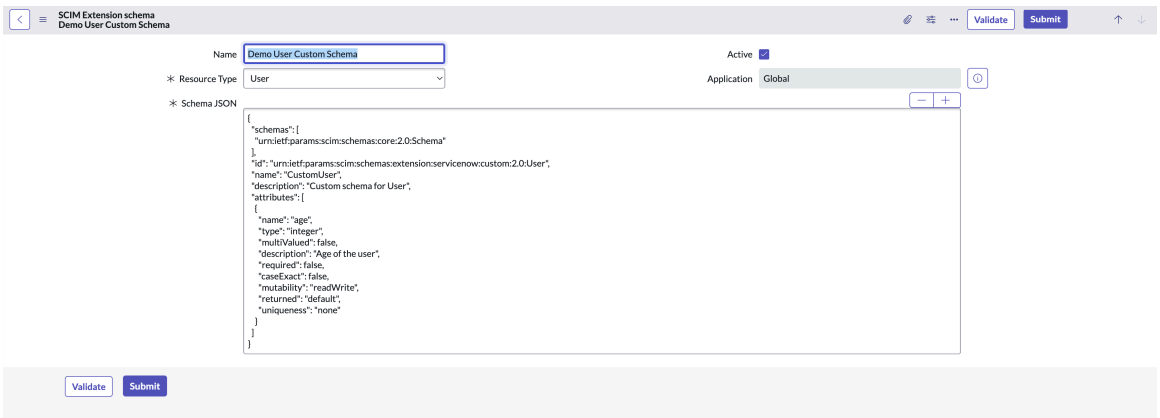
1. Navegue até **Todos** > **SCIM** > **Esquemas de extensão de SCIM**.
2. Clique em **Nova**.
3. No formulário, preencha os campos.

Nota: Somente um esquema de extensão pode ser mapeado para o campo **Tipo de recurso**. Por exemplo, usuário como um tipo de recurso pode ser mapeado para um esquema de extensão do usuário.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Esquema de extensão de SCIM

Campo	Descrição
Nome	Nome do esquema de extensão.
Ativo	Opção para ativar o esquema. Selecione este campo se o registro precisar ser considerado como um esquema de extensão personalizado. Somente um registro de esquema de extensão personalizado pode estar ativo por vez para um tipo de recurso específico, seja para o tipo de Usuário ou Grupo.
Tipo de recurso	Tipo de recurso que precisa ser mapeado para o esquema de extensão. A seguir estão as opções: ◦ **Usuário** ◦ **Grupo**
Aplicação	Escopo da aplicação para este registro.
Esquema JSON	Detalhes nos esquemas JSON. Para obter mais informações sobre como definir o esquema de extensão com atributos, consulte Datatracker.



4. Valide os atributos clicando em **Validar**.
5. Clique em **Enviar**.

Resultados

O esquema de extensão com atributos personalizados relacionados ao tipo de recurso Usuário ou Grupo é criado. Use as definições de ETL do SCIM para mapear os recursos com base no esquema de extensão nas tabelas sys_user e sys_user_group. Para obter mais informações, consulte Criar uma definição de ETL de SCIM.

Criar uma definição de ETL de SCIM

Use as definições de ETL de SCIM para mapear os atributos personalizados com as tabelas sys_user ou sys_user_group.

Antes de Iniciar

Função necessária: scim_admin

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Aviso: Conceda esta função com cuidado. A função scim_admin é equivalente a conceder a função de administrador ao usuário, porque a função scmin_admin pode incluir novos registros nas tabelas que podem ignorar lógicas de negócios ou proteções de ACL.

Nota:

- As definições de ETL de Grupo e Usuário de SCIM fazem parte do sistema de base para mapeamento de recursos. Você pode usar os mesmos mapeamentos de recursos e mudar os critérios conforme necessário, ou pode criar novos mapeamentos de recursos.
- Não há suporte para campos [*] por meio de RTE no mapeamento SCIM.

Procedimento

1. Siga as instruções em Criar definições de carga de transformação de extração (ETL).
2. Abra o registro recém-criado e exiba os detalhes.
3. Na seção Entidades de ETL, crie uma entidade clicando em **Novo**.
   Você precisa criar entidades para os seguintes usuários:
   - scim-user: para os campos que são do SCIM.
   - Tabela de usuário (sys_user) ou grupo (sys_user_group): para os campos que você deseja mapear da tabela de banco de dados com o SCIM. Por exemplo, para personalização de detalhes do usuário por meio do SCIM, você pode usar a tabela sys_user.

   a. No formulário, preencha os campos.

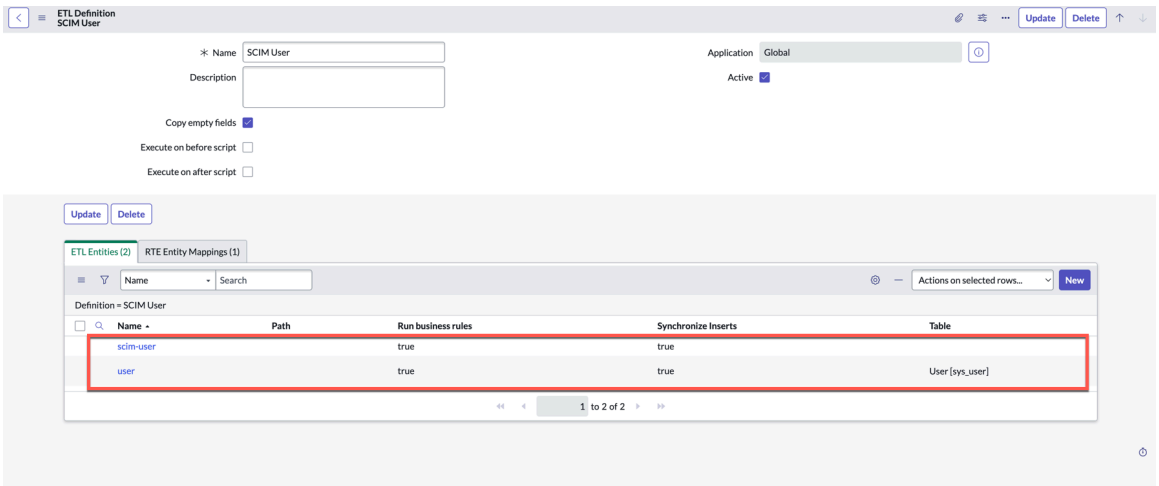
Formulário de entidade de ETL

Campo	Descrição
Nome	Nome da entidade de ETL.
Aplicação	Escopo da aplicação para este registro.
Tabela	Tabela de destino para a entidade de ETL.
Definição	Entidade de ETL selecionada.
Caminho	Caminho exclusivo para esta entidade. Não especifique nenhum caminho para a entidade que representa a tabela de conjunto para importação. Quando uma entidade representa uma coleção, o caminho deve terminar com um asterisco [*]. Este requisito se aplica a entradas intermediárias e à entidade da tabela de destino.
Sincronizar inserções	Opção para garantir apenas um registro com valores de campos unificados exclusivos sincronizando as inserções de registro.
Executar regras de negócio	Opção para executar regras de negócio.

   b. Clique em **Enviar**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

As entidades de ETL são criadas para scim-user e tabelas de usuário. Você precisa criar campos de entidade de ETL nessas entidades de ETL e mapear ambas as entidades criando um mapeamento de entidade de RTE.



4. Crie as entidades e mapeie-as.

   a. Abra o registro enviado (scim-user e usuário).

   b. Nos campos Entidade de ETL, adicione os campos clicando em **Novo**.

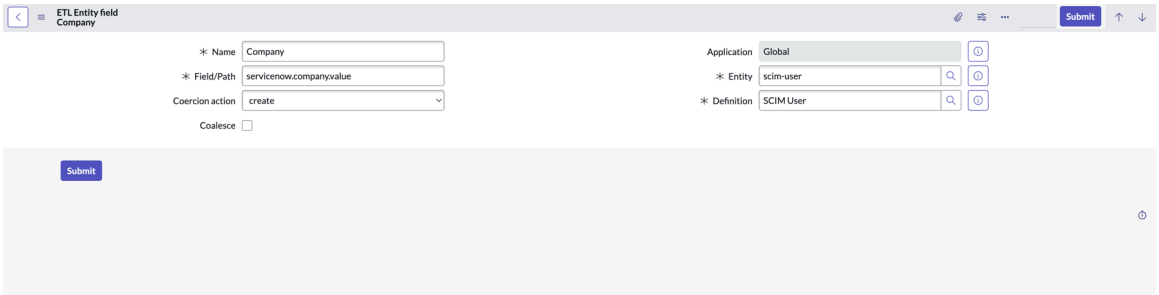
   c. No formulário, preencha os campos.

Formulário de entidade de ETL

Campo	Descrição
Nome	Nome da definição do campo de entidade de ETL.
Aplicação	Entidade de ETL selecionada à qual esta definição de campo pertence.
Campo/Caminho	Este campo é uma coluna ou um caminho. ▪ O campo é um nome de coluna quando a entidade é a tabela de importação ou destino. ▪ O campo é um caminho quando o campo tem estruturas aninhadas.
Entidade	Entidade à qual esta operação se aplica. Escolha a entidade usando o ícone de pesquisa.
Ação de coerção	O que o sistema deve fazer se uma referência ou opção não puder ser encontrada. As opções são as seguintes:

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

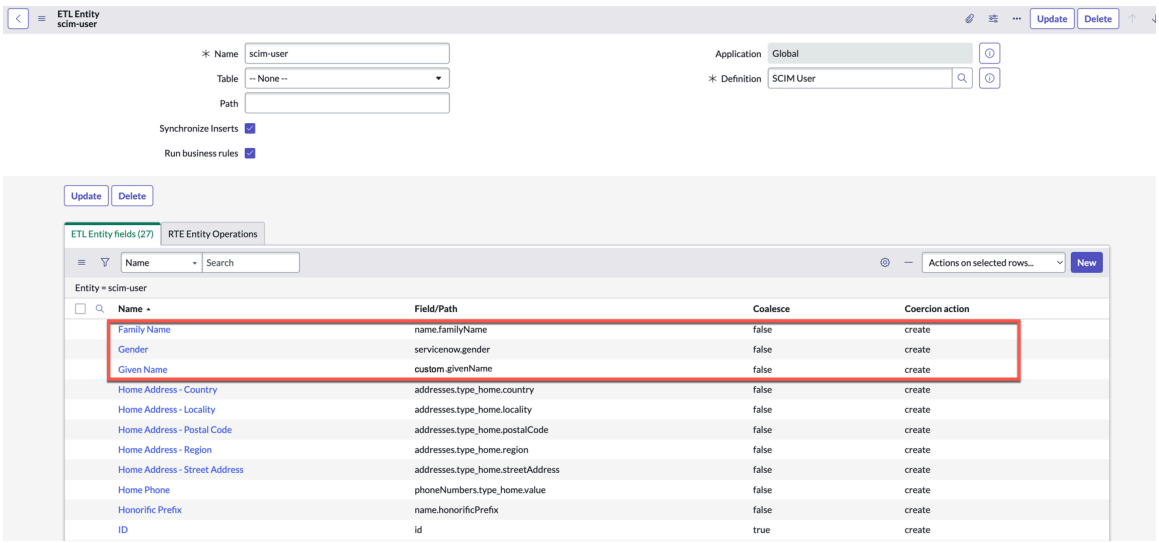
Campo	Descrição
	▪ **Criar**: crie uma nova referência ou opção. Atribua a referência ou opção ao registro atual. ▪ **Rejeitar**: não salve o registro inteiro no banco de dados. ▪ **Ignorar**: defina o valor atual como vazio.
Definição	Entidade de ETL selecionada à qual esta definição de campo pertence.
Aglutinar	Opção para consultar os registros existentes.



d. Envie as entradas clicando em **Enviar**.

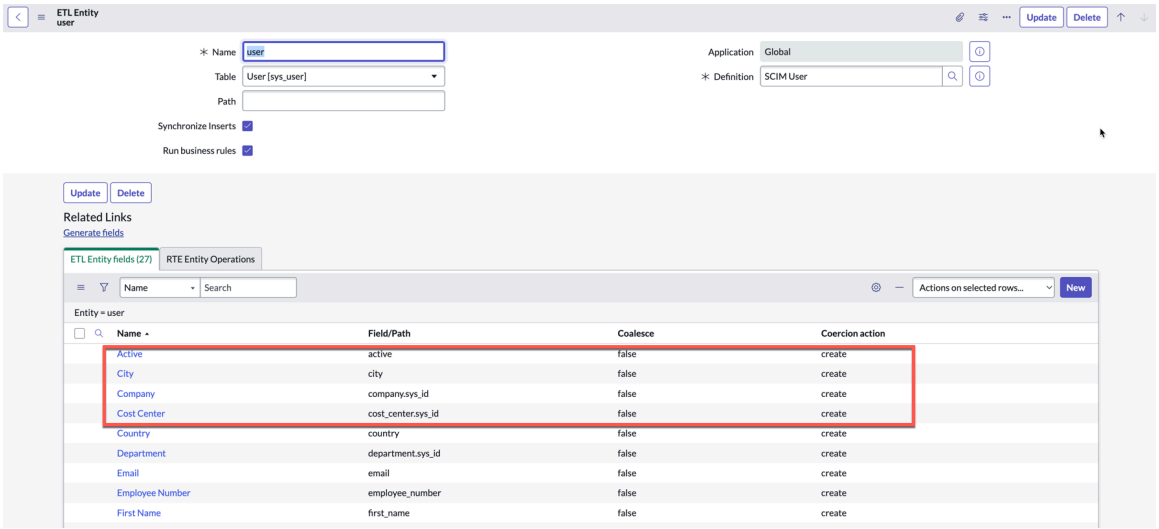
Você pode adicionar várias entradas como seu campo Entidade de ETL com base em seus requisitos.

A entidade de ETL scim-user pode ter entidades com a extensão principal (usuário), a extensão da ServiceNow ou a extensão personalizada.



