



チューリッヒのオペレーショナルテクノロジー管理

最終更新日: **2025年11月10日**

自動翻訳

これらの資料は、翻訳ソフトウェアを使用してお客様の便宜のために翻訳されています。正確な翻訳をご提供できるよう相当な努力を払っておりますが、いかなる自動翻訳も人間の翻訳者に代わることはなく、そのようなことは意図されておりません。翻訳は「現状のまま」提供されています。他言語への翻訳の的確性、信頼性または正確性については、明示または黙示を問わず、いかなる保証も行われません。翻訳ソフトには限界があるため、一部のコンテンツが正確に翻訳されていない場合があります。これらの資料の公用言語は英語です。翻訳の際に生じる相違または不一致は、コンプライアンスまたは履行の目的に関しては拘束力を有さず、法的効力はないものとします。

ここで示したいくつかの例と図は、説明の目的でのみ提供されています。ServiceNow 製品またはサービスへの実際の関連付けやつながりは意図されておらず、推測されるものではありません。

ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは米国および/またはその他の国における ServiceNow, Inc. の商標または登録商標です。その他の会社名および製品名は、それぞれの所有者の商標です。

下記の ServiceNow ウェブサイト利用規約をお読みください。 www.servicenow.com/terms-of-use.html

自動翻訳

本社
2225 Lawson Lane
Santa Clara, CA 95054
United States
(408) 501-8550

目次

オペレーショナルテクノロジー.....	5
オペレーショナルテクノロジー管理 ライセンスとサブスクリプション.....	7
OTM へのサブスクリプション.....	8
インストール ITOM SU ライセンス.....	8
OTM のサブスクリプション統計情報の表示.....	9
割り当てられたサブスクリプションユニットに対する OTM リソース使用状況の確認.....	10
OTM サブスクリプションで使用する CI 数の確認.....	11
OTM サブスクリプションユニットを利用する CI を表示する.....	13
OTM SU ライセンス参照.....	13
オペレーショナルテクノロジーマネージャー.....	17
探索.....	19
構成.....	22
統合.....	38
使用方法.....	120
参照.....	184
製造業プロセスマネージャー.....	192
探索.....	194
構成.....	196
使用方法.....	218
参照.....	246
オペレーショナルテクノロジー脆弱性対応.....	252
探索.....	253
構成.....	255
統合.....	266
使用方法.....	293
参照.....	302
オペレーショナルテクノロジーインシデント管理.....	306
探索.....	307
構成.....	310
使用方法.....	321
参照.....	334
オペレーショナルテクノロジー変更管理.....	337
探索.....	338
構成.....	340
使用方法.....	350
参照.....	364
オペレーショナルテクノロジーのナレッジ管理.....	366
探索.....	367
構成.....	367

使用方法..... 376

参照..... 383

オペレーショナルテクノロジー要求管理..... 386

探索..... 387

構成..... 388

使用方法..... 392

参照..... 393

..... 398

探索..... 400

構成..... 401

使用方法..... 402

産業用 ワークスペース..... 403

探索..... 404

構成..... 423

使用方法..... 444

ドメインセパレーションと OT..... 462

オペレーショナルテクノロジー

ServiceNow for オペレーショナルテクノロジーを使用すると、組織はデジタルワークフローを通じて運用を合理化し、生産性を向上させ、生産現場でのオペレーショナルテクノロジーアップタイムを最大化できます。

オペレーショナルテクノロジーの概要

オペレーショナルテクノロジーとServiceNow オペレーショナルテクノロジー管理ソリューションの概要をご覧ください。

https://player.vimeo.com/video/957122379?h=d9c04a0637&badge=0&autopause=0&player_id=0&app_id=58479

オペレーショナルテクノロジー、中核業務、工場労働者のエンパワメントにおけるメリット



Operational Technology

Contextualize and safeguard your Operational Technology systems, connect to digital workflows, and respond quickly to threats.



Core Operations

Streamline and digitize standard operating procedures (SOPs) and enable shared knowledge and collaboration across the enterprise.



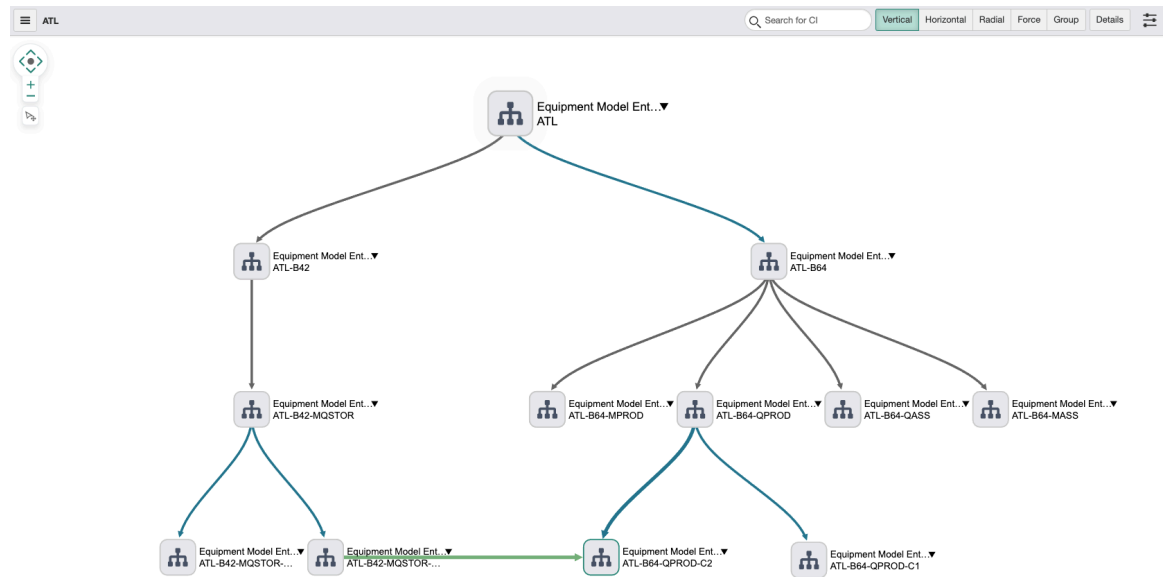
Factory Workers

Empower the workforce with digital tools and knowledge to adapt, collaborate, and excel in fast-changing conditions.

ServiceNow Operational Technology Management でアップタイムを最大化し、運用のレジリエンスを構築

インダストリーオペレーショナルテクノロジーが登場する前は、メーカーは環境を維持するために手動プロセスとレガシーナレッジに依存していました。彼らは、環境を完全に把握し、そのすべてを保護、監視、管理することが困難であることに気づきました。ServiceNow オペレーショナルテクノロジー管理ソリューションにより、産業組織はオペレーショナルテクノロジーシステムの完全なコンテキストビューを取得できるようになりました。このビューを使用すると、システムの安全性を維持し、稼働させ、本番プロセスやデジタルワークフローに接続できます。また、組織がイベントと脅威を評価し、優先順位を付け、対応できるようにすることもできます。

機器モデルの依存関係ビュー



デジタルマップを使用することで、組織は産業オペレーションのプロセス、システム、および関係をより詳細に可視化できます。このマップを使用すると、潜在的な本番環境への影響を簡単かつ迅速に管理および評価できます。

- i** 注: オペレーショナルテクノロジー管理ソリューションはNow Mobile[®] ではサポートされていません。

可視化の向上



オペレーショナルテクノロジーシステムの完全なコンテキストビューを取得して、システムの安全性と実行を維持します。

デジタルワークフロー



オペレーショナルテクノロジーシステムを本番プロセスとデジタルワークフローに接続します。

脆弱性管理



すべてを 1 か所で表示することで、イベントや脅威を評価し、優先順位を付け、対応することができます。

従業員への装備

ローコードおよびノーコードのアプリケーションをビルドして、従業員が共同モニタリング、拡張トラブルシューティング、問題解決、詳細な状況分析を実行できるようにします。

詳細については、[ソリューションの概要](#) を参照してください。

開始

- デモ [ナ](#) で機能のデモをご覧ください。
- オペレーショナルテクノロジーの要求方法と設定方法については、
 - [オペレーショナルテクノロジーマネージャー](#) の構成
 - [製造業プロセスマネージャー](#) の構成
 - [オペレーショナルテクノロジー脆弱性対応](#) の構成
 - [オペレーショナルテクノロジーインシデント管理](#) の構成
 - [オペレーショナルテクノロジー変更管理](#) の構成
 - [オペレーショナルテクノロジーのナレッジ管理](#) の構成
- オペレーショナルテクノロジー が共通サービスデータモデル (CSDM) テーブルを管理および使用する方法の詳細については、「[オペレーショナルテクノロジーテーブルと CSDM テーブル](#)」を参照してください。
- オペレーショナルテクノロジー の最新リリースの詳細については、次を参照してください。
[ServiceNow ストア - オペレーショナルテクノロジー リリースノート](#)。

アプリケーション

- [オペレーショナルテクノロジーマネージャー](#)
- [製造業プロセスマネージャー](#)
- [オペレーショナルテクノロジー脆弱性対応](#)
- [オペレーショナルテクノロジーインシデント管理](#)
- [オペレーショナルテクノロジー変更管理](#)
- [オペレーショナルテクノロジーのナレッジ管理](#)
- [オペレーショナルテクノロジー要求管理](#)
- [オペレーショナルテクノロジーの産業用ワークスペース](#)
- サービス管理: [IT Service Management](#)
- セキュリティ: [脆弱性対応](#)
- 可視化: [IT Operations Management \(ITOM\)](#)

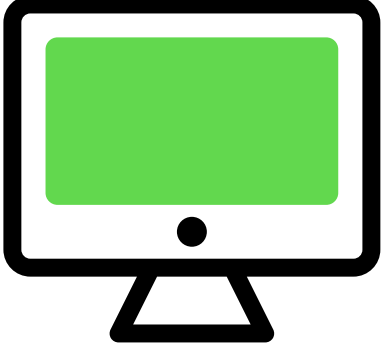
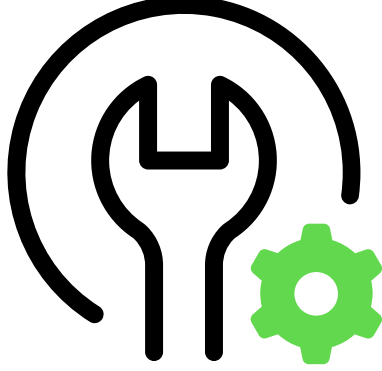
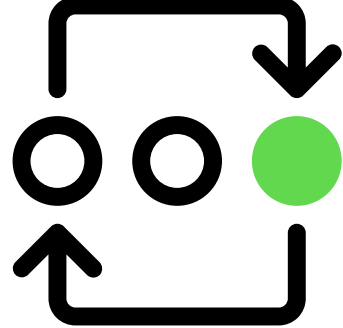
オペレーショナルテクノロジー管理 ライセンスとサブスクリプション

ServiceNow OTMライセンスは、監視対象のデバイスの数やサブスクリプションの期間などの要素を含むサブスクリプションユニットに基づいてOTMサブスクリプションの使用状況を計算して表示するため、オペレーショナルテクノロジー管理の重要な側面です。

オペレーショナルテクノロジー管理 ライセンスとサブスクリプションの概要

これにより、組織はコンプライアンスを確保し、リソースを効果的に割り当て、オペレーショナルテクノロジーシステムを保護し、変化するセキュリティと運用のニーズに適応するための OTM 機能の拡張について、情報に基づいた意思決定を行うことができます。OTMライセンスモジュールを使用して、OTM製品 (ServiceNow OT Foundation、ServiceNow OT ヴィジビリティ、ServiceNow OT 脆弱性に対応) のサブスクリプション関連の詳細にアクセスします。

開始

OTMライセンスの詳細	の ITOM SU ライセンスのインストール OTM	ライセンスの参照
 サブスクリプション関連の詳細について学習する	 プラグインの最新バージョンを更新する	 スケジュール済みジョブやテーブルなどのインストール済みコンポーネントについて把握します

サポートへの連絡

連絡先 [カスタマーサービス & サポート](#)

OTM へのサブスクリプション

ServiceNowプラットフォームでは、製造業のライセンス管理にOTMを採用しています。OTMには、IT Operations Management (ITOM)にあるライセンスと、OTMドメイン専用のライセンスが含まれます。

IT Operations Management (ITOM)ライセンスと同様の方法でOTMライセンスを監視します。ServiceNowインスタンス内でOTM、**ITOM** ライセンスカテゴリメタデータ (**OTM** ライセンス > **CI** タイプ別のライセンス) ページで、[**SKU** タイプ] 列に **otm** の値が表示されます。デフォルトでは、ライセンスフィルターは [**SKU** タイプ に otm を含む (SKU Type contains otm)] に設定されています。

インストール **ITOM SU** ライセンス

ServiceNow **ITOM SU** ライセンス [sn_itom_licensing] をインストールまたは更新して、最新のライセンス機能を確実に使用できるようにします。このアプリケーションには、デモデータが含まれています。まだインストールされていない場合は、関連する ServiceNow Store アプリケーションとプラグインをインストールします。

始める前に

- アプリケーションとその関連するすべての ServiceNow Store アプリケーションに有効な ServiceNow エンタイトルメントがあることを確認してください。詳細については、「」を参照してください。[のエンタイトルメントを取得 ServiceNow 製品またはアプリケーション](#)。
- 依存関係、ライセンスやサブスクリプションの要件、およびリリースの互換性については、ServiceNow Store の [ITOM SU ライセンス](#) アプリケーションリストを確認してください。

必要なロール：admin

このタスクについて

Q1 2022より前は、元のライセンスメカニズムはファミリーリリースの一部として提供されていました。それ以降は、ライセンスメカニズムは ServiceNow Store の ServiceNow ITOM SU ライセンスを使用して提供されます。ServiceNow ITOM SU ライセンスが自動的にインストールされます。このアプリケーションの更新が ServiceNow Store で利用可能になると、通知を受け取ります。

ITOM SU ライセンス とともに次のアイテムがインストールされます。

- スケジュール済みジョブ
- テーブル

詳細については、「[の ITOM SU ライセンスとともにインストールされるコンポーネント OTM](#)」を参照してください。

手順

1. 移動先 **すべて > システムアプリケーション > 利用可能なすべてのアプリケーション > すべて**。
2. フィルター基準と検索バーを使用して、アプリケーション (sn_itom_licensing) を検索します。

名前または ID でアプリケーションを検索できます。アプリケーションが見つからない場合は、ServiceNow Store へのリクエストが必要になることがあります。

[更新] ボタンの横のリストに、使用可能なバージョンが表示されます。

3. リストからバージョンを選択し、[更新] を選択します。

表示されるインストールダイアログには、アプリケーションとともにインストールされている依存関係が一覧表示されます。

4. プロンプトが表示された場合は、ServiceNow Store へのリンクに従って、依存関係のエンタイトルメントを取得します。
5. オプション: 利用できるデモデータをインストールするには、[デモデータのロード] チェックボックスをオンにします。
デモデータは、一般的なユースケース向けのアプリケーション機能を説明するサンプルレコードです。開発またはテストインスタンスで初めてアプリケーションをインストールする場合は、デモデータを読み込みます。
6. [更新] を選択します。

OTM のサブスクリプション統計情報の表示

組織で購入および消費された OTM アプリケーションサブスクリプションの数を表示し、リソース管理とオペレーショナルテクノロジーの最適化に関する貴重なインサイトを提供します。

始める前に

- 組織に有効な OTM サブスクリプションがあることを確認します。
- から利用可能な最新バージョンの ITOM SU ライセンスがインストールされていることを確認します。 [ServiceNow Store](#)。

必要なロール：sn_itom_license reader

このタスクについて

構成アイテム (CI) の割り当てとその割り当てレベルを評価して、組織の OTM サブスクリプション使用率を評価し、将来のサブスクリプション要件に備えます。

手順

1. 単品で購入した OTM サブスクリプションのサブスクリプション情報を表示するには、次の場所に移動します **OTM** ライセンス > ライセンスのサマリー。
2. **OTM 製品の [サブスクリプション] フォーム**に記載されているとおり、フォームに表示された詳細を確認します。

割り当てられたサブスクリプションユニットに対する **OTM** リソース使用状況の確認

OTM製品で管理できるリソース統計情報を確認して分析し、この情報をサブスクリプションユニットの平均割り当てと比較します。

始める前に

必要なロール：admin

このタスクについて

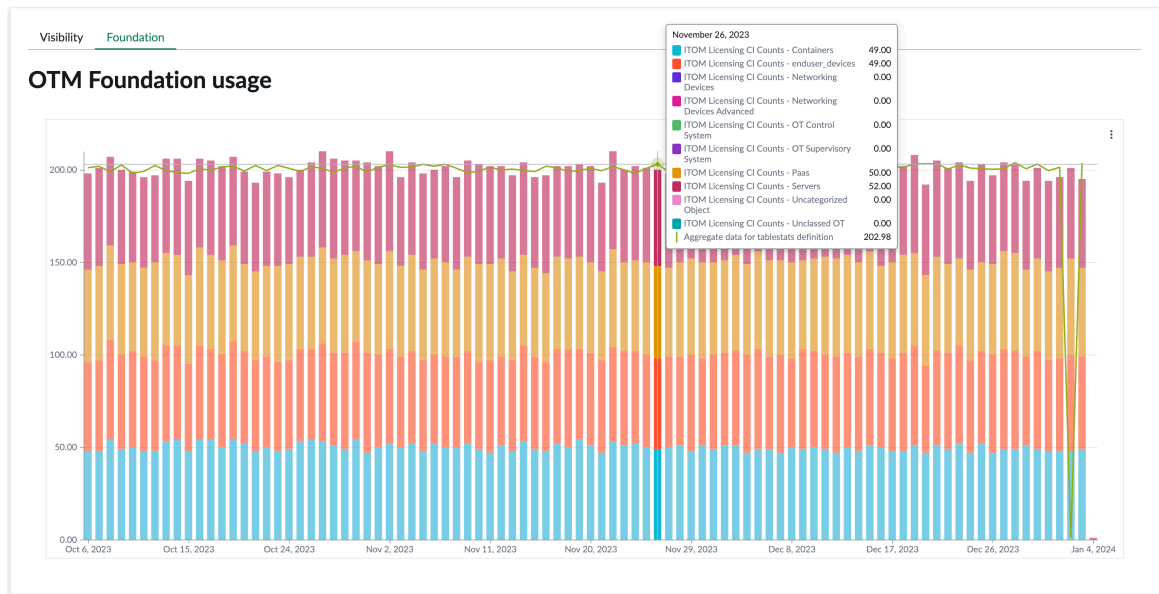
OTM ライセンスダッシュボードを使用して、OTMの詳細なライセンスデータの傾向を確認します。日次 CI 数または過去 90 日の平均を表示します。この機能は、日次カウントごとにドメイン固有の情報と特定の CI リストを提供するため、リソース使用率を経時的に効果的に監視および分析できます。

- ❗ 注：SG-OT Excel によって管理される CI は、last_scan 日より後、90 日以上前の日付でカウントされ、ライセンス消費リストに表示されます。

手順

1. 移動先 **すべて > OTM ライセンス > OTM ライセンスダッシュボード**。
2. 関連するタブを選択して、OTM 製品のダッシュボードを表示します。
たとえば、**[Foundation]** を選択します。

OTM ライセンスダッシュボード



3. バーをポイントすると、各カテゴリの CI の数が表示されます。
4. バーを選択すると、カウントされた CI のリストが表示されます。
5. 「OTM ライセンスダッシュボード」で説明されているダッシュボードを確認します。

OTM サブスクリプションで使用する CI 数の確認

日次カウントまたは直近 90 日間の CI データの平均を表示します。ServiceNow OT Foundation、ServiceNow OT Visibility and ServiceNow OT 脆弱性および対応は、OTM アプリケーションがサポートするライセンスリソースに関するインサイトを提供します。アプリケーション OTM 検出、監視、およびプロビジョニングするリソースは、CMDB に格納される構成アイテム (CI) です。OTM ライセンスモジュールは、この CI 情報を組織が購入したサブスクリプションに関する情報と組み合わせて、OTM アプリケーションによるサブスクリプションの使用に関する統計を作成します。

始める前に

- 組織に有効な OTM サブスクリプションがあることを確認します。
- から利用可能な最新バージョンの ITOM SU ライセンスがインストールされていることを確認します。 [ServiceNow Store](#)。

必要なロール：sn_itom_license reader

このタスクについて

ServiceNow では、ServiceNow OT Foundation、ServiceNow OT ヴィジビリティ、ServiceNow OT 脆弱性および対応の使用に対して料金が発生します。OTM サブスクリプションに含まれる製品と機能の詳細については、「[OTM へのサブスクリプション](#)」を参照してください。

ライセンス目的でデータを収集および統合する手順には、次の一連のアクションが含まれます。

1. OTM ライセンスシステムは、各 OTM 製品によって管理される構成アイテム (CI) の日次カウントを計算し、その後、これらの CI カウントを個別のライセンス可能な CI カテゴリに分類します。
2. 同一の構成アイテム (CI) が同じ OTM 製品内のさまざまな機能によって管理されている場合は、CI 数の重複を排除するように調整が行われます。

- IT 構成アイテム (IT CI) が OT 構成アイテムとして分類されている場合、CI は ITOM ライセンスではなく、OTM ライセンスの下で 1 回だけカウントされます。
- ライセンスモジュールは、OTM アプリケーションからの CI 数を統合して、過去 90 日間の日次 CI 数の平均を計算します。

i 注: SG-OT Excel によって管理される CI は、90 日前以降の日付でカウントされ、last_scan日付が 90 日以上前のライセンス消費としてリストされます。