A entidade de ETL do usuário pode ter entidades da tabela do banco de dados. Por exemplo, a tabela sys_user.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



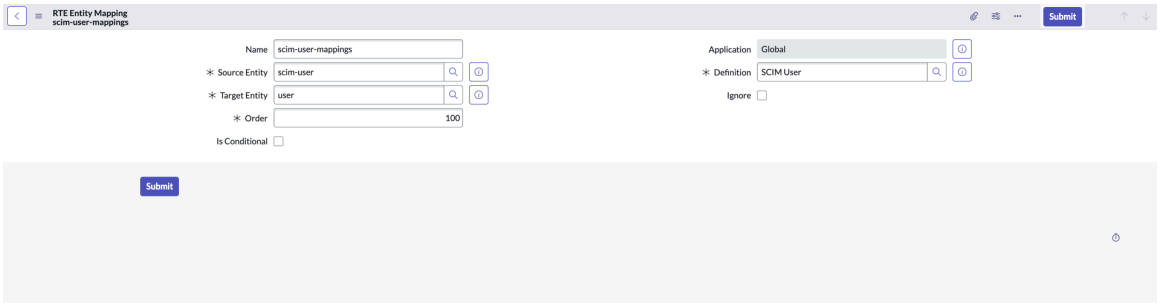
Nota: Para adicionar um filtro nos campos SCIM de entrada, use um sublinhado (_). Este sublinhado se traduz em um filtro de EQ. Por exemplo, o atributo *email.type_work.value* aplica o filtro de SCIM de e-mail *[type eq "work"].value*.

Depois que os campos são criados nos registros de Entidade de ETL do scim-user e do usuário, é necessário criar um registro de mapeamento de Entidade de RTE. Em seguida, você deve especificar a definição de origem e de destino para mapear ambos os campos.

5. Na seção Mapeamentos da Entidades de RTE, crie um mapeamento de entidade clicando em **Novo**
6. No formulário, preencha os campos.

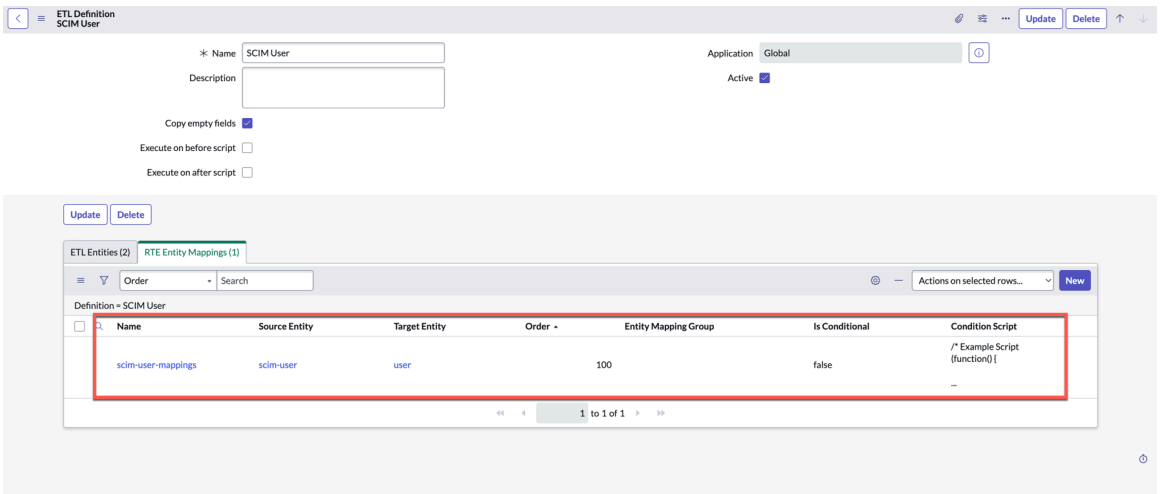
Campo	Descrição
Nome	Nome do mapeamento.
Entidade de origem	Entidade de origem para o mapeamento.
Entidade de destino	Entidade de destino para o mapeamento.
Ordem	Ordem na qual o mapeamento deve ser processado.
É condicional	Opção para designar o mapeamento como condicional.
Script de condição	Script que define as condições que devem ser atendidas para o mapeamento.
Aplicação	Escopo da aplicação para este registro.
Definição	Entidade de ETL selecionada à qual este mapeamento pertence.
Ignorar	Opção para designar se este mapeamento de entidade de ETL deve ser ignorado ao executar integrações de dados usando a Transformação robusta do conjunto para importação (RTE).

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



7. Clique em **Enviar**.

   O exemplo a seguir mostra um registro criado para mapear os registros de Entidade de ETL de scim-user e do usuário.



8. Abra o registro enviado (scim-user-mappings) e crie um mapeamento entre o scim-user e os registros de Entidade de ETL do usuário.

   a. Na seção Mapeamentos de campo de RTE, clique em **Novo**.

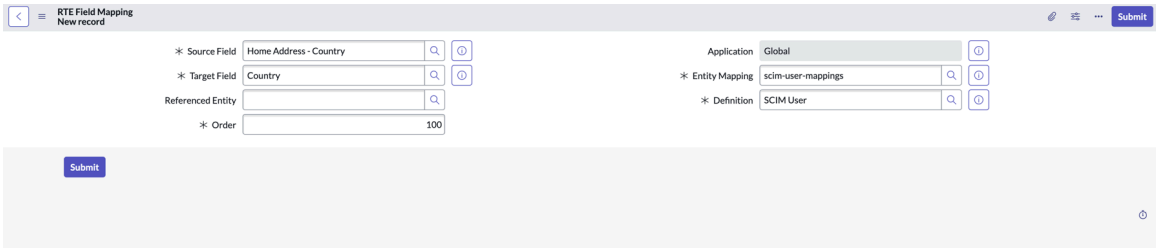
   b. No formulário, preencha os campos.

Campos da Entidade ETL

Campo	Descrição
Campo de origem	Escopo da aplicação para este registro.
Aplicação	Entidade de ETL selecionada à qual esta definição de campo pertence.
Campo de destino	Campo ETL de saída para a operação se a operação tiver uma única saída.
Mapeamento de entidade	Mapeamento de entidade ao qual esta operação se aplica.
Entidade referenciada	Entidade referenciada e a operação à qual ela se aplica.
Definição	Entidade de ETL selecionada à qual esta definição de campo pertence.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

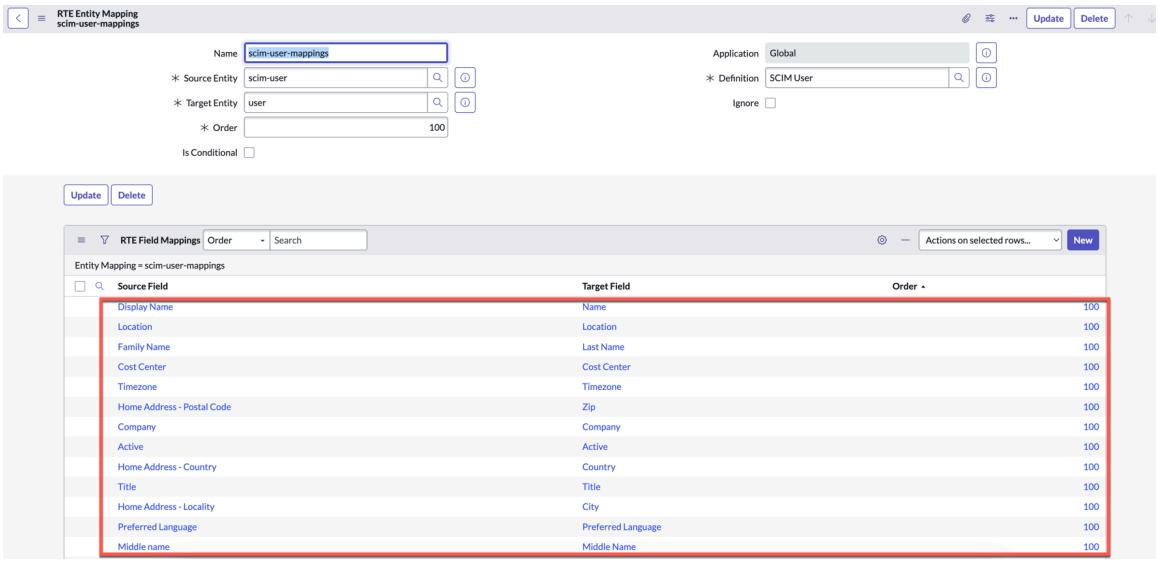
Campo	Descrição
Ordem	Ordem na qual a operação é executada na entidade.



O campo de origem **Endereço residencial - País** (entidade de ETL do scim-user) mapeia o campo de destino como **País** (entidade de ETL do usuário).

c. Envie as entradas clicando em **Enviar**.

Você pode adicionar várias entradas como seus mapeamentos de Entidade de RTE com base em seus requisitos.



Os campos de origem e de destino são mapeados conforme configurados. Quando você executa operações CRUD usando o SCIM, os valores personalizados são atualizados na respectiva tabela.

Resultados

Essas definições e mapeamentos de ETL permitem extrair dados de uma tabela de origem, transformar os dados conforme desejado e carregar os dados em uma tabela de destino.

Informações relacionadas

Criar definições de carga de transformação de extração (ETL)

Como lidar com campos não mapeados

Você pode lidar com campos não mapeados na personalização do SCIM de maneiras diferentes.

Durante a personalização do SCIM, os campos que não fazem parte das tabelas sys_user e sys_user_group podem ser mapeados executando as funções a seguir.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Personalizar SCIM (criar ou atualizar)

Você pode criar ou atualizar o Cliente de SCIM.

- O administrador do SCIM pode adicionar scripts personalizados nos scripts *onBefore* e *onAfter* para campos que não estão mapeados na definição de ETL ou no RTE.
- O administrador do SCIM pode substituir mapeamentos de RTE adicionando scripts personalizados nos scripts *onBefore* e *onAfter*.
- Você pode invocar uma API passível de script nos scripts de RTE *onBefore* ou *onAfter* para acessar a solicitação de entrada e executar transformações em outras tabelas, listas e atributos não mapeados.
- Você pode usar o método *sn_auth.SCIM2Util.getScimProviderCustomizationContext()* para fornecer o contexto de solicitação SCIM que contém o objeto *scimResource*. O *scimResource* no contexto representa o seguinte em cada operação:
  - **POST**: o recurso do SCIM enviado na carga da solicitação.
  - **PUT**: o recurso do SCIM atual do banco de dados substituído pelo recurso do SCIM enviado na carga da solicitação.
  - **PATCH**: o recurso do SCIM atual do banco de dados depois de executar as operações de patch.

A seguir está um exemplo de um script *onAfter*.

```
(function onAfter(source, target, importLog) {

    var ctx = sn_auth.SCIM2Util.getScimProviderCustomizationContext();
    gs.info("scim context ee: " + JSON.stringify(ctx.scimResource));

    var roles = ctx.scimResource.roles;
    if(roles) {
        var removingRolesGR = new GlideRecord("sys_user_has_role");
        removingRolesGR.addQuery("user", target.sys_user[0].sys_id);
        removingRolesGR.query();
        removingRolesGR.deleteMultiple();

    for (var i = 0; i < roles.length; i++) {
        var addingRolesGR = new GlideRecord("sys_user_has_role");
        addingRolesGR.setValue("user", target.sys_user[0].sys_id);
        addingRolesGR.setValue("role", roles[i].value);
        addingRolesGR.setValue("state", "active");
        addingRolesGR.insert();
        }
        }
        var customUserExtn = new
 global.SCIMProviderCustomization().getCustomExtensionUrn('User');
        var salary = ctx.scimResource[customUserExtn].salary;
        if (salary) {
            var gr = new GlideRecord("u_user_salary");
            gr.addQuery("user", target.sys_user[0].sys_id);
            gr.query();
            if (gr.next()) {
                gr.setValue("salary", salary);
                gs.info("scim update: " + gr.update());
            } else {
```

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

```
            gr.setValue("salary", salary);
            gr.setValue("user", target.sys_user[0].sys_id);
            gr.insert();
            }
           }

})(source, target, importLog);
```

Personalizar a resposta do SCIM

Para as chamadas de API GET, qualquer resposta de retorno para o cliente de SCIM pode ser personalizada usando o script, estendendo o script *SCIMProviderCustomization*.

Ao estender o script, o autor pode substituir os métodos *customizeUserResponse* e *customizeGroupResponse* para modificar as respostas dos recursos de Usuário e Grupo.

A propriedade *com.snc.integration.scim2.provider.customization.script.id* permite que o plug-in SCIM use o script que deve ser usado para personalização de resposta.

Veja a seguir um exemplo de extensão do script base.

```
var SCIMCustomizationScript = Class.create();
SCIMCustomizationScript.prototype =
 Object.extendsObject(SCIMProviderCustomization, {
    initialize: function() {
        SCIMProviderCustomization.prototype.initialize.call(this);
    },
    customizeUserResponse: function(context) {
        try {
            var rolesGR = new GlideRecord("sys_user_has_role");
            rolesGR.addQuery("user", context.scimResource.id);
            rolesGR.query();
            var i = 0;
            context.scimResource.roles = [];
            while (rolesGR.next()) {
                context.scimResource.roles[i] = {
                    display: rolesGR.getElement('role.name').getValue(),
                    value: rolesGR.getElement('role.sys_id').getValue()
                };
                i++;
            }
            var userGR = new GlideRecord("u_user_salary");
            userGR.addQuery("user", context.scimResource.id);
            userGR.query();
            if (userGR.next()) {
                var salary = userGR.getValue("salary");
                if (salary) {
                    var customExtensionValue =
 SCIMProviderCustomization.prototype.getCustomExtensionNodeValue.call(th
is, "User", context);
                    customExtensionValue.salary = salary;

 SCIMProviderCustomization.prototype.setCustomExtensionNodeValue.call(th
is, "User", context, customExtensionValue);
                }
            }
        } catch (ex) {
```

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

```
            gs.error("err: " + ex);
        }
        return context;
    },
    customizeGroupResponse: function(context) {
        return context;
    },
    type: 'SCIMCustomizationScript'
});
```

Nota:

- O parâmetro que os métodos *customizeUserResponse* e *customizeGroupResponse* contêm é um objeto de contexto com um atributo chamado *scimResource*. Este atributo tem todos os atributos de um objeto de recurso de usuário ou grupo.
- Uma inclusão de script personalizada só pode ser criada e exibida pelo administrador.
- Se um recurso de usuário ou grupo for modificado, você deverá retornar o contexto.
- Se não houver modificação de qualquer atributo no objeto de recurso, defina *com.snc.integration.scim2.provider.customization.script.id* como vazio ou retorne como nulo.
- Se determinados atributos forem persistentes por meio do script *onAfter*, eles deverão ser preenchidos com valores de banco de dados no objeto *scimResource* dentro do script personalizado. Esta ação é necessária para que o sistema possa fazer o seguinte:
  - Para obter o objeto *scimResource* correto em scripts *onAfter* durante a operação PUT e PATCH.
  - Para incluir os atributos que persistiram por meio do script *onAfter* na resposta de retorno para o cliente.