- ライセンスモジュールは、OTM アプリケーションの日次平均 CI 数を、顧客契約で指定されたライセンスの詳細と照合して、ライセンス関連の統計情報を生成します。

そのため、購入したサブスクリプションユニットを組織がどのように使用しているかを示す統計情報を表示できます。

OTM アプリケーションごとに購入した CI 数とサブスクリプションについて、次の情報を表示します (個別)。

- 合計数:個々の OTM アプリケーションごとに、CI タイプ別に分類された、90 日間にわたって収集された CI 数の平均。

i 注: SG-OT Excel によって管理される CI は、90 日前以降の日付でカウントされ、last_scan日付が 90 日以上前のライセンス消費としてリストされます。

- サブスクリプションユニット率:比率は、サブスクリプションを必要とする特定の CI カテゴリの CI の数を決定します。ライセンスモジュールは、顧客契約からこの比率情報を取得します。
- 消費されたサブスクリプションユニットの合計数:各 OTM アプリケーション内の各 CI カテゴリに対して組織で使用するサブスクリプションの量。この計算は、各 CI カテゴリ内の CI の数にサブスクリプションユニット率を適用することによって実行されます。
- 消費されたサブスクリプションユニットの合計数:すべての OTM アプリケーションによって消費されたサブスクリプションユニットの合計。

ドメイン別 OTM 分類されたサブスクリプションユニット (SU) の消費量にアクセスできます。このデータは、さまざまな組織に消費と経費を割り当てするのに役立ちます。

手順

1. 移動先 **OTM** ライセンス > ライセンスレポート。

ITOM Licensing CI Counts View: License_report CI Category Search					Actions on selected rows... New
All > SKU > otm > Aggregated = true > Total Count > 0					6 total ITOM Licensing CI Counts
CI Category	Domain	Total Count	Subscription Unit Ratio	Total Subscription Units Consumed	
Application: Visibility (6)					
Networking Devices	global	17	25:1	0	
OT Control System	global	210	3:1	70	
OT Field Device	global	19	10:1	1	
OT Supervisory System	global	7	1:1	7	
Servers	global	20	1:1	20	
Unclassified OT	global	49	1:1	49	
		Sum		147	
		Sum		147	

- オプション: 過去 90 日間の日次 CI 数の平均を表示します。
- オプション: 日次 CI 数を表示するには、フィルターを変更して [集計済み] を **false** に設定します。

(Optional) 必要に応じて、列をソートしてビューを変更できます。[作成日時] 列には、CI 情報が最後に更新された日時を示すタイムスタンプが表示されます。

OTM サブスクリプションユニットを利用する CI を表示する

OTMアプリケーション (ServiceNow OT Foundation、ServiceNow OT ヴィジビリティ、ServiceNow OT 脆弱性と応答) ごとに、現在カウント可能な CI のリストを生成します。

始める前に

- 組織に有効な OTM サブスクリプションがあることを確認します。
- から利用可能な最新バージョンの ITOM SU ライセンスがインストールされていることを確認します。 [ServiceNow Store](#)。

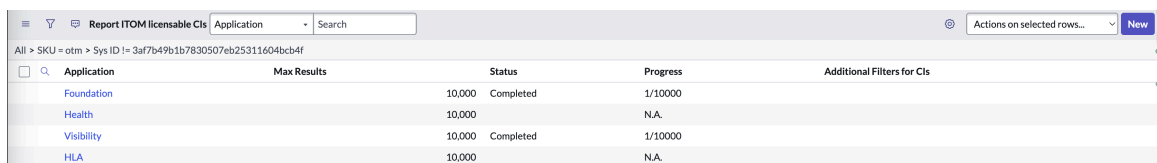
必要なロール：sn_itom_license reader

このタスクについて

生成された CI リストは、最新の日次 CI 数と強く相関しています。ただし、最後の日次カウント以降に変更が発生した場合、生成されたリストの CI の数が最新の日次カウントとわずかに異なる可能性があります。

手順

1. 移動先 **すべて > OTM ライセンス > OTM のライセンス可能な CI** をレポート。
[ITOM のライセンス可能な CI をレポート] ページが表示されます。
2. ライセンスされた CI を表示するアプリケーションを選択します。
 - 基盤
 - ヴィジビリティ
 - HLA
 - 健全性



Application	Max Results	Status	Progress	Additional Filters for CIs
Foundation	10,000	Completed	1/10000	
Health	10,000		N.A.	
Visibility	10,000	Completed	1/10000	
HLA	10,000		N.A.	

3. 選択したアプリケーションのレポートを作成するには、[ライセンス可能な CI を入力] を選択します。
4. 確認メッセージに同意し、レポートを生成するには、[はい] を選択します。

新しいレポートで、以前に生成されたレポートのデータが置き換えられます。レポートをキャンセルするには、アプリケーションを選択し、[ジョブのキャンセル] オプションを選択します。
5. 数分待ってから、ページを更新します。
レポートの処理が完了すると、アプリケーションのステータスが [完了] と表示されます。
6. アプリケーションを選択し、[ライセンス可能な CI を表示] を選択します。

OTM SKU の [ライセンス可能な CI ITOM] ページには、OTMライセンスを持つ CI のリストが表示されます。

OTM SU ライセンス参照

参照トピックを使用して、OTM ライセンスとともにインストールされるコンポーネント、OTM 製品のサブスクリプションフォーム、OTM ライセンスダッシュボードの概要に関する貴重なインサイトを得ることができます。サブトピックをナビゲートして、これらの重要な側面のそれぞれに関する

具体的なガイダンスとリファレンスにアクセスし、OTM サブスクリプションとライセンス要件を効果的に管理するのに役立ちます。

の ITOM SU ライセンスとともにインストールされるコンポーネント OTM

いくつかのタイプのコンポーネント (スケジュール済みジョブやテーブルなど) が、OTM SU ライセンスプラグインのアクティブ化とともにインストールされます。

インストールされるスケジュール済みジョブ

スケジュール済みジョブ	説明
ITOM 除外テーブル更新ストア	除外リストを更新します。
ITOM ライセンス集計ストア	過去 90 日間の日次 CI 数の平均を計算します。
ITOMHealthCIReporterWithOTOMCountOTOMStore	OTM健全性のライセンス可能な CI のリストをコンパイルします。
ITOM Health ライセンス使用回数ストア	OTM健全性の日次 CI 数を計算します。
OTOM ライセンス可視化 CI リストストア	OTMヴィジビリティのためにライセンス可能な CI のリストをコンパイルします。
OTM 基盤ライセンス CI リストストア	OTM Foundation のライセンス可能な CI のリストをコンパイルします。
OTM 基盤ライセンス使用回数ストア	OT 基盤の毎日のライセンス可能な CI 数を計算します。

インストールされるテーブル

テーブル	説明
ITOM LU Discovery ソースマッピング [itom_lu_discovery_source_mapping]	各カテゴリのライセンス可能な検出ソースのリストが含まれています。
ITOM LU Governance アプリのマッピング [itom_lu_governance_app_mapping]	ガバナンスアプリケーションとそれぞれのライセンス可能な CI とのマッピングを含むレコードのリスト。
ITOM LU Governance CI [itom_lu_governance_ci]	Governance ライセンスでカウントされる CI のリストが含まれています。
ITOM ライセンス除外メタデータ [itom_license_exclusion_metadata]	さまざまなライセンスに適用可能な除外ルールが含まれています。
ライセンスの除外 [license_exclusion_list]	除外ルールに基づいてライセンス数から除外する必要がある CI のリストが含まれています。

テーブル	説明
可視化 LU 一時 [visibility_lu_temp]	Discovery ライセンスでカウントされる CI のリストが含まれています。
ITOM ライセンスカテゴリメタデータ [itom_lu_category_metadata]	ライセンスのメタデータが含まれています。
ITOM ライセンスの検出ソース [itom_lu_discovery_sources]	すべての検出ソースのカテゴリが含まれます。

OTM 製品の [サブスクリプション] フォーム

当社製品のサブスクリプションフォームにある必須フィールドとインジケータについて学び、サブスクリプション管理を簡素化し、OTM 製品の使用を明確にします。

個別に購入したアイテム (単品) について、次のサブスクリプション統計情報を表示します。

名前

OTM アプリケーションの名前。

購入日

アプリケーションごとに購入したサブスクリプションの数。

キャパシティ定義 ID

アプリケーションからサブスクリプションユニットの日次消費データを取得するために使用される ID。

開始日/終了日

このサブスクリプションがアクティブなままである期間。

単品サブスクリプション

ライセンスモジュールは、次のようにサブスクリプションの利用量を計算して表示します。

単品サブスクリプション

[サブスクリプション] ウィンドウには、購入して割り当てられた、OTM アプリケーションへのサブスクリプションの情報が表示されます。

購入した単品サブスクリプションを表示する [サブスクリプション] ウィンドウ

Name	Start date	End date	Purchased	Allocated
Operational Technology Visibility - Subs...	2021-11-30	2024-11-29	25840	460

OTM ライセンスダッシュボード

OTMライセンスダッシュボードを使用して、取得したサブスクリプションに関連するリソース消費とステータスを評価します。ダッシュボードには、OTM アプリケーションごとに専用のレポートが表示され、90 日間の日次使用回数とサブスクリプションユニットの平均使用率が視覚的に表示されます。OTM ライセンスダッシュボードは、ITOM ライセンスアプリケーションバージョン 4.0 の不可欠なコンポーネントであり、ServiceNow Store からアクセスできます。

ストアでアプリを要求する

ServiceNow Store Web サイトにアクセスして利用可能なすべてのアプリを表示し、ストアにリクエストを送信する方法について確認してください。リリースされたすべてのアプリのリリースメモ情報については、「[ServiceNow Store バージョンの履歴リリースノート](#)」を参照してください。