Funções de ajuda

A seguir estão algumas das funções de ajuda para personalização do SCIM. Essas funções permitem que você obtenha ou defina diferentes tipos de informações.

Funções de ajuda

Função	Finalidade
SCIMProviderCustomization.prototype.getExtensionSchemaValue(this, "User");	Obter o valor do esquema de extensão personalizado.
SCIMProviderCustomization.prototype.getExtensionSchemaValue(this, "User");	Obter o valor do esquema da extensão da ServiceNow.
SCIMProviderCustomization.prototype.getCustomExtensionSchemaValue(this, "User", context);	Obter o nó do esquema personalizado da resposta.
SCIMProviderCustomization.prototype.getExtensionSchemaValue(this, "User", context);	Obter o nó do esquema personalizado da ServiceNow da resposta.
SCIMProviderCustomization.prototype.setCustomExtensionSchemaValue(this, "User", context, customExtensionValue);	Definir o nó do esquema personalizado na resposta.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A seguir está um exemplo de uso da função de ajuda:

```
var customExtensionUrn =
SCIMProviderCustomization.prototype.getCustomExtensionUrn.call(this,
 "User");
var customExtensionValue =
SCIMProviderCustomization.prototype.getCustomExtensionNodeValue.call(th
is, "User", context);
customExtensionValue.age = "18";
SCIMProviderCustomization.prototype.setCustomExtensionNodeValue
 call(this, "User", context, customExtensionValue);
```

Nota: O RTE oferece suporte à configuração de dados em tabelas diferentes das tabelas sys_user e sys_user_group.

Criando uma definição de origem

Crie uma definição de origem para capturar informações sobre de qual origem de identidade um recurso é provisionado.

Antes de Iniciar

Função necessária: scim_admin

Aviso: Conceda esta função com cuidado. A função scim_admin é equivalente a conceder ao usuário a função de administrador, porque a função scmin_admin pode adicionar ou atualizar Informações de identificação pessoal (PII).

Por Que e Quando Desempenhar Esta Tarefa

Usando uma definição de fonte, a fonte de identidade de provisionamento pode ser mapeada para uma entidade OAuth usando aquela autenticada durante o provisionamento.

Depois que uma definição de origem é criada, todos os recursos provisionados dessa origem de identidade são mapeados para seu ID de definição de origem correspondente.

A definição de origem captura as informações de origem necessárias, como ao fazer o seguinte:

- Identifica o Cliente de SCIM do qual o recurso é provisionado.
- Resolve informações duplicadas fornecidas pelo ID externo:
  - Se várias origens de identidade estiverem provisionando recursos, poderá haver dois ou mais recursos com o mesmo valor de ID externo porque o ID externo é exclusivo para a origem da identidade.
  - Se vários recursos forem retornados com um filtro de SCIM de ID externo, os recursos poderão ser resolvidos com base na definição de origem da origem de identidade solicitante.

Nota: Uma definição de origem pode ser criada somente para a origem da identidade, que usa um método de autenticação OAuth.

Procedimento

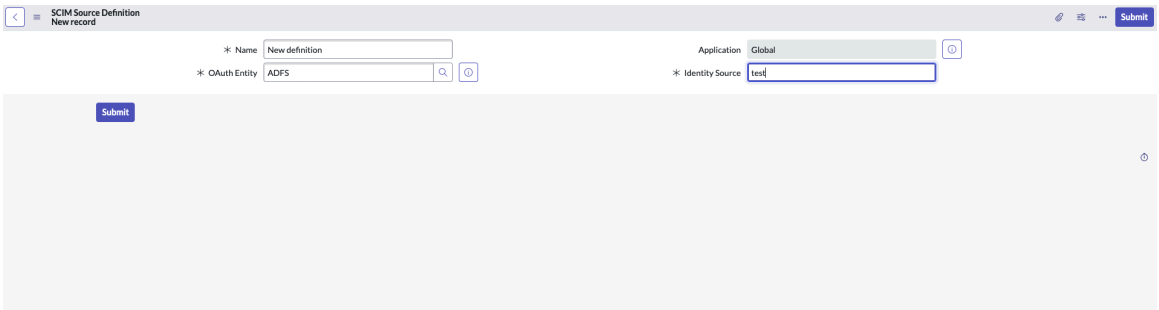
1. Navegue até **Todos** > **SCIM** > **Definição de origem**.
2. Na página Definições de origem do SCIM, clique em **Novo**.
3. No formulário, preencha os campos.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Definição da origem de SCIM

Campo	Descrição
Nome	Nome da definição de origem.
Aplicação	Escopo da aplicação para este registro.
Entidade OAuth	A entidade OAuth do usuário de integração. A entidade é usada para provisionar o usuário pelo provedor de origem de identidade.
Origem da identidade	O nome do provedor de origem de identidade. Por exemplo, Azure AD, Okta e assim por diante

Nota: Habilite a propriedade *com.snc.integration.scim2.resolve.externalid.conflict* para retornar somente os recursos de SCIM criados pela origem da identidade da solicitação. Por padrão, todos os recursos correspondentes com um filtro de ID externo são retornados.



4. Clique em **Enviar**.

Resultados
A definição de origem de SCIM é criada. Use as definições de ETL do SCIM para mapear os recursos com base no esquema de extensão nas tabelas sys_user e sys_user_group. Para obter mais informações, consulte Criar uma definição de ETL de SCIM.

Cliente de SCIM

O Cliente de SCIM facilita o provisionamento e atualiza os recursos de identidade por meio de operações CRUD expostas pelo endpoint do SCIM em um sistema externo.

Explorar

Saiba mais sobre o cliente de SCIM.

Ativar

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

	Ativar o cliente de SCIM.
Propriedades do cliente de SCIM Veja os detalhes sobre como personalizar o SCIM.	Solução de problemas Saiba mais sobre a definição de origem para SCIM.

Como explorar o cliente do SCIM

O Cliente de SCIM facilita o provisionamento e atualiza os recursos de identidade por meio de operações CRUD expostas pelo endpoint do SCIM em um sistema externo.

O Cliente do SCIM é usado para criar, atualizar e excluir recursos de identidade em um sistema que é compatível com solicitações REST em conformidade com SCIM. O cliente é usado para gerenciamento de ciclo de vida de identidade e para sincronização de atributo de identidade em instâncias da ServiceNow ou entre a ServiceNow e outros provedores de SCIM.

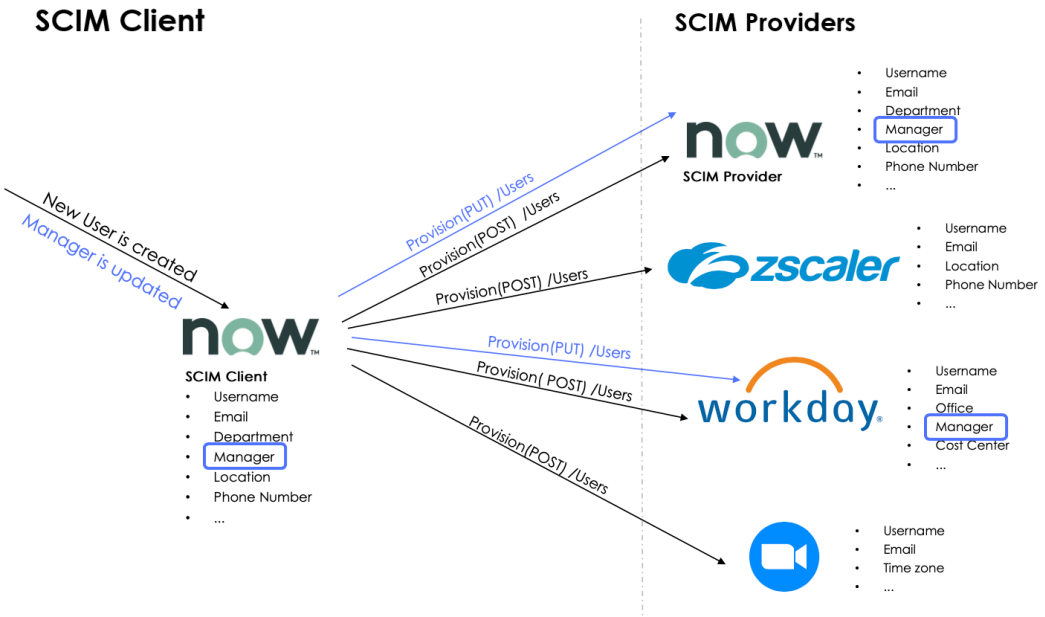
Como as APIs são expostas pelo cliente, você pode automatizar o processo de criação, atualização ou exclusão de quaisquer recursos em um único ou em vários provedores de SCIM. Por exemplo, se um desenvolvedor ingressar na empresa, você precisará fornecer acesso ao Git, ao local de trabalho e assim por diante.

O cliente de SCIM permite que você execute as seguintes ações:

- Provisionar identidades e acesso para associação de usuário ou grupo.
- Sincronizar a identidade e os recursos relacionados com os sistemas compatíveis com o SCIM.
- Integrar qualquer Provedor de SCIM na ServiceNow®.
- Desprovisionar identidades e acesso.

O Cliente de SCIM fornece APIs passíveis de script que o desenvolvedor de integração pode usar para criar fluxos de trabalho ou automações para realizar trabalhos específicos. Para saber mais sobre a API passível de script, consulte API SCIM2Client.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Configurações para Cliente de SCIM

Para configurar o Cliente de SCIM, execute as seguintes tarefas:

- Crie uma mensagem REST para todas as chamadas de saída de um Provedor de SCIM específico. Para obter mais informações, consulte Criar uma mensagem REST.
- Crie um Provedor de SCIM para buscar tipos de recursos e informações de esquemas do Provedor de SCIM com a mensagem REST. Habilite a configuração do Método HTTP (PUT ou PATCH) para atualizar um recurso no Provedor de SCIM. Para obter mais informações, consulte Criar um Provedor de SCIM.
- Crie os mapeamentos de atributos SCIM para atributos da ServiceNow para um tipo de recurso específico e Provedor de SCIM. Para saber mais, consulte Criar um Mapeamento de recursos do Provedor de SCIM.
- Execute o mapeamento do campo SCIM com a tabela do banco de dados e o nome do campo. Passe o valor padrão ou grave um script para obter o valor. Para obter mais informações, consulte Criar um mapeamento do atributo SCIM.

Ativar o plug-in do Cliente de SCIM

Para a ativação do Cliente de SCIM, instale o plug-in SCIM v2 - ServiceNow Cross-domain Identity Management Client (com.snc.integration.scim2.client).

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Navegue até **Todos** > **Aplicações do sistema** > **Todas as aplicações disponíveis** > **Todas**.
2. Encontre o plug-in SCIM v2 - ServiceNow Cross-domain Identity Management Client (com.snc.integration.scim2.client) usando os critérios de filtro e a barra de pesquisa.

   Pesquise o plug-in pelo nome ou ID. Se não conseguir encontrar um plug-in, talvez seja necessário solicitá-lo ao pessoal ServiceNow.

3. Selecione **Instalar** para iniciar o processo de instalação.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota: Quando a separação de domínio e o administrador delegado estão habilitados em uma instância, o usuário administrativo deve estar no domínio **global.** Caso contrário, será exibido o seguinte erro: `A instalação da aplicação não está disponível porque há outra operação em execução: ativação de plug-in para <plugin name>.`

Você verá uma mensagem após a conclusão da instalação.

Propriedades do Cliente de SCIM, tabelas, APIs passíveis de script e registros em log

O plug-in SCIM v2 - ServiceNow Cross-domain Identity Management Client (com.snc.integration.scim2.client) inclui as seguintes propriedades do sistema, tabelas, APIs passíveis de script e registros em log.

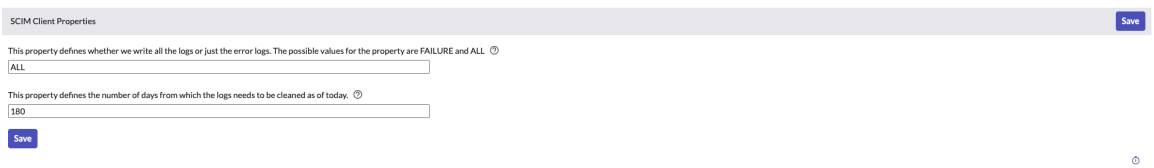
Propriedades

O Cliente de SCIM adiciona as seguintes propriedades do sistema.

Propriedades

Nome	Descrição
com.snc.integration.scim2.client.log.property.scope	Esta propriedade determina se todos os registros em log devem ser gravados ou apenas os registros em log de erros. Os valores possíveis são **FALHA** ou **TODOS**: Valor padrão: **TODOS**
com.snc.integration.scim2.client.log.cleanup.duration	Esta propriedade determina o número de dias para apagar os registros em log. Valor padrão: **180**

Para definir as propriedades, navegue até **Todos** > **SCIM** > **Propriedades do Cliente de SCIM**.



Tabelas

O Cliente de SCIM adiciona as tabelas a seguir.

Tabelas

Nome	Descrição
Provedor de SCIM (sys_scim_provider)	Armazena dados para cada provedor de SCIM, como nome, definições de recurso de mensagem REST e assim por diante.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabelas

Nome	Descrição
Mapeamento de recursos do provedor de SCIM (sys_scim_provider_resource_mapping)	Armazena as informações da tabela primária para cada provedor e nome de recurso.
Mapeamento de atributo SCIM (sys_scim_attribute_mapping)	Armazena os detalhes da origem de onde cada valor de atributo SCIM deve vir, como o campo da tabela, o script e assim por diante.
Registro em log do Cliente de SCIM (sys_scim_client_logs)	Armazena os status de cada chamada acionada para o Provedor de SCIM.

API passível de script

A API SCIM2Client chama o Sistema para o Provedor do Cross-domain Identity Management (SCIM) (função do servidor) criar, atualizar ou excluir dados em um provedor de serviço (SP). A API passível de script do Cliente de SCIM deve ser usada nos scripts que estão sendo executados no contexto do sistema ou por um usuário administrador do sistema.

Por exemplo, você pode usar o script ao executar o fluxo de trabalho do hub de integração como um usuário do sistema, ao executar os trabalhos agendados e assim por diante.