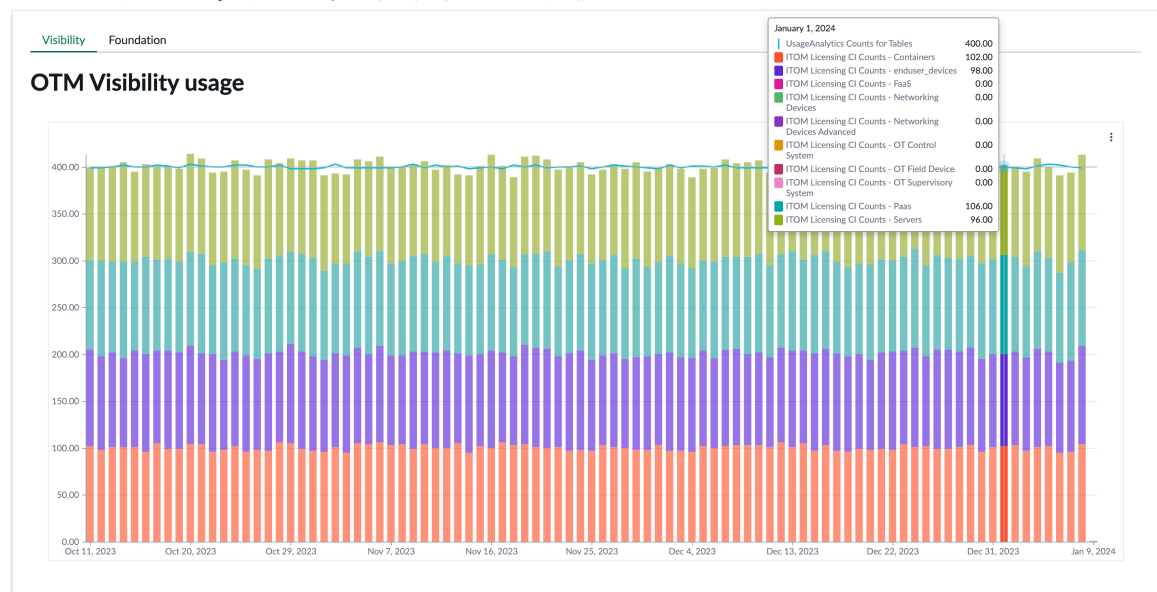
必要な **ServiceNow AI Platform** ロール

admin

アセスメントダッシュボードへのアクセス

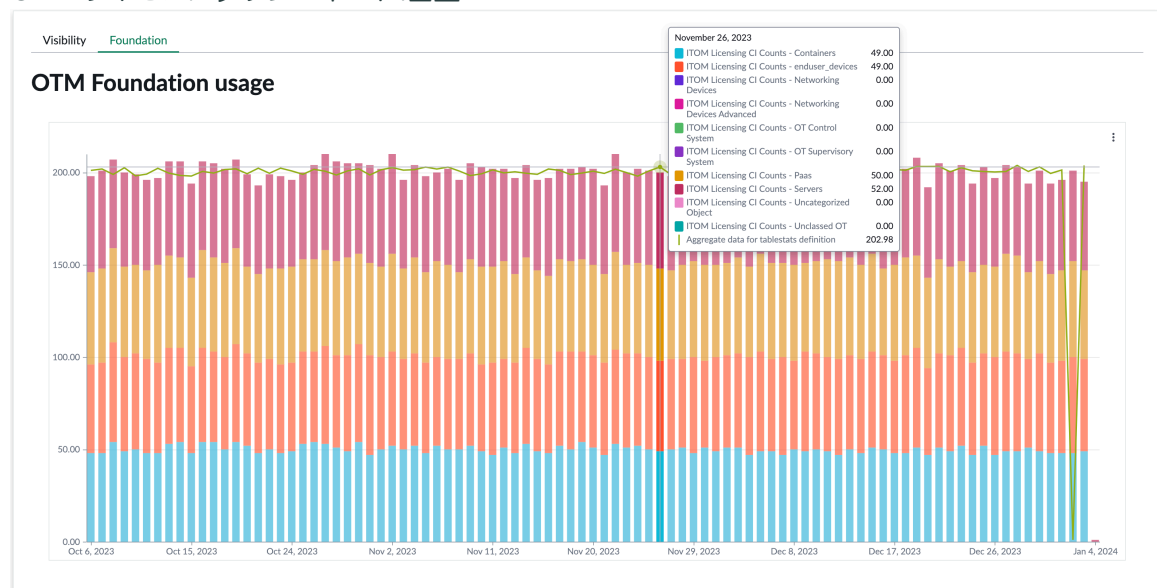
OTMのダッシュボードを開くには、次の場所に移動します すべて > **OTM ライセンス** > **OTM ライセンスダッシュボード**。

OTM ライセンスダッシュボード:ヴィジビリティ



自動翻訳

OTM ライセンスダッシュボード:基盤



ユースケース

組織内のさまざまなユーザーがこのダッシュボードをどのように使用するかの例については、次のユースケースを参照してください。

ユーザー	ダッシュボードの使用方法
admin	さまざまな OTM 製品のリソース使用率を検証します。組織が特定のリソースで購入したサブスクリプションユニットの数を超えたケースを報告します。

- i** 注: ServiceNowアプリケーションは、構成アイテム (CI) としてアプリケーションサービスを構成するデバイスおよびアプリケーションを参照します。

データの可視化

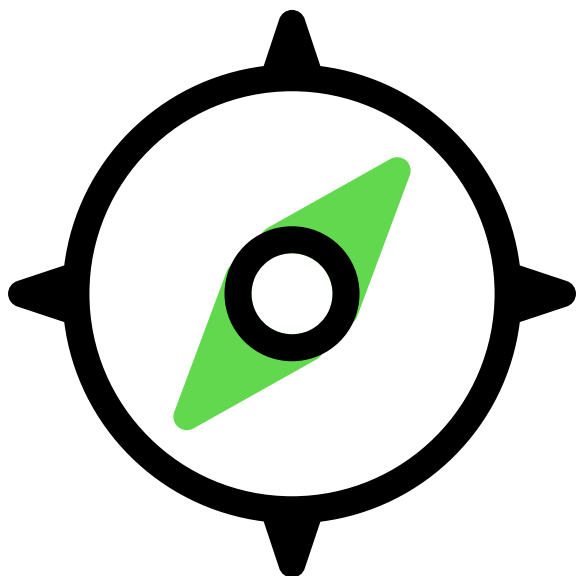
ダッシュボードには、次の可視化が含まれています。

タイトル	ソーステーブル	説明
OTM Visibility の使用状況と OTM 基盤の使用状況	ITOM ライセンス CI 数 [itom_lu_ci_counts] およびテーブルの利用状況 アナリティクスカウント [usageanalytics_count]	ITOM アプリケーションごとに過去 120 日間のさまざまなライセンス可能なカテゴリの CI の数を表すバーを表示します。ダッシュボードには、過去 90 日間のサブスクリプションユニットの平均利用量を表す線も表示されます。 i 注: SG-OT Excel によって管理される CI は、90 日前以降の日付でカウントされ、last_scan日付が 90 日以上前のライセンス消費としてリストされます。

オペレーショナルテクノロジーマネージャー

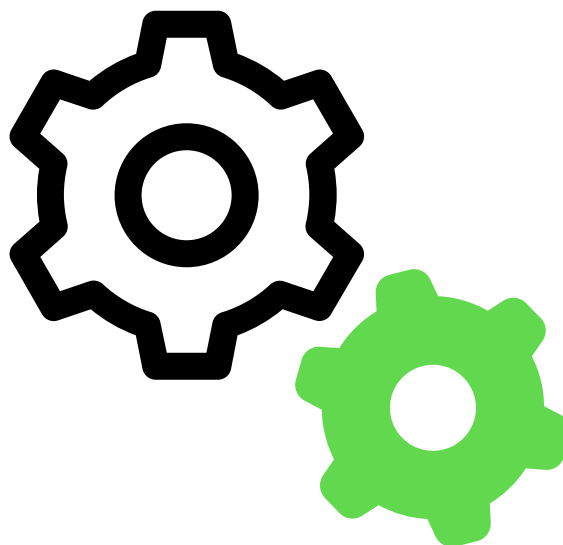
オペレーショナルテクノロジーマネージャー アプリケーションは、組織がServiceNow オペレーショナルテクノロジーソリューションを使用できるようにする基盤データと関係を作成します。オペレーショナルテクノロジーマネージャー は、ServiceNow AI Platform 内の 構成管理データベース (CMDB)、サービスグラフコネクタ、およびディスカバリーアプリケーションの使用をサポートしています。

探索



メーカーがどのように使用するかを学ぶ オペレーショナルテクノロジーマネージャー

構成



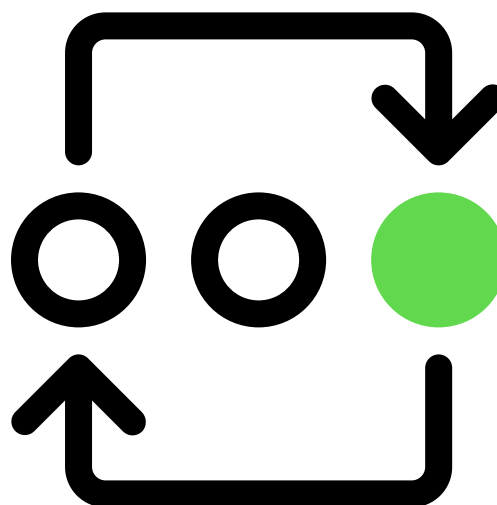
実装の計画と構成

使用方法



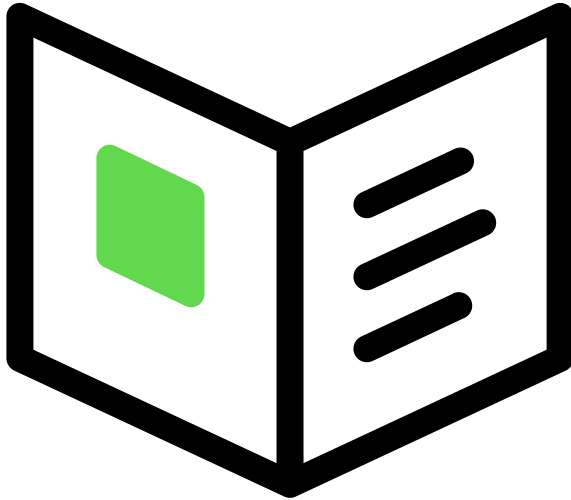
オペレーショナルテクノロジーデバイスのインポート、検出、レビュー

統合



他のアプリケーションと統合して オペレーショナルテクノロジーマネージャー を拡張します

参照



関連情報とアプリケーションの詳細を取得

オペレーショナルテクノロジーマネージャーの詳細

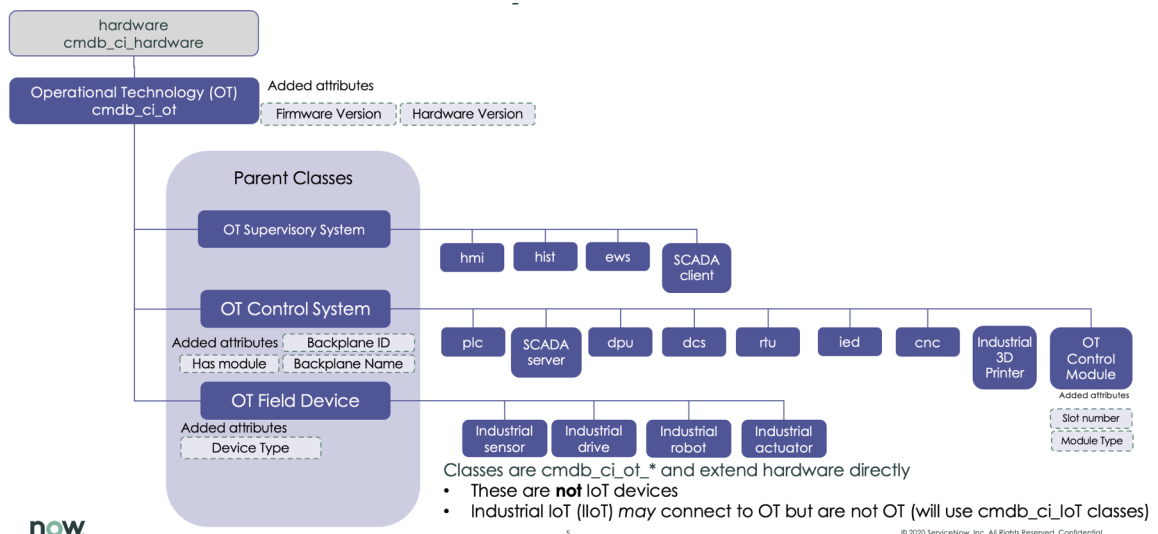
オペレーショナルテクノロジーマネージャー アプリケーションを使用して、企業が ServiceNow オペレーショナルテクノロジー ソリューションを使用できるようにする基盤データと関係を作成する方法について説明します。