A seguir estão alguns dos casos de uso para usar as APIs passíveis de script:

- Como administrador, provisione informações de identidade de scripts em segundo plano, regras de negócio, chamadas de inclusão de script, fluxos de trabalho e assim por diante.
- Como administrador, execute um trabalho agendado ou um trabalho sob demanda para provisionamento de identidade.
- Execute um fluxo de trabalho ou subfluxo de trabalho com a etapa de script usando a chamada de API passível de script de provisionamento.
- Adicione o script de provisionamento diretamente em uma regra de negócio ou em uma inclusão de script. O script pode ser acionado por usuários não administradores. Este caso de uso funciona nas seguintes situações:
  - O usuário tem acesso ao token, o que significa que o usuário tem a função para gerar o token do modelo REST.
  - O usuário tem acesso para recuperar os valores de atributo SCIM das tabelas mapeadas.

Para saber mais sobre a API passível de script, consulte API SCIM2Client.

Registros em log do Cliente de SCIM

Os Registros em log do Cliente de SCIM exibem o status de provisionamento sobre as APIs do SCIM. Para exibir o status de provisionamento, navegue até **Todos** > **SCIM** > **Registros em log do Cliente de SCIM**.

Criar uma mensagem REST

Configure uma mensagem REST para todas as chamadas de saída de um Provedor de SCIM específico.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: administrador

Procedimento
1. Navegue até **Todos** > **Serviços Web do Sistema** > **Saída** > **Mensagem REST**.
2. Clique em **Novo**.
3. No formulário, preencha os campos.

Provedor de SCIM

Campo	Descrição
Nome	Nome descritivo desta mensagem
Endpoint	URL base do Provedor de SCIM. Por exemplo, `https://example.service-now.com/api/now/scim`.
Tipo de autenticação	Tipo de autenticação a ser usado para se conectar ao Provedor de SCIM externo. Para obter mais informações, consulte Autenticação REST de saída.
Cabeçalhos HTTP	O tipo de conteúdo esperado do Provedor de SCIM externo. Por exemplo, o nome do cabeçalho é o tipo de conteúdo no seguinte corpo de solicitação de API: `tipo de conteúdo: application/scim+json`

4. Na lista de métodos HTTP relacionada, clique em **Novo**.
5. Configure os seguintes métodos HTTP.

Nota: Os URLs têm variáveis que você deve substituir.

Métodos HTTP

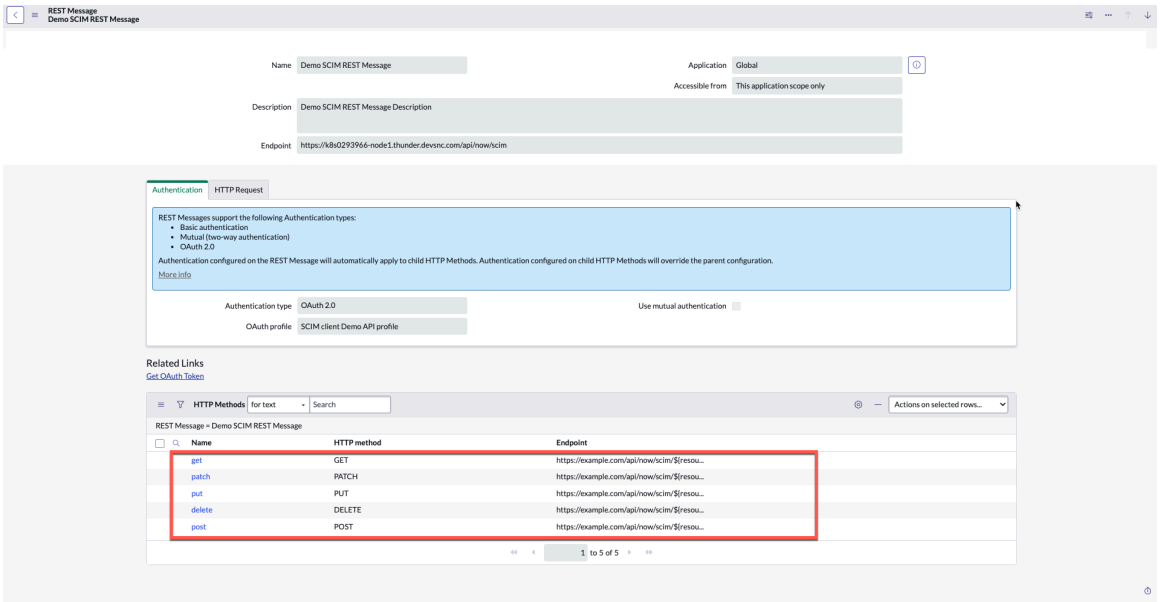
Métodos	URL de amostra
GET	`https://example.com/api/now/scim/${resourceName}`
PATCH	`https://example.com/api/now/scim/${resourceName}/${resourceId}`
PUT	`https://example.com/api/now/scim/${resourceName}/${resourceId}`
DELETE	`https://example.com/api/now/scim/${resourceName}/${resourceId}`

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Métodos	URL de amostra
POST	`https://example.com/api/now/scim/${resourceName}/${resourceId}`

Nota:

- Você deve criar todos os métodos HTTP para a operação do Cliente de SCIM.
- Uma mensagem REST de amostra é enviada do sistema de base.



6. Clique em **Enviar**.

Resultados

O registro da mensagem REST é criado.

O que Fazer Depois

Use a mensagem REST para criar um Provedor de SCIM. Para obter mais informações, consulte Criar um Provedor de SCIM.

Para saber mais sobre como criar uma mensagem REST, consulte Criar uma mensagem REST.

Criar um Provedor de SCIM

Crie um Provedor de SCIM para buscar tipos de recursos e informações de esquemas do Provedor de SCIM com a mensagem REST. Habilite a configuração do Método HTTP (PUT ou PATCH) para atualizar um recurso no Provedor de SCIM.

Antes de Iniciar

Nota: Um provedor de SCIM de amostra faz parte do sistema de base. Você pode usá-lo e configurá-lo com base em seus requisitos ou criar um novo registro.

Função necessária: administrador

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

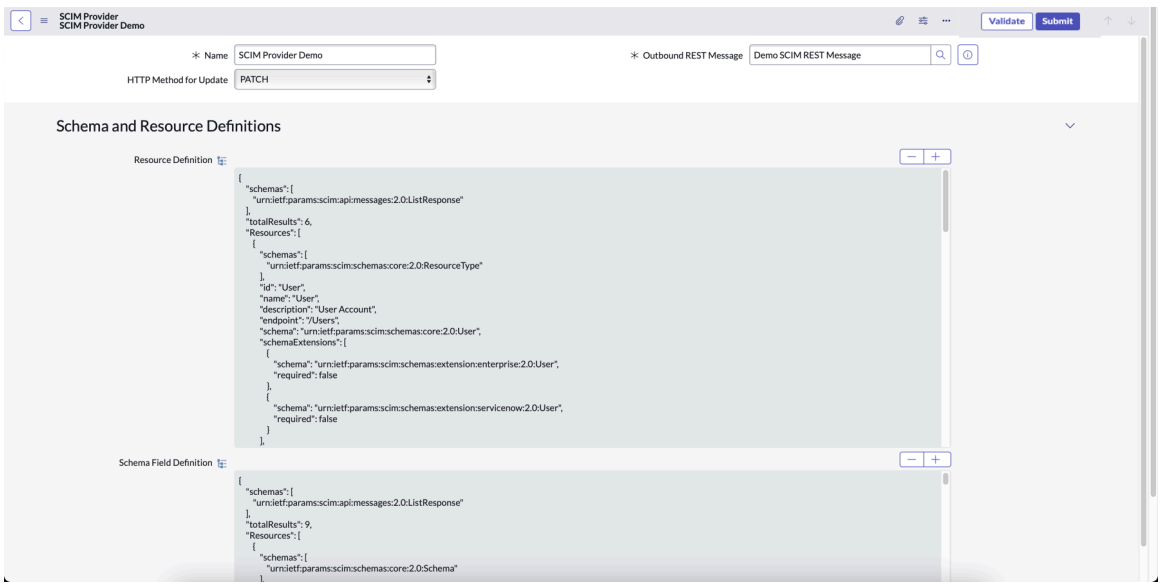
1. Navegue até **Todos** > **Cliente de SCIM** > **Provedor de SCIM**.
2. Na página Provedores de SCIM, clique em **Novo**.
3. No formulário, preencha os campos.

Formulário do Provedor de SCIM

Campo	Descrição
Nome	Nome do Provedor de SCIM
Mensagem de saída do REST	Mensagem usada para chamar a API do Provedor de SCIM. Para obter mais informações, consulte Criar uma mensagem REST.
Método HTTP para atualização	Tipo de método HTTPS usado para atualizar o mapeamento de recursos. O método PATCH ou PUT pode ser usado pelo Cliente ao atualizar o recurso de identidade durante o provisionamento de um recurso já existente.

Nota:

- Os campos **Definição de recurso** e **Definição de campo de esquema** são obtidos dos endpoints públicos */ResourceTypes* e */Schemas* do provedor de SCIM. Esses campos são preenchidos automaticamente depois que a mensagem REST é selecionada.
- Se a mensagem REST, os Esquemas ou os Tipos de recurso forem atualizados no Provedor de SCIM, clique em **Recarregar** e em **Atualizar** para atualizar os campos **Definição de Recurso** e **Definição de campo de esquema**.



4. Clique em **Enviar**.

Resultados

Os detalhes do Provedor de SCIM foram criados com sucesso. Use o Mapeamento de recursos do Provedor de SCIM para mapear os detalhes do Provedor de SCIM para

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

os recursos, como usuários ou grupos. Para obter mais informações, consulte Criar um Mapeamento de recursos do Provedor de SCIM.

Criar um Mapeamento de recursos do Provedor de SCIM

Defina os mapeamentos de atributos SCIM para atributos da ServiceNowpara um determinado tipo de recurso e Provedor de SCIM.

Antes de Iniciar

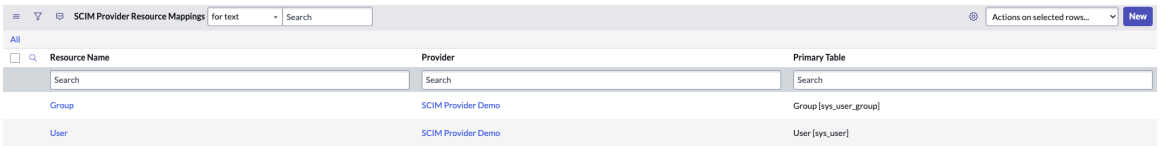
Função necessária: administrador

Procedimento

1. Navegue até **Todos** > **Cliente de SCIM** > **Mapeamento de recursos do provedor de SCIM**.

   O Mapeamento de recursos do Provedor de SCIM é enviado com o mapeamento de Usuário e Grupo por padrão.

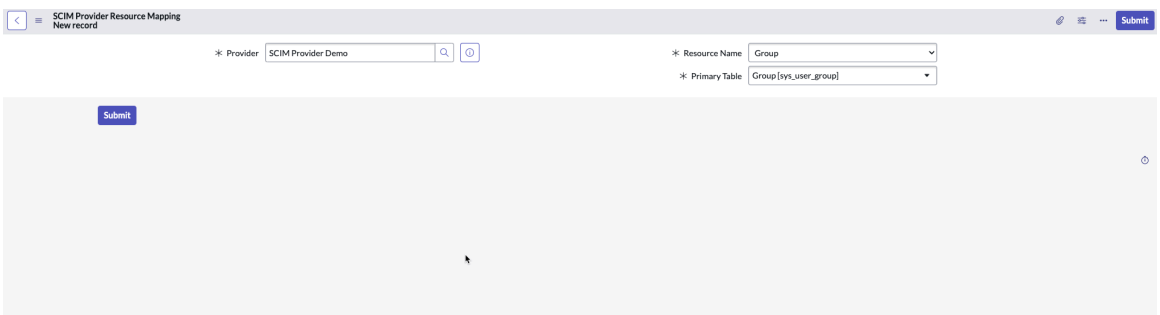
   Nota: Os mapeamentos de Usuário ou Grupo contêm mapeamentos de amostra, que você pode usar como referência. Você também pode criar mapeamento com base nos recursos do usuário ou do grupo.



2. Crie um mapeamento de recursos clicando em **Novo**.
3. No formulário, preencha os campos.

Mapeamento de recursos

Campos	Descrição
Provedor	Nome do Provedor de SCIM. Consulte o nome do Provedor configurado ao criar um Provedor de SCIM.
Nome do recurso	Recurso para o qual o mapeamento deve ser definido.
Tabela Primária	A tabela que contém o sys_id do recurso que está sendo mapeado.



4. Clique em **Enviar**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resultados

O registro é criado e exibido na página Mapeamento de recursos do Provedor de SCIM. Use os Mapeamentos de atributo SCIM para mapear ainda mais os atributos de esquemas. Para obter mais informações, consulte Criar um mapeamento do atributo SCIM.

Criar um mapeamento do atributo SCIM

Crie um mapeamento de atributo SCIM e use-o como uma fonte única de recurso para os campos da tabela da ServiceNow.

Antes de Iniciar

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

A seguir estão os tipos de mapeamento de atributo e suas descrições.

Tipos de mapeamentos de atributo

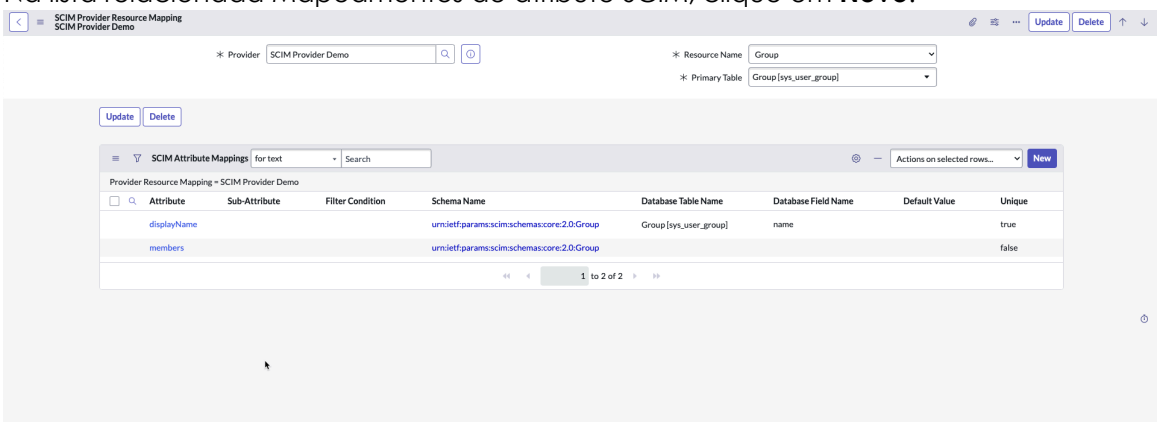
Tipo de mapeamento de atributo	Descrição
Direto	O atributo SCIM é preenchido com a ajuda dos campos **Nome da tabela do banco de dados** e **Nome do campo do banco de dados**.
Constante	O atributo SCIM é preenchido com a ajuda de um valor padrão especificado.
Script/personalização	O atributo SCIM é preenchido com a ajuda do valor de retorno de um script. Este atributo requer a habilitação da opção de executar script.

Nota:

- O atributo de senha não é compatível
- Um exemplo de mapeamento de atributo para os recursos de Usuário e Grupo faz parte do sistema de base. Você pode usar e configurar os mapeamentos com base em seus requisitos ou pode criar um novo registro.

Procedimento

1. Navegue até **Todos** > **Cliente de SCIM** > **Mapeamento de recursos do Provedor de SCIM**.
2. Selecione o Mapeamento de recursos de SCIM que é criado para a configuração.
3. Na lista relacionada Mapeamentos de atributo SCIM, clique em **Novo**.



© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. No formulário, preencha os campos.

Formulário de Mapeamentos de atributos SCIM

Campos	Descrição
Mapeamento dos recursos do provedor	Mapeamento de atributos para uma combinação de provedor-recurso. Se este campo não for preenchido automaticamente, use a opção de pesquisa. Selecione o registro Mapeamento de recursos do provedor.
Nome de Esquema	Nome do esquema do atributo SCIM para o qual o mapeamento deve ser definido. Por exemplo, *urn:ietf:params:scim:schemas:core:2.0:User*.
Atributo	Atributo para o qual o mapeamento deve ser definido. Por exemplo, *userName*.
Subatributo	Subatributo (se houver) para o qual o mapeamento deve ser definido. Por exemplo, se houver um atributo de tipo complexo como *name.familyName*, o atributo será o **nome** e o subatributo será **sobrenome**.
Tipo de Campo	O tipo de dados do atributo SCIM. Este campo é preenchido automaticamente a partir dos esquemas definidos pelo Provedor de SCIM. Por exemplo, **booliano**.
Valores múltiplos	Valores múltiplos que são atribuídos ao atributo. Um atributo pode ter valores múltiplos, como e-mail comercial, e-mail residencial ou outro e-mail. Por exemplo, *emails*. Este campo é preenchido usando os esquemas definidos pelo provedor de SCIM.
Condição do filtro	Alguns atributos de valores múltiplos podem ter informações adicionais que podem ser especificadas usando uma

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campos	Descrição
	Condição do filtro. As opções de condição do filtro são preenchidas usando os esquemas definidos pelo Provedor de SCIM. Por exemplo, o atributo *phoneNumbers* tem vários tipos, como trabalho, para celular, casa e assim por diante
Exclusivo	Opção para identificar exclusivamente um recurso entre os sistemas do Cliente de SCIM e do Provedor de SCIM. Atributos de valores múltiplos não podem ser marcados como exclusivos. Por exemplo, para um Recurso do usuário, o atributo *username* pode se tornar exclusivo.
Nome da tabela do banco de dados	Use este campo para mapear o nome da tabela de atributos para o nome da tabela da ServiceNow. Se escolher o mapeamento de atributo direto, você deverá definir este campo. Por exemplo, o *username*Atributo SCIM pode ser mapeado para o campo **Usuário** no campo **Nome da tabela do banco de dados**.
Nome do campo do banco de dados	O campo Nome do campo de banco de dados mapeia o atributo SCIM para o nome do campo da ServiceNow a ser mapeado com o atributo SCIM. Se escolher o mapeamento de atributo direto, você deverá definir este campo. Por exemplo, o *username*Atributo SCIM pode ser mapeado para o campo **ID do Usuário** no campo **Nome do campo do banco de dados**.
Valor Padrão	Detalhes sobre o valor padrão que é passado para o Provedor de SCIM. Pode ser usado se o mapeamento de atributo direto do campo retornar nulo ou se o padrão puder ser usado para retornar um valor codificado. No caso de um valor codificado, o nome da tabela de banco de dados e o nome do campo devem ser **Nenhum**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campos	Descrição
	Por exemplo, o valor do subatributo primário do e-mail comercial pode ser codificado como **verdadeiro**.
Executar script	Opção para buscar o valor do atributo via script. Esta opção é necessária para os atributos de valores múltiplos que não contêm uma condição do filtro. Para um tipo complexo de atributo, um script pode fornecer o valor em um nível de atributo ou subatributo. Por exemplo, o atributo **Membros** do recurso de grupo não tem condição do filtro. Portanto, a opção de script deve ser definida no nível de atributo primário do atributo **Membros**.
Script	Script usado para buscar o valor do atributo. O tipo de retorno do script deve ser uma cadeia de caracteres ou um JSON convertido como cadeia de caracteres. A saída do script deve estar no formato apropriado conforme esperado pelo provedor para esse atributo.

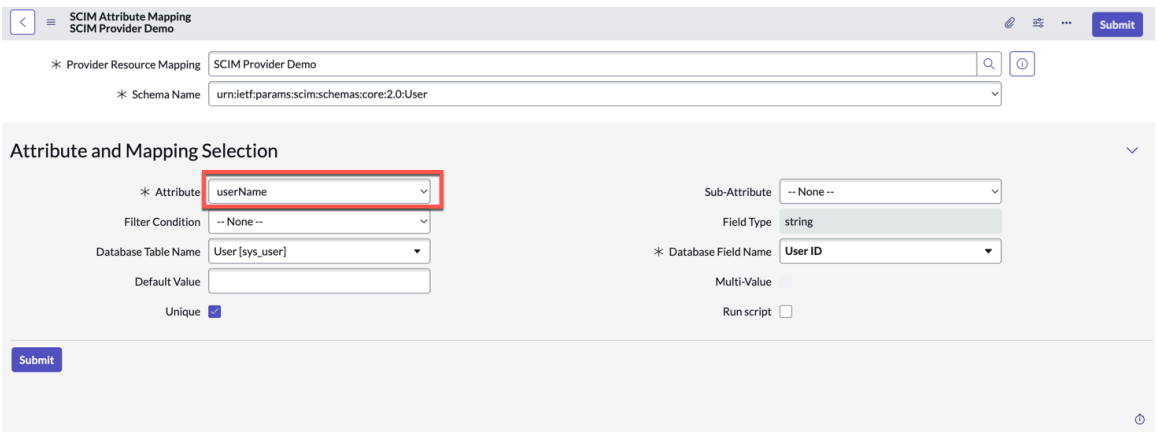
5. Clique em **Enviar**.

Referências de mapeamento de atributos

Os mapeamentos de atributo permitem que você use os atributos como uma única fonte de recurso para os campos da tabela da ServiceNow.

Atributo

O atributo para o qual o mapeamento deve ser definido. Por exemplo, *userName*.



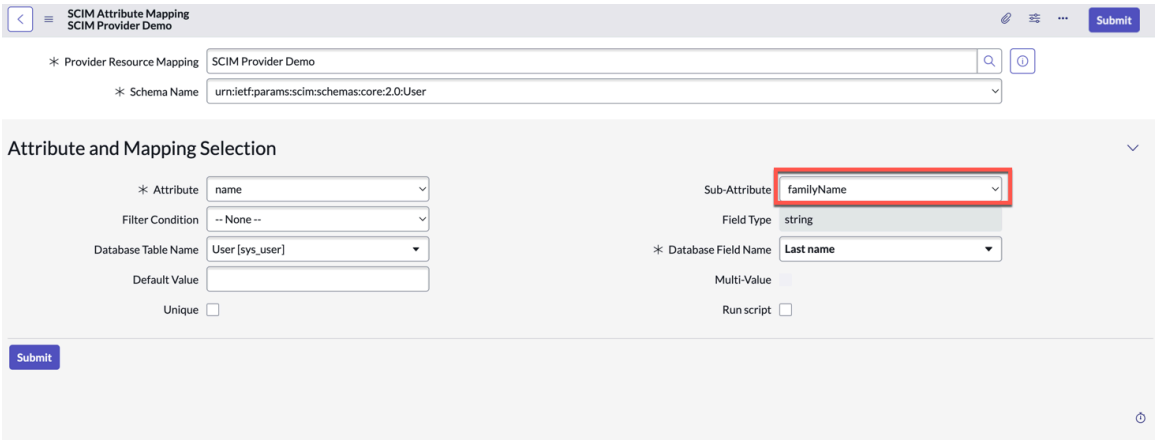
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Subatributo

Selecione o subatributo, se houver, para o qual um mapeamento precisa ser definido.

Por exemplo, se houver um atributo de tipo complexo como *name.familyName*, o atributo será *name* e o subatributo será *familyName*.

Para atributos simples, como nome de usuário, o valor do **Subatributo** seria **Nenhum**.

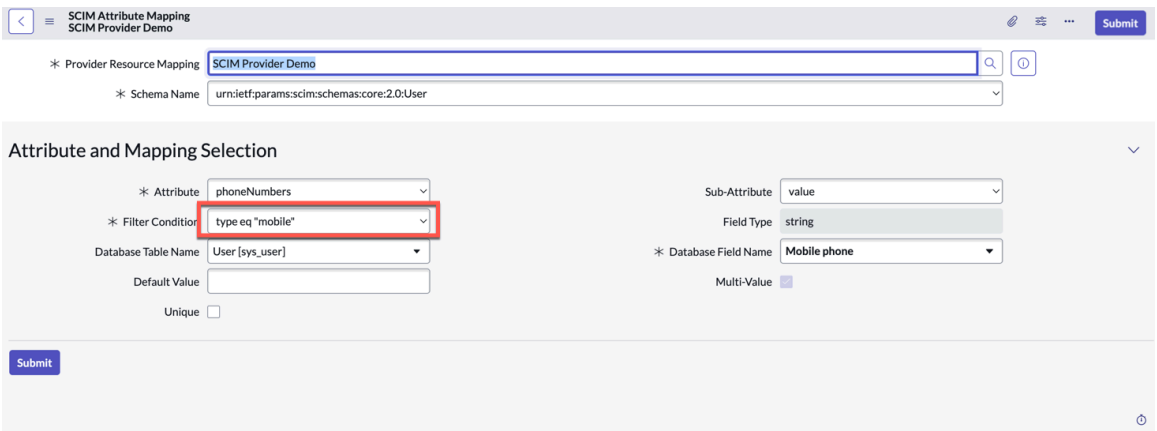


Condição do Filtro

Um atributo de valores múltiplos pode ter informações adicionais que podem ser especificadas usando uma condição do filtro. As opções para a condição do filtro são preenchidas usando os esquemas definidos pelo Provedor de SCIM.

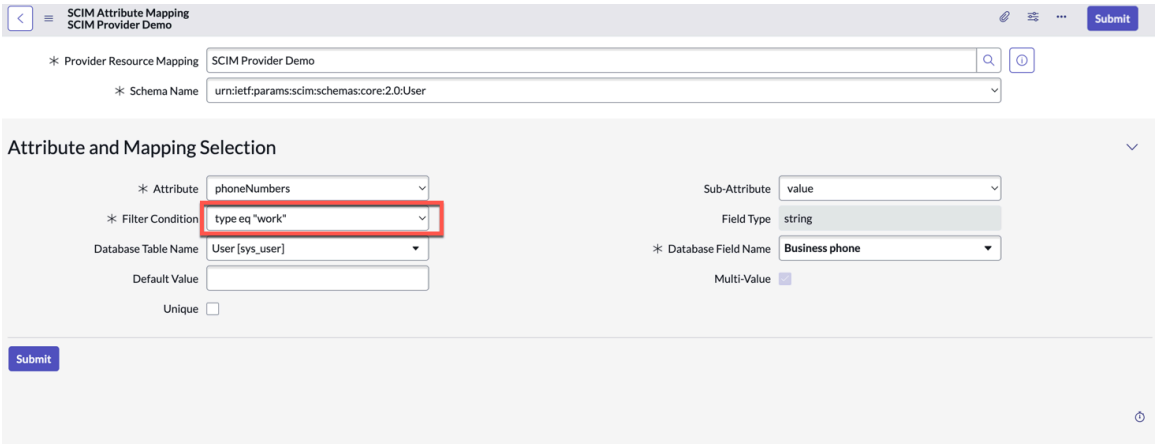
Por exemplo, o atributo *phoneNumbers* tem vários tipos, como trabalho, para celular, casa e assim por diante.

Você pode especificar uma condição do filtro dentre um conjunto de valores possíveis. Por exemplo, o atributo *phoneNumber* pode ter a condição do filtro como **type eq "mobile"**.



Em vez disso, o atributo *phoneNumber* pode ter uma Condição do filtro como **type eq "work"**.