オペレーショナルテクノロジーマネージャー は、ServiceNow AI Platform の 構成管理データベース (CMDB)、サービスグラフ コネクタ、およびディスカバリーアプリケーションの使用をサポートしています。

オペレーショナルテクノロジーマネージャー (OT) 構成アイテム拡張クラス

オペレーショナルテクノロジーマネージャーは、次の図に示すように、CMDB クラス階層を拡張する オペレーショナルテクノロジー (OT) 構成アイテム (CI) 拡張クラスを使用します。

OT CI 拡張クラスが OT デバイスと等しい



オペレーショナルテクノロジーマネージャー クラスの説明、識別ルール、識別子エントリ、および該当する場合は依存関係が含まれます。サービスグラフ アプリケーションは、これらのクラス拡張を使用して CI に入力し、さまざまなテクノロジーやソフトウェアを検出します。詳細については、「[運用テクノロジー \(OT\) 拡張クラス](#)」を参照してください。

の CMDB CI クラス オペレーショナルテクノロジーマネージャー

オペレーショナルテクノロジーマネージャー は 構成管理データベース (CMDB) CMDB CI クラスモデルアプリケーションの一部であるこれらの構成アイテム (CI) クラスを追加します。

i 注: このアプリケーションの詳細については、CMDB CI クラスモデルアプリケーションを参照してください。 [ServiceNow ストア](#)。

オペレーショナルテクノロジーマネージャーワークフローの CMDB CI クラス

クラス	説明	拡張された CI クラス
ネットワーク侵入検知システム	ネットワーク侵入検知システム (NIDS) [cmdb_ci_nids] クラスは、パッシブネットワークモニタリングアプライアンスと、それが検出するネットワーク上のデバイスとの間の関係をビルドします。	cmdb_ci_nids

OT デバイスデータのインポートと検出

既存の オペレーショナルテクノロジー デバイスデータを ServiceNow AI Platformにアップロードするには、複数の方法を使用できます。

サービスグラフ コネクタ (Excel)

サービスグラフコネクタ (Excel) 機能を使用して、入力済みの Excel フラットファイルスプレッドシートからオペレーショナルテクノロジーデータをインポート Microsoft. 統合ハブ抽出変換ロード (ETL) のスプレッドシートを使用して、このデータをCMDBにアップロードします。詳細については、「[Microsoft Excel のサービスグラフコネクタ](#)」を参照してください。

オペレーショナルテクノロジー の ディスカバリー

産業用コントロールシステム (ICS) ネットワーク内の指定された Purdue レベルのオペレーショナルテクノロジーデバイスを検出するには、オペレーショナルテクノロジー機能のディスカバリーを繰り返し実行します。これは、標準的な ディスカバリープロセスと同様の方法で動作します。ただし、その ディスカバリー は通常、OT ディスカバリースケジュールの作成時に選択したレベルに応じて、Purdue レベル 3 ~ 3.5 で行われます。詳細については、「[OT ネットワークの IT ディスカバリー](#)」を参照してください。

i 注: 産業用制御システムの Purdue レベルの詳細については、「https://subscription.packtpub.com/book/networking_and_servers/9781788395151/1/ch01lvl1sec10/the-purdue-model-for-industrial-control-systems」を参照してください。

サービスグラフServiceNow パートナーからのコネクタ

ServiceNow パートナーは、既存の OT データのアップロードに使用できる サービスグラフ コネクタも提供しています。

OT ネットワークと標準 IT ネットワークの違い

オペレーショナルテクノロジーネットワークにあるデバイスと標準的な情報技術 (IT) ネットワークにあるデバイスでは、構成管理データベース (CMDB) によるデバイスの処理方法に違いがあります。

Information Technology Operations Management (ITOM) で管理される構成アイテム (CI) は、CMDBでタイプ IT として分類されます。これらは、Purdue モデルのレベル 4 と 5、または Enterprise レベルに存在します。

OT データモデルで管理されるデバイスは、Purdue モデルのレベル 0 ～ 3.5 に存在し、OT デバイスには次の 2 つの主要コンポーネントがあります。

1. CI クラスレコード。これは、IT クラス、または OT クラスの CI です。
2. OT デバイスの詳細レコード。OT デバイスタイプ (機能) およびその他の OT 固有の属性を説明するものです。

i 注: OT データモデルと拡張クラスの詳細については、「[オペレーショナルテクノロジー \(OT\) 拡張クラス](#)」を参照してください。

次の図は、これらの違いを示しています。

オペレーショナルテクノロジー **CMDB** クラスモデルが **Purdue** レベルをサポート



i 注: Purdue レベルの詳細については、「https://subscription.packtpub.com/book/networking_and_servers/9781788395151/1/ch01lvl1sec10/the-purdue-model-for-industrial-control-systems」を参照してください。

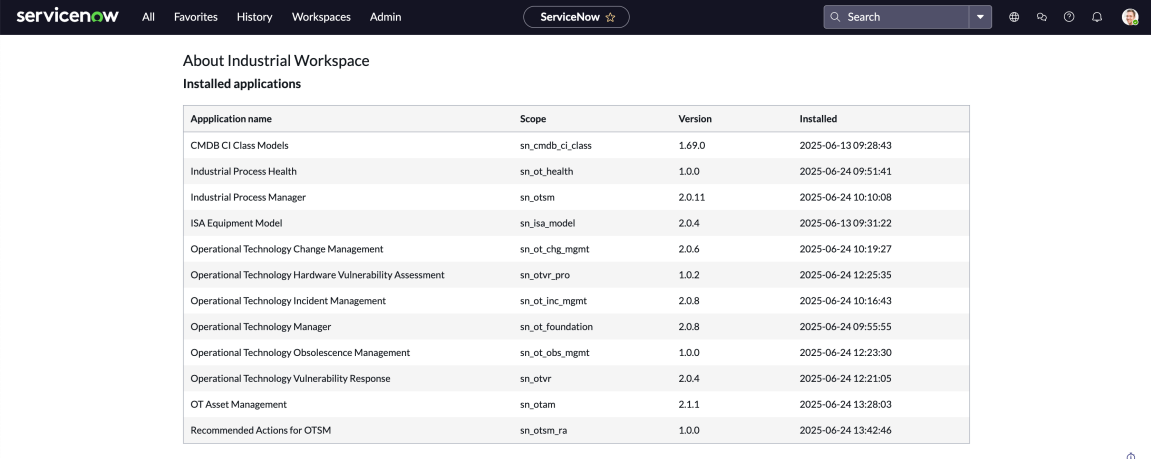
インストールされている オペレーショナルテクノロジー アプリケーションの表示

インスタンスにインストールした オペレーショナルテクノロジー (OT) アプリケーションを表示して、オペレーショナルテクノロジー管理 ソリューションの使用方法をより明確に把握できます。

cmdb_ot_viewer ロールまたは cmdb_ot_isa_viewer ロールがアサインされている場合は、次に移動して、インスタンスにインストールした OT アプリケーションを表示できます。すべて > 産業用ワークスペースアドミン > 産業用ワークスペースについて。

インストール済みアプリケーションテーブルには、インスタンスにインストールされて利用可能な各アプリケーションのアプリケーション名、スコープ、バージョン、

およびインストール日が含まれています。次の画像は、テーブルの例を示していま



The screenshot shows the 'About Industrial Workspace' page in ServiceNow. Under the 'Installed applications' section, there is a table with the following data:

Application name	Scope	Version	Installed
CMDB CI Class Models	sn_cmdb_ci_class	1.69.0	2025-06-13 09:28:43
Industrial Process Health	sn_ot_health	1.0.0	2025-06-24 09:51:41
Industrial Process Manager	sn_otsm	2.0.11	2025-06-24 10:10:08
ISA Equipment Model	sn_isa_model	2.0.4	2025-06-13 09:31:22
Operational Technology Change Management	sn_ot_chg_mgmt	2.0.6	2025-06-24 10:19:27
Operational Technology Hardware Vulnerability Assessment	sn_otvr_pro	1.0.2	2025-06-24 12:25:35
Operational Technology Incident Management	sn_ot_inc_mgmt	2.0.8	2025-06-24 10:16:43
Operational Technology Manager	sn_ot_foundation	2.0.8	2025-06-24 09:55:55
Operational Technology Obsolescence Management	sn_ot_obs_mgmt	1.0.0	2025-06-24 12:23:30
Operational Technology Vulnerability Response	sn_otvr	2.0.4	2025-06-24 12:21:05
OT Asset Management	sn_otam	2.1.1	2025-06-24 13:28:03
Recommended Actions for OTSM	sn_otsm_ra	1.0.0	2025-06-24 13:42:46

す。

オペレーショナルテクノロジーマネージャー の構成

ServiceNow オペレーショナルテクノロジー ソリューションのデータ基盤を作成できるように、オペレーショナルテクノロジーマネージャー アプリケーションを構成します。

タスク	目的
1. オペレーショナルテクノロジー (OT) 拡張クラスをインストールします。	オペレーショナルテクノロジー処理で使用するために構成管理データベース (CMDB) クラス階層を拡張します。
2. オペレーショナルテクノロジーマネージャーをインストールします。	オペレーショナルテクノロジーマネージャー アプリケーションをインストールします。
3. オペレーショナルテクノロジー ロールを割り当てます。	ロールを割り当てて、各ユーザーが使用できるアクションをコントロールします。
4. サービスグラフコネクタをインポートするための Microsoft Excel スプレッドシートを準備します。	Microsoft Excel スプレッドシートを作成し、ServiceNow AI Platformにアップロードする既存のオペレーショナルテクノロジーデータを入力します。 詳細については、「 サービスグラフコネクタインポート用のインポート前 OT ワークシートエントリレビューツールの準備 」を参照してください。
5. インポートタスクを使用して Excel スプレッドシートをインポートします。	オペレーショナルテクノロジーデータを構成管理データベース (CMDB) にアップロードします。 詳細については、「 インポートタスクによる Microsoft Excel のサービスグラフコネクタの使用 」を参照してください。