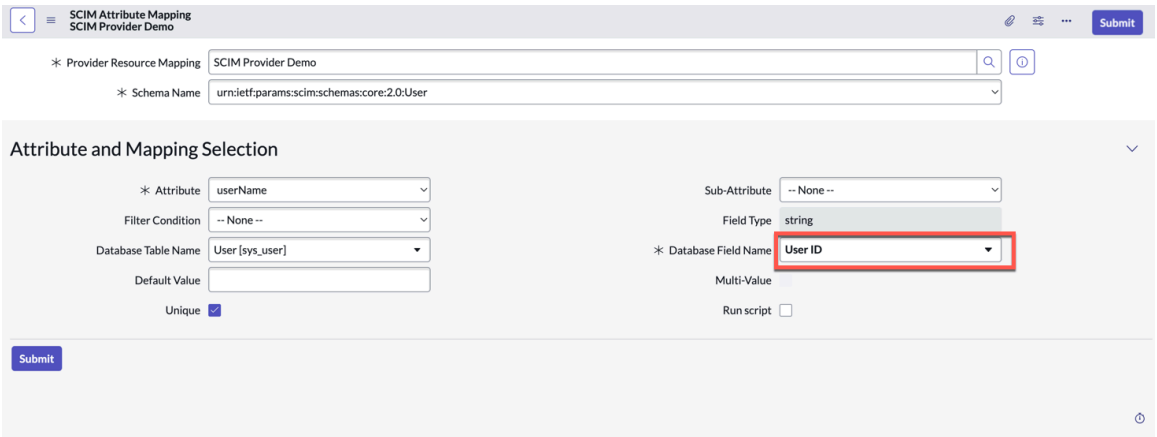
© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



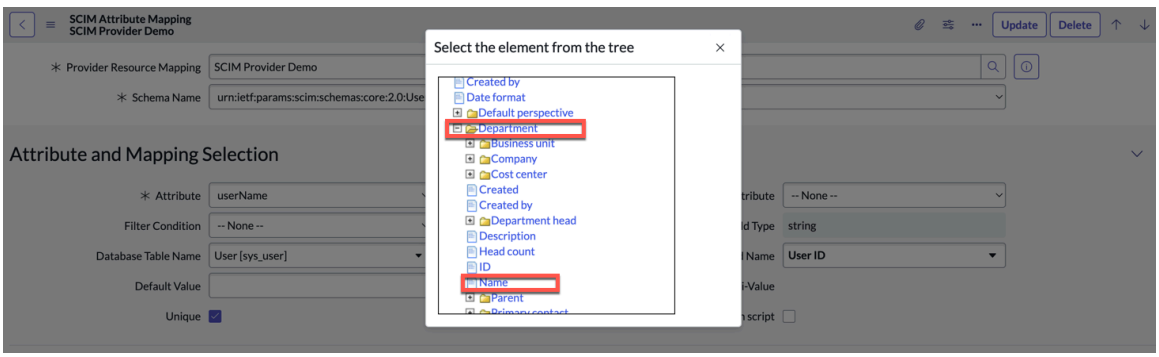
Nome do campo do banco de dados

Se a opção de mapeamento de atributo direto for escolhida, este atributo precisará ser definido. O campo **Nome do campo do banco de dados** representa o nome do campo da ServiceNow que é mapeado com o atributo SCIM.

Por exemplo, o atributo SCIM *`username`* pode ser mapeado para um usuário como o campo **Nome da tabela do banco de dados** e para o campo ID do usuário como o campo **Nome do campo do banco de dados**.

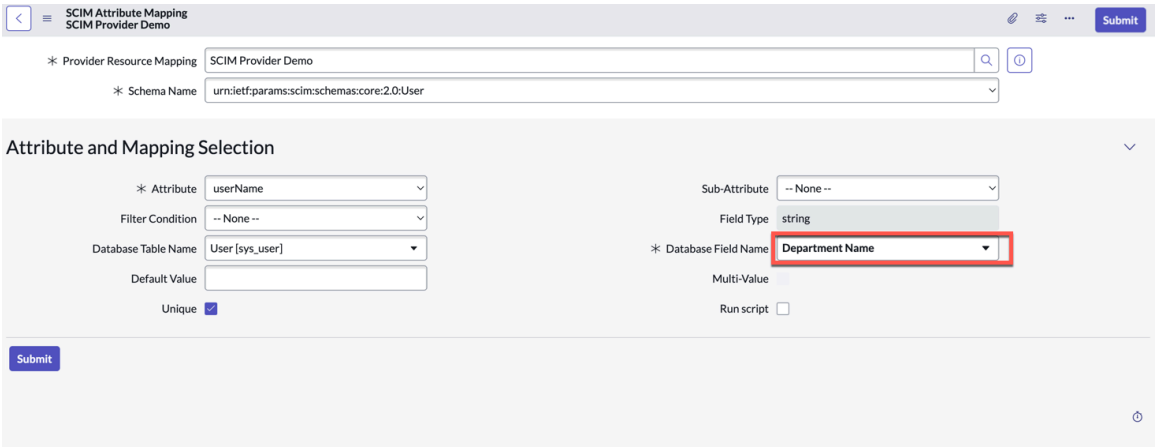


Você também pode fazer referência com pontos usando o **Nome do campo de banco de dados**. Por exemplo, o atributo SCIM **departamento** pode ser mapeado para o campo **Nome do departamento**.



Aqui, a tabela do banco de dados é **Usuário** e o Nome do campo do banco de dados é **Nome do departamento**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

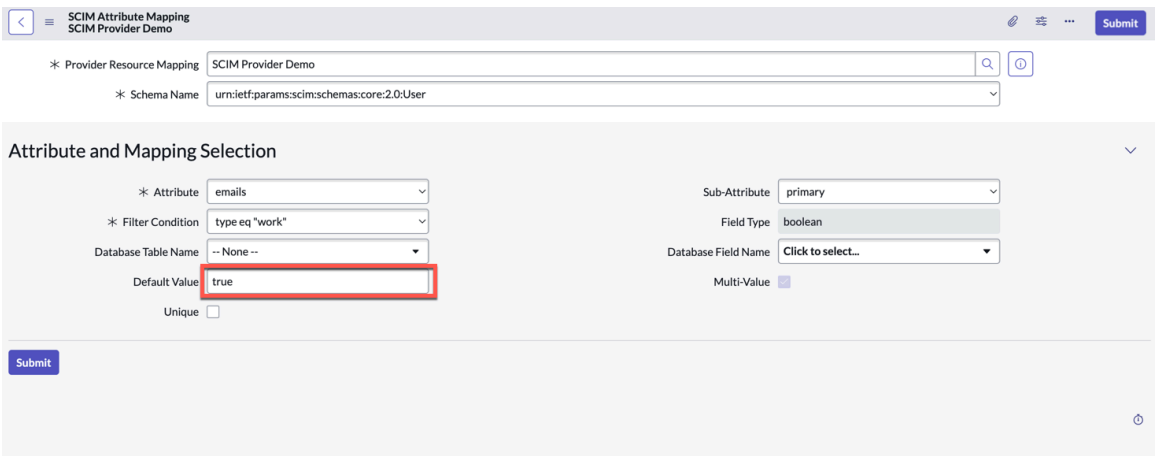


Valor Padrão

O valor padrão será passado para o Provedor de SCIM se o mapeamento de atributo direto desse campo retornar nulo. O valor padrão também pode ser usado para retornar um valor codificado.

No caso de um valor codificado, o nome da tabela de banco de dados e o nome do campo devem ser **Nenhum**.

Por exemplo, o valor do subatributo principal do e-mail de trabalho pode ser codificado como **verdadeiro**.

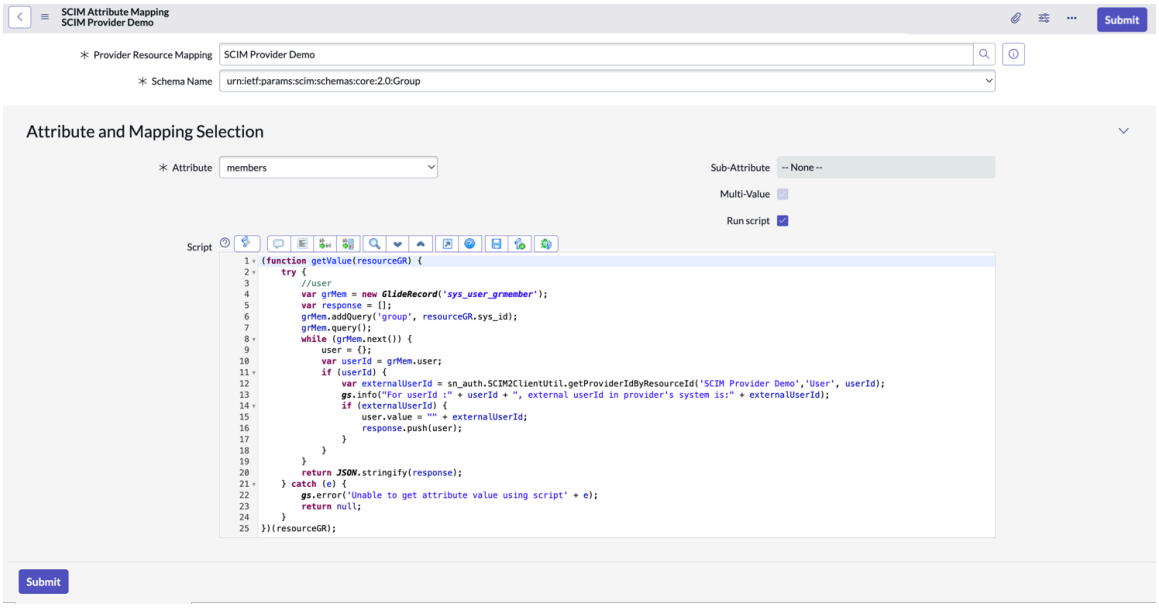


Script

O script é usado para buscar o valor do atributo. O tipo de retorno do script deve ser sempre uma cadeia de caracteres ou um JSON convertido como uma cadeia de caracteres. A saída do script deve estar no formato apropriado conforme esperado pelo provedor para esse atributo.

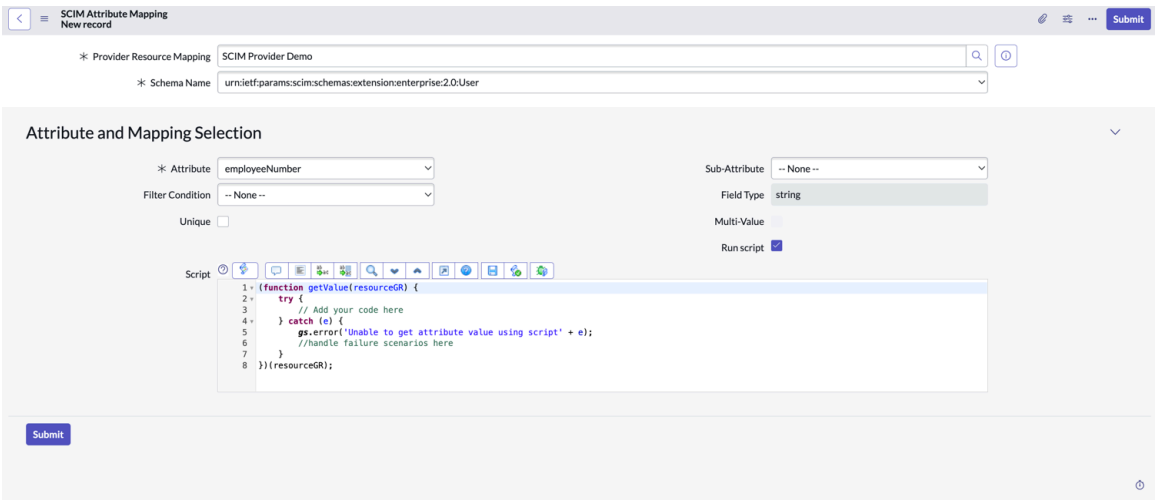
A seguir está um script de exemplo para um atributo de valores múltiplos.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



A saída do script deve ter uma matriz JSON em cadeia de caracteres.

A seguir está um script de exemplo de um atributo de valor simples.



A saída do script deve ser uma cadeia de caracteres.

Solução de problemas do Cliente de SCIM

As ações de solução de problemas podem ajudar a resolver problemas comuns ao configurar ou executar o Cliente de SCIM.

Solução de problemas

Problema	Ação
A resposta contém a seguinte mensagem: `"message":"Unable to access the table core_company with id: 0c441abbc6112275000025157c651c89, Please cross check the Access control rules"`	A mensagem será exibida se a API for chamada em um contexto de usuário e o usuário não tiver acesso à tabela. Você deve certificar-se de que a API passível de script seja chamada no contexto do sistema.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Solução de problemas

Problema	Ação
A resposta contém a seguinte mensagem: `{"message":"User Not Authenticated","detail":"Required to provide Auth information”}`	• Certifique-se de que o token seja gerado por meio da mensagem REST correspondente e que seja válido. • Certifique-se de que a API passível de script seja chamada no contexto do sistema.
A resposta contém a seguinte mensagem: `Script execution failed, the reason is: Cannot cast java.lang.Integer to java.lang.String`	No mapeamento de atributo SCIM, se o campo for definido para buscar de um script com esse problema, certifique-se de que o tipo de retorno seja sempre uma cadeia de caracteres.
A resposta contém a seguinte mensagem: `"status": "400", "scimType": "invalidValue", "detail": "Manager id : 02826bf03710200044e0bfc8bcbe5ds8 doesn't exist"`	Para qualquer atributo SCIM que espera o ID, esse ID é sempre do sistema do provedor. Certifique-se de que o ID transmitido na carga seja válido no sistema do provedor.

Áreas para verificar a solução de problemas

A seguir estão algumas das áreas que podem ser verificadas quanto a erros na solução de problemas ao usar o Cliente de SCIM:

- Se for encontrado algum problema ao executar qualquer uma das APIs passíveis de script, consulte a seção de registros em log do Cliente de SCIM.

Campos de registros em log

Campo	Descrição
ID de Solicitação	ID exclusivo que representa uma API passível de script chamada.
Provedor de SCIM	Nome do provedor para o qual a API é chamada.
Recurso	Nome do recurso para o qual a API é chamada.
ID do recurso	O ID para o qual a API é chamada. Para exclusão, o ID representa o ID do recurso no sistema do provedor e o ID está no sistema do cliente.
Ação	API que é chamada
Status	Status do registro em log como um sucesso ou falha

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Mensagem	Mensagem de sucesso ou erro A mensagem de erro pode ser do provedor de SCIM ou devido a problemas de configuração no Cliente de SCIM.

- Verifique o corpo da solicitação configurando e exibindo as chamadas de saída. Para saber mais, consulte Registro em log de serviço web de saída.
- Atualize os níveis de registro em log adicionando o tipo de conteúdo, testando a amostra e navegando para o formulário de método HTTP correspondente na mensagem REST do provedor correspondente.
- Se o corpo da solicitação estiver truncado, aumente o limite usando a propriedade do sistema *glide.outbound_http.content.max_limit*.

Auditoria de identidade e acesso

Use a Auditoria de identidade e acesso para entender as mudanças feitas para usuários, grupos, funções e ACLs.

Explorar

Conheça os recursos e o valor comercial da Auditoria de identidade e acesso.

Configurar

Entenda como configurar a Auditoria de identidade e acesso.

Avaliação

Exiba os resultados da Auditoria de identidade e acesso.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Explorar Auditoria de identidade e acesso

Use a Auditoria de identidade e acesso para entender as mudanças feitas para usuários, grupos, funções e ACLs.