タスク	目的
6. OT ネットワークの IT ディスカバリー機能を実行します。	産業用コントロールシステム (ICS) ネットワーク内の指定された Purdue レベルの オペレーショナルテクノロジー (OT) デバイスを検出します。 オペレーショナルテクノロジー のディスカバリーの詳細については、「 OT ネットワークの IT ディスカバリー 」を参照してください。
7. ServiceNow パートナーが提供するサービスマニファーストグラフコネクタをインストールします。	パートナーが提供する ServiceNow, Inc. コネクタを、ServiceNow Storeで利用可能になったときにインストールします。
8. [オペレーショナルテクノロジー (OT)] メニューで [すべての OT デバイス] または [IP アドレス別のすべての OT デバイス] を選択します。	Excel スプレッドシートをインポートした後、または OT ネットワークの IT ディスカバリー機能を実行した後、社内の OT デバイスの詳細情報を編集または表示します。

の CSDM フレームワークの実装 オペレーショナルテクノロジー

CSDMフレームワークに従うことで、レポートと分析における一貫した精度という主な目標を確実に達成し、オペレーショナルテクノロジー (OT) 環境を効果的に管理できます。

CSDM OT フレームワーク

CSDMフレームワークの実装は段階的に完了する必要があります。詳細については、「[CSDM フレームワークを段階的に実装する](#)」を参照してください。

オペレーショナルテクノロジー 製品ビュー

オペレーショナルテクノロジーは、ライフサイクルのさまざまな段階で OT デバイスと本番プロセスの幅広い管理に対応する製品をカバーしています。この製品ビューの目的は、オペレーショナルテクノロジー 主要エンティティがコア 共通サービスデータモデル (CSDM) (CSDM) フレームワークでどのように機能するかを理解することです。

オペレーショナルテクノロジーマネージャー

企業が オペレーショナルテクノロジー ソリューションを使用できるようにするための基盤データと関係を作成します。詳細については、「[オペレーショナルテクノロジーマネージャー](#)」を参照してください。

製造業プロセスマネージャー

オペレーショナルテクノロジー ソリューションに必要な ISA-95 機器モデルデータ基盤を作成できます。詳細については、「[製造業プロセスマネージャー](#)」を参照してください。

オペレーショナルテクノロジー脆弱性対応

サイトレベルでの OT デバイスの脆弱性についての効果的な優先順位付けと修復が可能になります。詳細については、「[オペレーショナルテクノロジー脆弱性対応](#)」を参照してください。

オペレーショナルテクノロジーインシデント管理

エンジニアが OT デバイスと本番プロセスの問題を迅速に解決できるようになります。詳細については、「[オペレーショナルテクノロジーインシデント管理](#)」を参照してください。

オペレーショナルテクノロジー変更管理

組織が OT デバイスと本番プロセスに変更を実装できるようにします。詳細については、「[オペレーショナルテクノロジー変更管理](#)」を参照してください。

オペレーショナルテクノロジーのナレッジ管理

組織が、OT インシデントに関連するナレッジ記事で OT システムに関する情報を取得できるようになります。詳細については、「[オペレーショナルテクノロジーのナレッジ管理](#)」を参照してください。

オペレーショナルテクノロジー要求管理

OT サービスカタログにアクセスして OT カatalogアイテムを要求し、定義されたフローに基づいて実行できるようにします。OT ワーカーは、Catalogアイテムから OT 要求を作成して送信できます。これにより、一貫したエクスペリエンスが提供され、部門横断型要求が容易になります。詳細については、「[オペレーショナルテクノロジー要求管理](#)」を参照してください。

オペレーショナルテクノロジーと CSDM テーブル

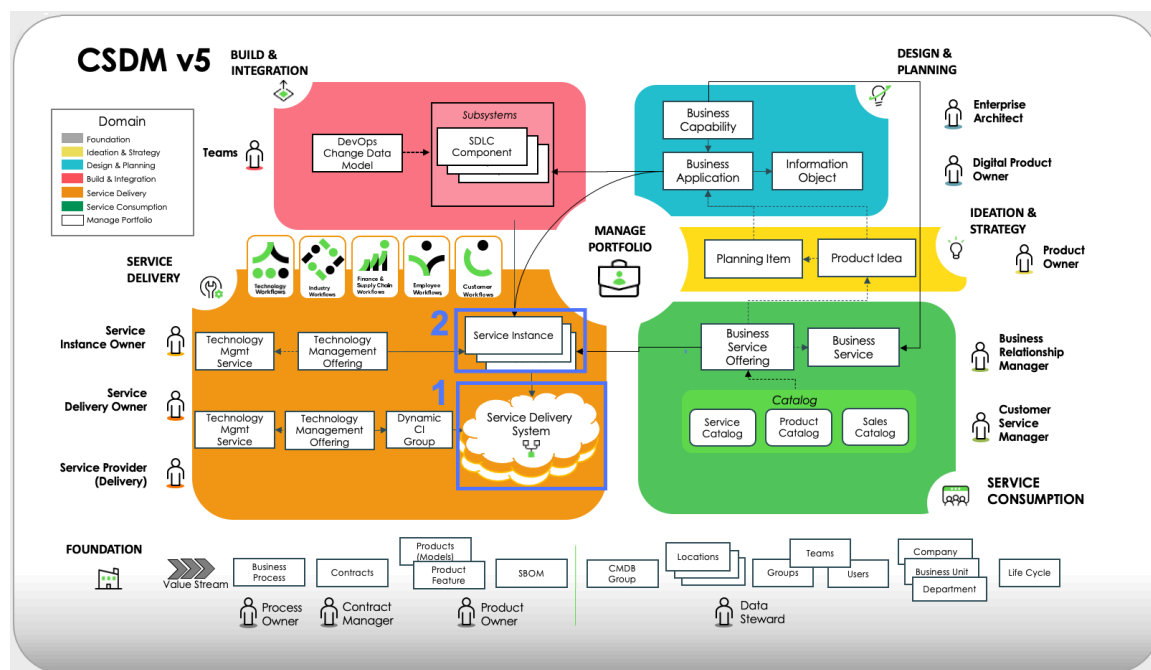
オペレーショナルテクノロジーは CSDM テーブルを管理および使用します。いくつかの ServiceNow 製品は、オペレーショナルテクノロジーのメリットを活用し、それに対して価値を付加します。

オペレーショナルテクノロジーによって管理される CSDM テーブル

オペレーショナルテクノロジー (OT) によって管理されるテーブルには、主に次の 3 つのカテゴリがあります。

- オペレーショナルテクノロジー デバイス：OT (ICS または PCN) ネットワークで検出された構成アイテム。
- ISA 設備階層モデルエンティティ：OT デバイスによって自動化された産業プロセス。
- OT システムサービス:分散制御システム (DCS) などの他のコントロールシステムを作成します。

この図の番号は、インシデント管理によって管理される CSDM テーブルに対応しています。

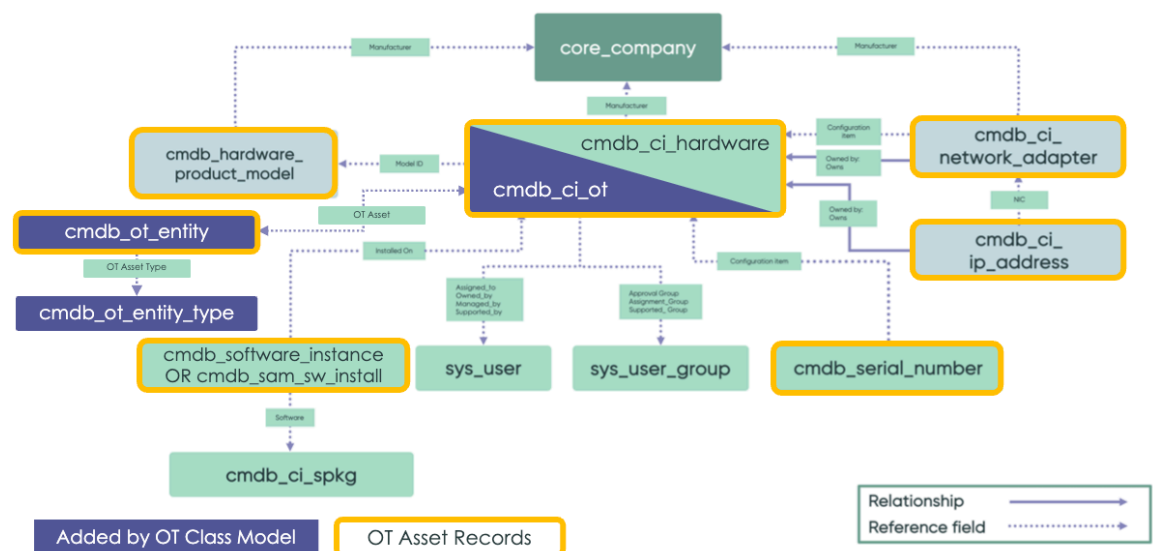


オペレーショナルテクノロジーによって使用される **CSDM** テーブル

1. OT デバイス：

- a. ハードウェアを拡張することによって、オペレーショナルテクノロジー ハードウェアクラス (cmdb_ci_ot) に対して構成アイテムクラスが作成されました。詳細については、「[オペレーショナルテクノロジー \(OT\) 拡張クラス](#)」を参照してください。
- b. OT デバイスの詳細 (cmdb_ot_entity) 参照を使用して OT デバイスの詳細を cmdb_ot_entity テーブルに追加することで、任意の CI クラス (関連する既存のハードウェアクラスおよび新しい OT クラス) を OT デバイスとして指定できます。OT デバイスの詳細には、Purdue レベルや OT デバイスタイプなどの OT 固有の特性が含まれています。
- c. OT デバイスタップでは、産業または生産プロセスを自動化する CI の機能を記述します。cmdb_ot_entity_type テーブルには、これらの機能またはロールが記述されています。

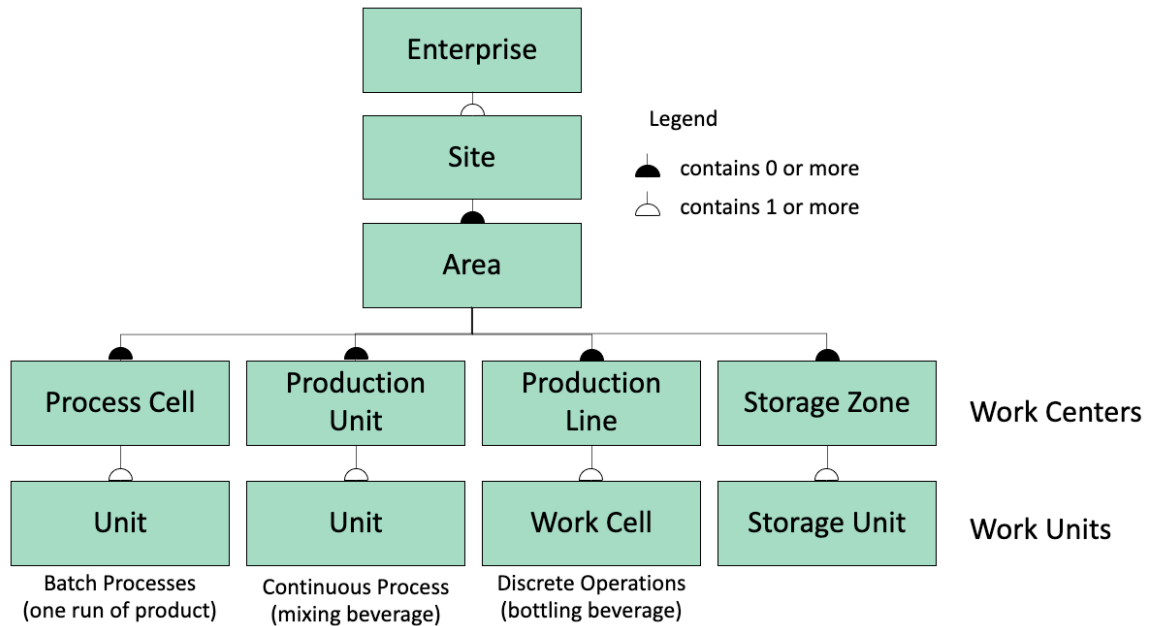
ここに示すように、単一の OT デバイスは少なくとも 2 つのレコード (1 つの CI レコードと 1 つの OT エンティティレコード) で表されます。デバイスには、最大 6 つのテーブルに 6 つ以上のレコードを含めることができます (たとえば、CI に複数の IP アドレスと MAC アドレスがある場合など)。



2. 設備モデルのエンティティ：

- a. 機器モデルエンティティクラスは、計算されたアプリケーションサービスを拡張し、次の目的で使用されます。
 - i. OT デバイスまたは機器モデルエンティティのサイトを表します。親のない機器モデルエンティティテーブル (cmdb_ci_ot_isa_entity) のレコードはサイトと見なされます。
 - ii. 生産プロセスの一部の ISA 機器モデルエンティティを表します。
- b. 機器モデルテンプレート (isa_entity_template) を使用して、産業環境にある機器モデルエンティティ間の関係をさらに記述することができます。
 - i. レベル (isa_entity_level) は、機器モデルエンティティの階層レベルを示します。デフォルトの ISA-95 テンプレートの場合、ここに表示されるレベル (エリア、作業センター、および作業単位) はベースシステムに含まれています。
 - ii. レベルタイプ (isa_entity_type) は、指定されたレベルの機器モデルエンティティによって表されるプロセスのタイプを示します。デフォルトの ISA-95 テンプレートの場合、ここに表示

されているタイプ (プロセスセル、生産単位、生産ライン、およびストレージゾーン) はベースシステムに含まれています。



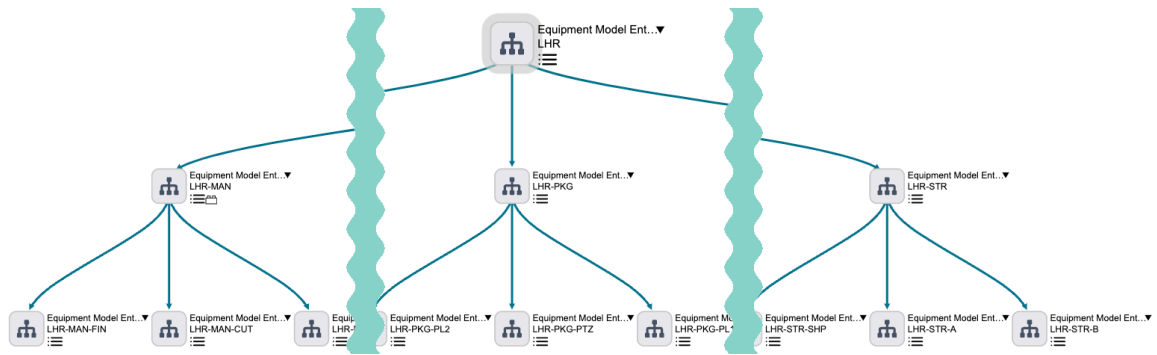
3. OT システムサービス:

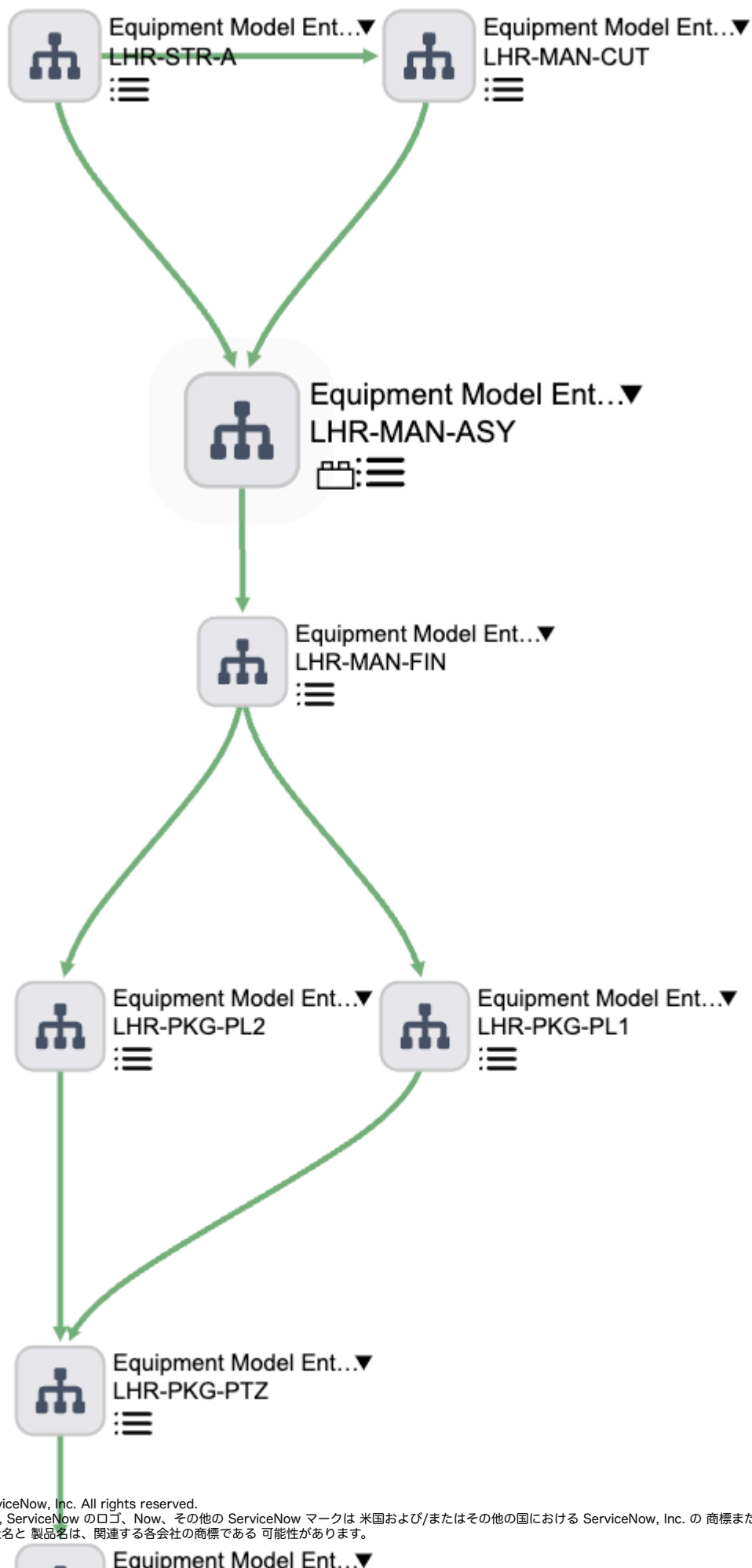
- OT システムサービスクラスは計算されたアプリケーションサービスを拡張し、OT システムサービスの作成に使用されます
- OT システムサービスは、機器モデルエンティティ、ソフトウェアアプリケーションのテクニカルサービス、およびビジネスオファリングに関連付けることができます。
- OT システムサービスは、次のアイテムに関連付けることができます。
 - OT システムサービスの一部である OT デバイス
 - OT システムサービスが管理する機器モデルエンティティ

CSDM には、OT デバイスと機器モデルエンティティが互いにどのように関連しているかをより正確に区別する関係タイプ (オペレーショナルテクノロジー固有) が含まれています。

- Producer for::Consumer of** : 機器モデルエンティティ間の生産プロセス (マテリアルフロー) を示します。
- Contains Element::Element of** : 機器モデルエンティティ間の階層関係を示します。
- Automated by::Automates** : OT デバイスと、OT デバイスが自動化する機器モデルエンティティの関係を示します。
- Detects::Detected by** : どのネットワーク侵入検知システム (NIDS) クラス (cmdb_ci_nids) が OT ネットワーク上の OT デバイスを検出したかを示します。
- Owns::Owned by** : OT コントロールモジュールが OT コントロールシステム (PLC、DCS など) によって所有されている場合の関係を示します。

次の依存関係マップは、OT デバイスと機器モデルエンティティの関係を示しています。





オペレーショナルテクノロジーに付加価値を提供する製品

OT を以下のいずれかの ServiceNow 製品と併用すると、OT の価値をさらに高めることができます。

オペレーショナルテクノロジーのディスカバリー

オペレーショナルテクノロジーのディスカバリーは、IT クラスのハードウェアおよびソフトウェア CI に関する詳細を提供し、OT スケジュールごとに Purdue レベルやサイトなどの追加の OT デバイスコンテキストを提供するように構成できます。OT のディスカバリーは オペレーショナルテクノロジーマネージャー 製品の一部です。

製造業プロセスマネージャー

OT デバイスが機器モデルエンティティにアサインされると、それらの間に *automated by::automates* 関係が作成されます。これは、産業用 ワークスペースで手動で行うか、[OT サブネットマッピング] メニューアイテムにある「ゾーンベースの IP ネットワークグループ間の自動マッピング (AMAZING)」機能を使用して、OT サブネットと機器モデルエンティティ間の関係を使用して行うことができます。