A auditoria de identidade e acesso ajuda a entender as informações críticas sobre quem modificou o quê, onde e quando em relação às contas de usuário, grupos e funções.

Ajuda a detectar usuários mal-intencionados, rastrear atividades incomuns na instância ServiceNow® e cumprir os padrões de conformidade de capacidade de rastrear mudanças de acesso.

A Auditoria de identidade e acesso (Identity Security Audit) é um plug-in (`com.glide.security.audit`) que é instalado automaticamente.

O recurso de Auditoria pode ser ativado ou desativado alternando a propriedade do sistema`glide.identity.security.audit.enabled`. Por padrão, a propriedade está definida como `verdadeira`.

A Auditoria de identidade e acesso permite que você:

- Exiba as mudanças feitas nos últimos 30 dias em usuários, grupos, atributos das ACLs de função, associações de função, associações de grupo e funções das ACLs.
- Rastreie as mudanças em sua instância ServiceNow.
- Ajude a mitigar possíveis riscos regulatórios e de segurança.
- Demonstre conformidade com auditores de diferentes grupos na organização.
- Demonstre que a organização não está vulnerável a ameaças relacionadas à falta de visibilidade no grupo de usuários e mudanças de função.

Personas do usuário na Auditoria de identidade e acesso

A seguir estão as diferentes personas de usuário na Auditoria de identidade e acesso:

- **Administrador**: exibe os registros de auditoria e a configuração.
- **Administrador de segurança**: exibe estas trilhas de auditoria. Modifique a configuração para habilitar ou desabilitar a auditoria de uma determinada tabela ou mudar os campos auditados.

Tabelas de auditoria

As tabelas a seguir podem ser auditadas usando a Auditoria de identidade e acesso:

- Grupo [sys_user_group]
- Função [sys_user_role]
- Controle de acesso [sys_security_acl]
- Usuário [sys_user]
- Função do grupo [sys_group_has_role]
- Função do usuário [sys_user_has_role]
- Funções de acesso [sys_security_acl_role]
- Função contida [sys_user_role_contains]
- Membro do grupo [sys_user_grmember]

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Módulos da Auditoria de identidade e acesso

A Auditoria de identidade e acesso contém os seguintes módulos na instância ServiceNow:

Módulo	Descrição
Resultados de Auditoria	Exibe as auditorias ocorridas na instância ServiceNow.
Configurar tabelas e campos	Configure as tabelas e os campos do sistema com os campos disponíveis da Auditoria de identidade e acesso.
Configurar período de retenção	Configure o período de retenção dos dados auditados. O período máximo que pode ser definido é de 30 dias.
Trilhas de usuários	Exibe auditorias de usuários.
Trilhas de grupos	Exibe auditorias de grupos.
Trilhas de funções	Exibe auditorias de funções.
Trilhas de ACL	Exibe auditorias de ACL.

Resultados da auditoria de identidade

Exibe auditorias ocorridas na instância ServiceNow®.

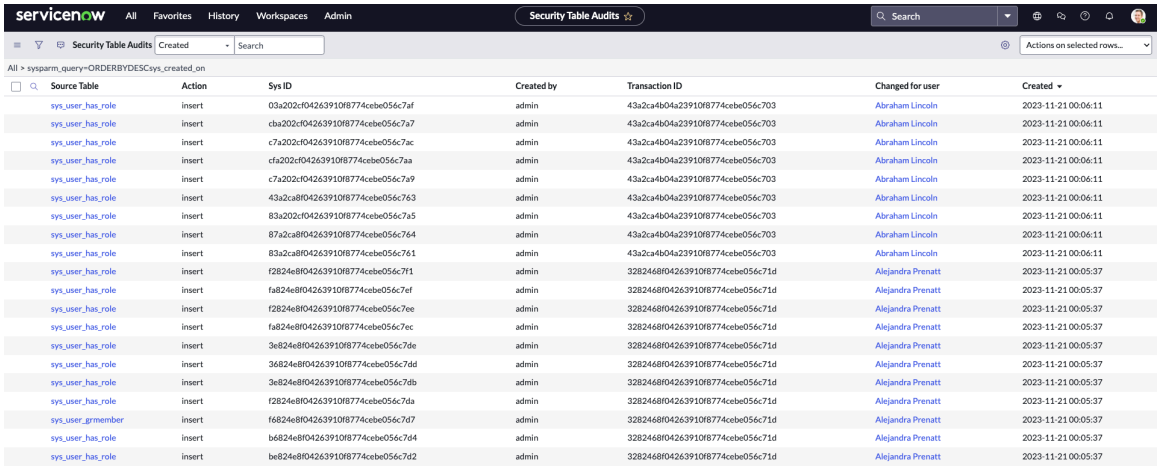
Os Resultados de auditoria exibem as mudanças feitas em usuários, grupos, funções e ACLs na instância ServiceNow.

Para acessar os Resultados de auditoria, navegue até **Todos** > **Segurança do sistema** > **Auditoria de identidade e acesso** > **Resultados de auditoria**. A página Auditorias da tabela de segurança será exibida com as seguintes informações.

Auditorias da tabela de segurança

Nome da Coluna	Descrição
Tabela de origem	Detalhes da tabela de origem em que a auditoria ocorreu.
Ação	Descreve a ação de auditoria.
Sys_id	Detalhes sobre o sys_id do registro auditado.
Criado por	Detalhes de quem criou a auditoria.
ID de Transação	Uma ID exclusiva que representa todas as ações na auditoria específica realizada.
Alterado para usuário	Nome do usuário quando a auditoria foi realizada.
Criado em	A data e a hora em que a auditoria foi realizada.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Trilhas de usuários

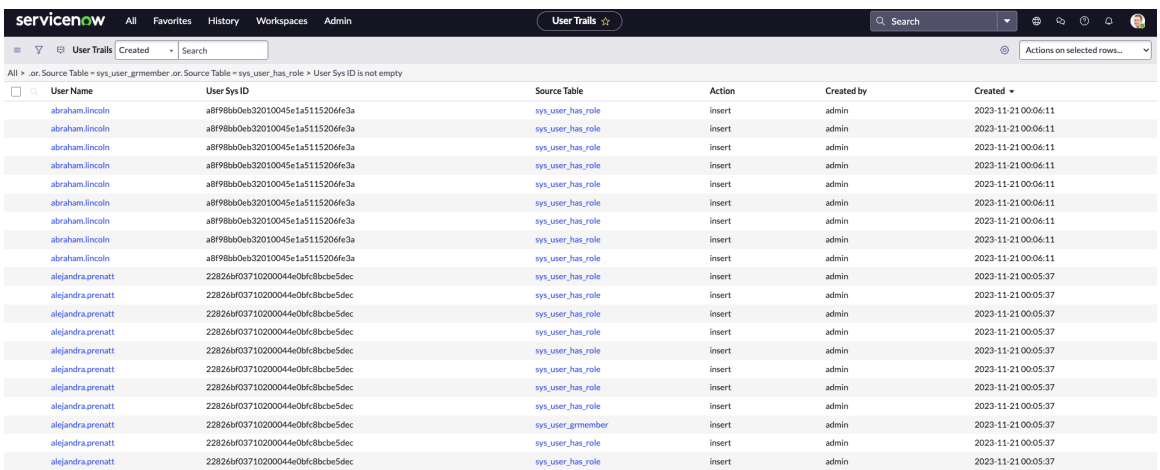
Exibe auditorias de usuários na instância ServiceNow®.

As Trilhas de usuários exibem mudanças de atributo de identidade, mudanças de associação de função e mudanças de associação de grupo de um usuário.

Para acessar as Trilhas do usuário, navegue até **Todos** > **Segurança do sistema** > **Auditoria de identidade e acesso** > **Trilhas de usuários**. A página Trilhas de usuários será exibida com as seguintes informações.

Trilhas de usuários

Nome de usuário	Nome do usuário.
ID do sistema do usuário	Detalhes sobre o sys_id do usuário para o registro auditado.
Tabela de origem	Detalhes sobre a tabela de origem em que a auditoria foi realizada.
Ação	Descreve a ação de auditoria.
Criado Por	O usuário que fez a mudança.
Criado em	A data e a hora em que a auditoria foi realizada.



© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Trilhas de grupos

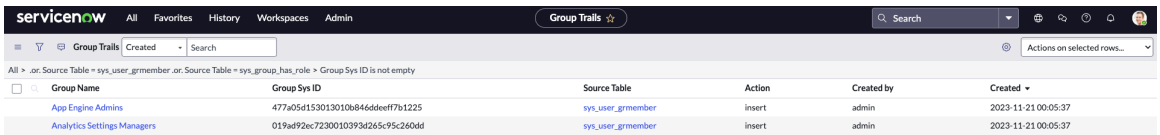
Exibe auditorias de grupos na instância ServiceNow®.

Trilhas de grupos exibem mudanças de atributo, mudanças de associação e mudanças de funções de um grupo.

Para acessar as Trilhas de grupos, navegue até **Todos** > **Segurança do sistema** > **Auditoria de identidade e acesso** > **Trilhas de grupos**. A página Trilhas de grupos será exibida com as seguintes informações.

Trilhas de grupos

Nome do grupo	Nome do grupo.
ID do sistema do grupo	Detalhes sobre o sys_id do grupo para o registro auditado.
Tabela de origem	Detalhes sobre a tabela de origem em que a auditoria foi realizada.
Ação	Descreve a ação de auditoria.
Criado Por	O usuário que fez a mudança.
Criado em	A data e a hora em que a auditoria foi realizada.



Trilhas de funções

Exibe auditorias de funções na instância ServiceNow®.

As Trilhas de funções exibem mudanças de atributo e de relação primária-secundária de uma função.

Para acessar as Trilhas de funções, navegue até **Todos** > **Segurança do sistema** > **Auditoria de identidade e acesso** > **Trilhas de funções**. A página Trilhas de funções será exibida com as seguintes informações.

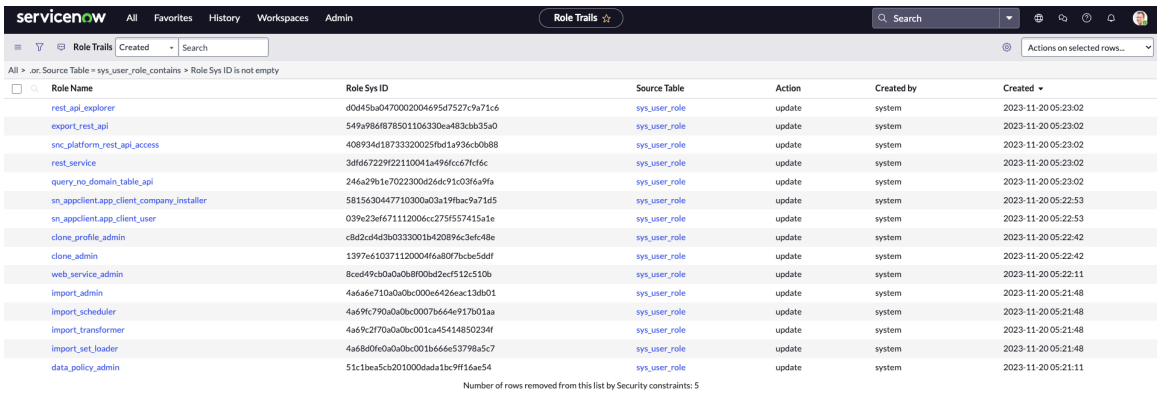
Trilhas de funções

Nome da função	Nome da função.
ID do sistema de função	Detalhes sobre a função sys_id do registro auditado.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Trilhas de funções

Tabela de origem	Detalhes sobre a tabela de origem em que a auditoria foi realizada.
Ação	Descreve a ação de auditoria.
Criado Por	O usuário que fez a mudança.
Criado em	A data e a hora em que a auditoria foi realizada.



Trilhas de ACL

Exibe auditorias de ACLs na instância ServiceNow®.

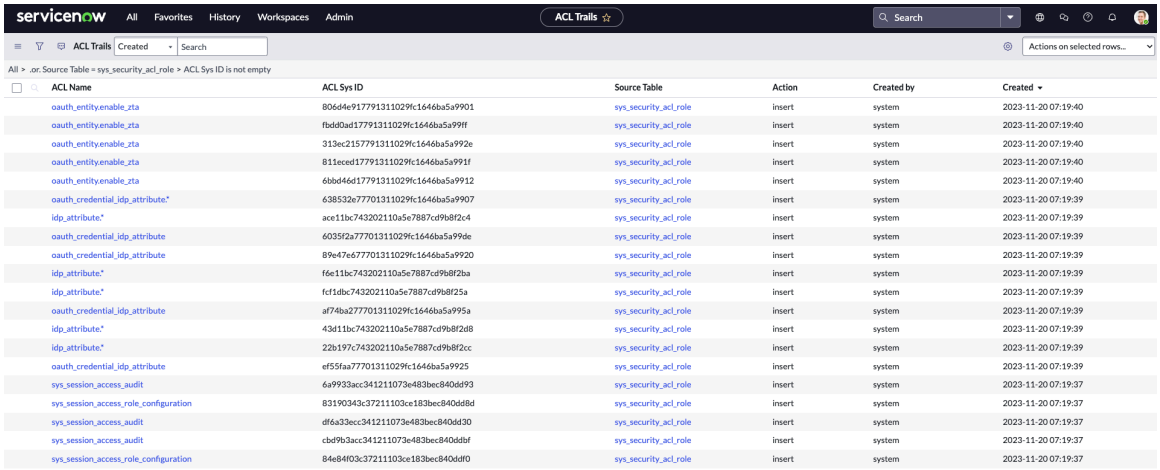
As trilhas de ACL exibem mudanças de atributo e mudanças de relação de função necessárias para uma ACL.

Para acessar as Trilhas de ACL, navegue até **Todos** > **Segurança do sistema** > **Auditoria de identidade e acesso** > **Trilhas de ACL**. A página Trilhas de ACL será exibida com as seguintes informações.

Trilhas de ACL

Nome da ACL	O nome da ACL.
Sys id da ACL	Detalhes sobre o sys_id da ACL para o registro auditado.
Tabela de origem	Detalhes sobre a tabela de origem em que a auditoria foi realizada.
Ação	Descreve a ação de auditoria.
Criado Por	O usuário que fez a mudança.
Criado em	A data e a hora em que a auditoria foi realizada.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Campos auditáveis de segurança

Exibe detalhes em nível de tabela e campo que serão auditados na instância ServiceNow®.

Campos auditáveis de segurança exibe os detalhes das tabelas e dos campos que serão auditados na instância ServiceNow.

Para acessar a página Campos auditáveis de segurança, navegue até **Todos** > **Segurança do sistema** > **Auditoria de identidade e acesso** > **Configurar tabelas e campos**. A página Campos auditáveis de segurança será exibida com as seguintes informações.

Campos auditáveis de segurança

Nome da Coluna	Descrição
Tabela para auditoria	Detalhes da tabela auditada.
Destino do armazenamento de auditoria	Detalhes do destino em que os detalhes da auditoria são armazenados.
Lista de Campos	A auditoria será feita para os campos especificados na lista.
Criar	Audite as mudanças relacionadas à operação Criar.
Atualizar	Audite as mudanças relacionadas à operação Atualizar.
Excluir	Audite as mudanças relacionadas à operação Excluir.
Ativo	Audite somente se a configuração da tabela estiver ativa.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

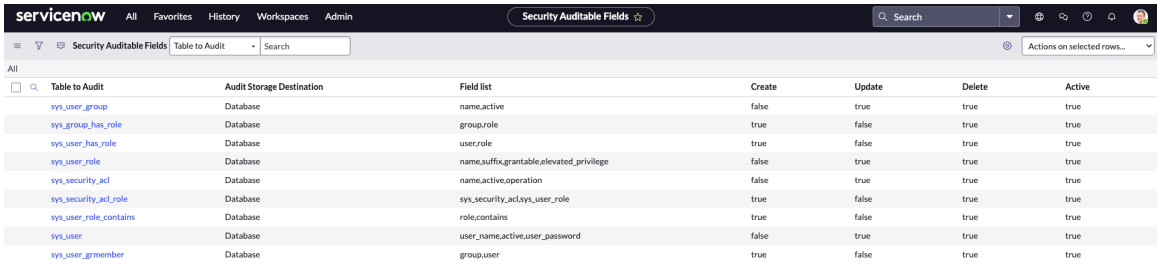


Table to Audit	Audit Storage Destination	Field list	Create	Update	Delete	Active
sys_user_group	Database	name,active	false	true	true	true
sys_group_has_role	Database	group,role	true	false	true	true
sys_user_has_role	Database	user,role	true	false	true	true
sys_user_role	Database	name,suffix,grantable,elevated_privilege	false	true	true	true
sys_security_acl	Database	name,active,operation	false	true	true	true
sys_security_acl_role	Database	sys_security_acl,sys_user_role	true	false	true	true
sys_user_role_contains	Database	role,contains	true	false	true	true
sys_user	Database	user_name,active,user_password	false	true	true	true
sys_user_grmember	Database	group,user	true	false	true	true

As seguintes tabelas podem ser auditadas usando a Auditoria de identidade e acesso:

- Grupo [sys_user_group]
- Função [sys_user_role]
- Controle de acesso [sys_security_acl]
- Usuário [sys_user]
- Função do grupo [sys_group_has_role]
- Função do usuário [sys_user_has_role]
- Funções de acesso [sys_security_acl_role]
- Função contida [sys_user_role_contains]
- Membro do grupo [sys_user_grmember]

Configurar tabelas e campos

Use a Auditoria de identidade e acesso para entender as mudanças feitas para um usuário, grupo, função e ACL.

Antes de Iniciar

Função necessária: security_admin

Você deve promover sua função a administrador de segurança para configurar tabelas e campos para a Auditoria de identidade e acesso.

As seguintes tabelas podem ser configuradas para auditoria:

- Grupo [sys_user_group]
- Função [sys_user_role]
- Controle de acesso [sys_security_acl]
- Usuário [sys_user]
- Função do grupo [sys_group_has_role]
- Função do usuário [sys_user_has_role]
- Funções de acesso [sys_security_acl_role]
- Função contida [sys_user_role_contains]
- Membro do grupo [sys_user_grmember]

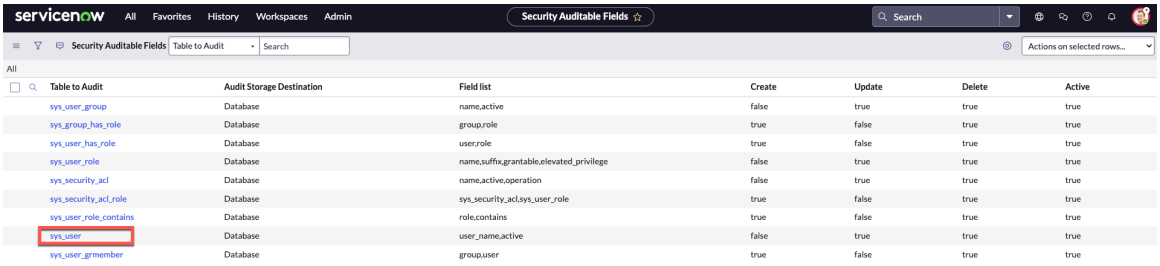
Nota: Para entender quais campos podem ser configurados para as tabelas, consulte Campos compatíveis e não compatíveis com Auditoria de identidade e acesso.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

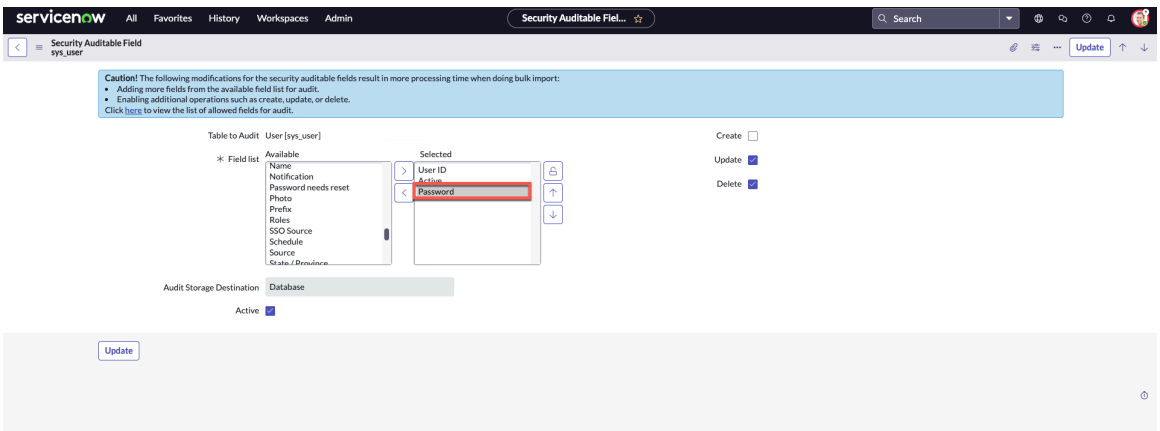
1. Navegue até **Todos** > **Segurança do sistema** > **Auditoria de identidade e acesso** > **Configurar tabelas e campos**.
2. Selecione a tabela cujo campo você deseja auditar.

   Por exemplo, **sys_user**.



3. Adicione o campo a ser auditado.

   Por exemplo, **Senha**.

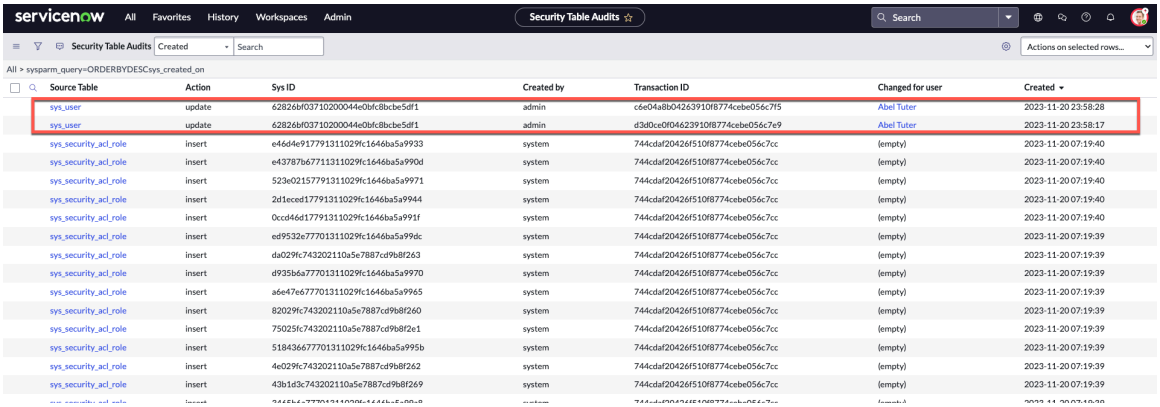


> **Nota:** As seguintes modificações nos campos auditáveis de segurança resultam em mais tempo de processamento ao realizar a importação em massa:
>
> - Como adicionar mais campos da lista de campos disponíveis para auditoria.
> - Como habilitar operações adicionais, como criar, atualizar ou excluir.

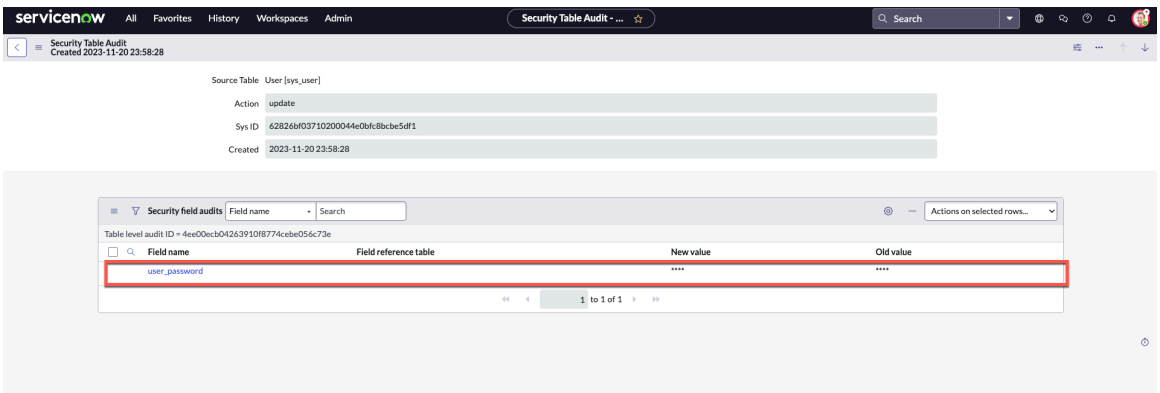
4. Atualize o registro.

   Quaisquer mudanças no campo de senha adicionam um novo registro às Auditorias da tabela de segurança. Neste exemplo, a auditoria exibe um campo de senha alterada para o usuário **Abel Tuter**.

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Selecionar o registro criado exibe os detalhes das mudanças.



Configurar período de retenção

Configure o período de retenção para a Auditoria de identidade e acesso.

Antes de Iniciar

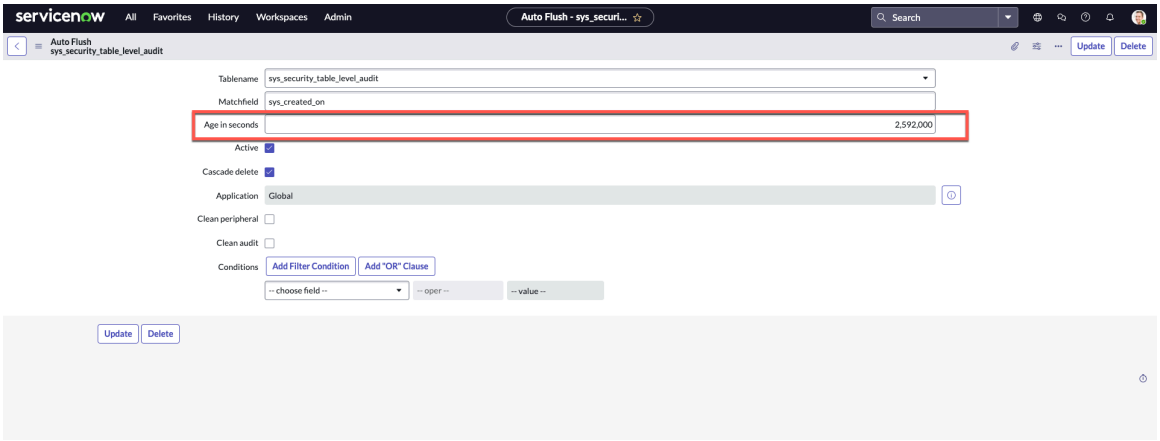
Função necessária: administrador

Procedimento

1. Navegue até **Todos** > **Segurança do sistema** > **Auditoria de identidade e acesso** > **Configurar período de retenção**.
2. No formulário, você pode mudar a Idade em segundos.

> **Nota:** O número máximo de dias para a Auditoria de identidade e acesso é de 30 dias (2.592.000 segundos).

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. Salve ou atualize o registro.

Campos compatíveis e não compatíveis com Auditoria de identidade e acesso

Lista de campos compatíveis e não compatíveis com a auditoria.

A validação de campos de auditoria evita que alguns campos sejam escolhidos em field_list na tabela Configuração de auditoria do campo de segurança (sys_sec_field_audit_config).

Campo compatível ou não com Auditoria

Tabela	Campos compatíveis ou não
Todas as tabelas	Campos que não são compatíveis: • Criado em (sys_created_on) • Criado por (sys_created_by) • Atualizado por (sys_updated_by) • Atualizado em (sys_updated_on)
O usuário tem a função (sys_user_has_role)	Campos que são compatíveis: • Usuário • Função • Herdados • Contagem
Usuário (sys_user)	Campos que não são compatíveis: • Último login (last_login) • Hora do último login (last_login_time) • Último dispositivo de login (last_login_device) • Habilitar autenticação multifator (enable_multifactor_authn)

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo compatível ou não com Auditoria

Tabela	Campos compatíveis ou não
	• Perspectiva padrão (default_perspective) • Integração de calendário (calendar_integration) • ID federado (federated_id) • A senha precisa ser redefinida (password_needs_reset) • Tentativas com falha (failed_attempts) • Última senha (last_password) • Servidor LDAP (ldap_server) • Bloqueado (locked_out) • Notificação (notification) • Funções (roles) • Domínio (sys_domain) • Caminho do domínio (sys_domain_path) • Formato de hora (time_format) • ID do usuário com hash (hashed_user_id) • Nome da classe (sys_class_name) • Contagem de modificações (sys_mod_count)

© 2024 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.