オペレーショナルテクノロジー脆弱性対応

サードパーティのセキュリティプラットフォームとの OT 認定統合からレコードをインポートして脆弱性一致アイテム (VIT) レコードが作成されると、OT デバイスが VIT に関連付けられます。これにより、次の両方の機能が有効になります。

- マップされた機器モデルエンティティの重要度に基づくリスク計算。
- サイトベースのアサイン先グループによる修正のための適切なローカルチームへの VIT のアサイン。

オペレーショナルテクノロジーインシデント管理

OT のインシデント管理は、ほとんどの OT デバイスの IT とは別に実行されます。OT インシデントレコードにより、OT デバイスに関連する問題へのサイトベースのアクセスと表示が可能になります。

オペレーショナルテクノロジー変更管理

OT 変更要求により、OT デバイスまたは産業機器の構成を変更することができます。

オペレーショナルテクノロジーのナレッジ管理

オペレーショナルテクノロジーのナレッジ管理を使用すると、OT インシデントに関連するナレッジ記事で OT システムに関する情報をキャプチャできます。

オペレーショナルテクノロジー要求管理

OT サービスカタログにアクセスして OT カタログアイテムを要求し、定義されたフローに基づいて実行できるようにします。OT ワーカーは、カタログアイテムから OT 要求を作成して送信できます。これにより、一貫したエクスペリエンスが提供され、部門横断型要求が容易になります。

オペレーショナルテクノロジーからメリットを得る製品

IT Service Management (ITSM)

サービスには、サイト、本番プロセス、OT デバイスのコンテキストと、その下に階層化された情報とテクノロジーがあります。

Information Technology Operations Management (ITOM)

管理対象の OT デバイスハードウェアおよびソフトウェアとともに、本番プロセスのビジネスコンテキストを理解します。

セキュリティオペレーション

保護対象の OT デバイスハードウェアおよびソフトウェアとともに、本番プロセスのビジネスコンテキストを理解します。

ガバナンス、リスク、コンプライアンス (GRC)

監査人は、本番プロセスフローと、関連する情報オブジェクトをより適切に活用できます。これは、監査人が、監査のスコーピング、リスクの測定、および監査アクティビティの管理のための設計時のデータ機密性を理解するために役立ちます。

資産管理

ソフトウェアおよびハードウェアのライフサイクルプロセスが本番プロセスに及ぼす影響を管理します。

オペレーショナルテクノロジーマネージャーのユースケース

このセクションでは、オペレーショナルテクノロジーマネージャー のユースケースについて説明します。

オペレーショナルテクノロジーマネージャー のユースケース

オペレーショナルテクノロジーマネージャー アプリケーションは、オペレーショナルテクノロジーソリューションを使用できるようにするための基盤データと関係を作成します。ServiceNow AI Platform での 構成管理データベース (CMDB)、サービスグラフコネクタ、および ディスカバリーアプリケーションの使用をサポートします。

産業用ワークスペース の OT ヴィジビリティダッシュボードには、OT デバイスのインベントリが要約されます。ダッシュボードの詳細については、「[オペレーショナルテクノロジー ヴィジビリティダッシュボード](#)」を参照してください。

主要な機能

- オペレーショナルテクノロジーマネージャー は、CMDB クラス階層を拡張する OT 構成アイテム (CI) 拡張クラスを使用します。
- OT ネットワークの IT ディスカバリーは OT 固有のルールに制限されており、OT 関連のメタデータを OT ディスカバリースケジュールに追加できます。
- サービスグラフ Connector (Excel) は、入力された Microsoft Excel フラットファイルスプレッドシートから OT データをインポートします。このデータは検証され、CMDB の OT デバイスの詳細を表すための適切なテーブルレコードと関係に変換されます。

結果

オペレーショナルテクノロジーマネージャー ユースケースでは、次のことができます。

- 産業環境における OT デバイスの依存関係を可視化します。
- サイト固有の RBAC を使用して、サイトごとに OT デバイスのライフサイクルを管理します。
- 確実なデータ基盤を作成し、インフラストラクチャの重要なレベルを定義します。

製造業プロセスマネージャー のユースケース

製造業プロセスマネージャー アプリケーションを使用して、オペレーショナルテクノロジーソリューションに必要な ISA-95 機器モデルデータ基盤を作成します。

主要な機能

製造業プロセスマネージャー ワークスペースでは、次の操作を実行できます。

- ISA-95 モデルを使用して、産業環境の各サイトの本番プロセスを記述します。
- 機器モデルエンティティとそれらの相互関係および OT デバイスとの関係を管理します。
- OT サブネットと機器モデルエンティティの関係を使用して、すべての OT デバイスの関係を自動化する機器モデルエンティティに自動的にマッピングします。

結果

製造業プロセスマネージャー を使用すると、各サイトの機器モデルのカスタムバージョンを作成できます。

オペレーショナルテクノロジー脆弱性対応 のユースケース

オペレーショナルテクノロジー脆弱性対応 により、サイトレベルでの OT デバイスの脆弱性についての効果的な優先順位付けと修復ができます。

主要な機能

- 修復オーナーワークスペースは、脆弱性一致アイテム (VIT) を本番プロセスにマッピングします。
- OT VIT のリスク計算は、OT デバイスによって自動化された機器モデルエンティティの重要度に基づいて行うことができます。
- VIT で OT デバイスにアサインされたサイトに基づいて、修復オーナーに VIT を自動アサインします。

結果

OT デバイスの CMDB 関係を活用することで、自動化する本番プロセスの重要度に基づいて脆弱なデバイスまたはアイテムを優先順位付けできます。

OT エンジニアまたは OT 脆弱性マネージャーは、オペレーショナルテクノロジー脆弱性対応 を使用して次のような質問の答えを見つけることができます。

- 使用している OT デバイスにどのような脆弱性があるか？ ☒
- OT 固有のリスクを使用して脆弱性の修正を優先するにはどうすればよいか？
- OT の脆弱性の修正に向けての進捗状況はどのようなものか？

産業用ワークスペースの OTVR (PA) ダッシュボードと OT 脆弱性リスクロールアップダッシュボードは、システムの脆弱性を要約したものです。OTVR (PA) ダッシュボードの詳細については、「[オペレーショナルテクノロジー脆弱性対応 \(PA\) ダッシュボード](#)」を参照してください。OT 脆弱性リスクロールアップダッシュボードの詳細については、「」を参照してください。

オペレーショナルテクノロジーインシデント管理 のユースケース

OT インシデントは、OT ネットワーク上の OT デバイスによって提供されるサービスが中断されると発生します。インシデントが最初に作成されたときに OT デバイスが不明な場合があります。オペレーショナルテクノロジーインシデント管理 により、エンジニアは OT デバイスと本番プロセスの問題を迅速に解決できます。

主要な機能

ユーザーが産業用 ワークスペースから OT インシデントを作成すると、OT インシデントを IT インシデントと区別するために、インシデントに OT のネットワークタイプが自動的にアサインされます。このフィールドは、デフォルトでは表示されません。

結果

オペレーショナルテクノロジーインシデント管理によって、エンジニアが OT デバイスと本番プロセスの問題を迅速に解決できるようになります。これにより、OT インシデントを IT インシデントとは別に管理できます。

オペレーショナルテクノロジー変更管理 のユースケース

オペレーショナルテクノロジー変更管理 を使用すると、チームメンバーは OT デバイスまたは産業機器の構成の変更について共同作業を行うことができます。

主要な機能

- すべてのステークホルダーを結び付ける、デジタル化変更ワークフロー。
- さまざまな変更管理プロセス (ワークフロー) を持つサイト。
- IT Change Management と オペレーショナルテクノロジー変更管理 は分離されていますが、必要に応じて組み合わせることができます。
- オペレーショナルテクノロジーインシデント管理およびオペレーショナルテクノロジー脆弱性対応アプリケーションと統合されたオペレーショナルテクノロジー変更管理ワークフロー。
- ダウンタイムスケジュールに合わせて調整された、設備モデルエンティティの工場フロアの変更。

結果

次の例は、組織に オペレーショナルテクノロジー変更管理 を適用する方法を示しています。

- OT デバイスの脆弱性の修正を担当する OT 修復オーナーが、一連の脆弱性を修正するための変更を開始する。
- OT 構成とプラントエンジニアリングアクティビティを担当する OT 技術者が、作業現場で故障したロボットアームを修理するための変更を実行したいと考えています。
- 全体的な生産アクティビティを担当するプラント長が、エンジニアリングチームによって要求された変更をレビューして承認したいと考えています。

オペレーショナルテクノロジーのナレッジ管理 のユースケース

オペレーショナルテクノロジーのナレッジ管理 は、OT インシデントに関連するナレッジ記事で オペレーショナルテクノロジー (OT) システムに関する情報をキャプチャするのに役立ちます。組織は、これらのナレッジ記事を使用して、ユーザーが適切な情報にアクセスできるようにし、ユーザーとの誤解を防ぐことができます。

主要な機能

- オペレーショナルテクノロジー管理ソリューションで既存のナレッジ管理 ServiceNow AI Platform 機能を使用する機能。
- OT インシデントに関連するすべてのナレッジベース記事を参照し、インシデントレコードから直接ナレッジ記事を作成する機能。
- ナレッジマネージャーとナレッジユーザーの OT ナレッジベースを構成する機能。
- 産業用 ワークスペースでナレッジ記事を作成する機能。
- ナレッジ記事の公開、編集、廃止、または削除の承認を要求する機能。
- 更新された情報を使用して既存のナレッジ記事を編集する機能。

結果

次の例は、チームに オペレーショナルテクノロジーのナレッジ管理 を適用する方法を示しています。

- 数年の経験を持つ OT エンジニアは、ガイドワーカーと若手技術者のために、OT デバイスの知識を 1 か所に集約したいと考えています。
- 生産プロセスオペレーションを担当する最前線の作業者と技術者は、工場フロアの問題に気付き、修復について説明するナレッジ記事を必要としています。

オペレーショナルテクノロジー要求管理 のユースケース

オペレーショナルテクノロジー要求管理 を使用すると、OT サービスカタログにアクセスして OT カタログアイテムを要求し、定義されたフローに基づいてアイテムを履行できます。OT ワーカーは、カタログアイテムから OT 要求を作成して送信できます。これにより、一貫したエクスペリエンスが提供され、部門横断型要求が容易になります。

主要な機能

- 単一のビューで複数のカタログ要求を効率的に管理できます。
- 透明性を高め、要求プロセスを迅速化し、自動通知と承認によって遅延を最小限に抑えます。
- カタログ要求の作成と更新に使用できる製品とサービスのメニューを維持します。

結果

次の例は、チームに オペレーショナルテクノロジー要求管理 を適用する方法を示しています。

- OT エンジニアは、さまざまな OT 製品やサービスの OT 要求を 1 か所で提出および管理できます。
- プラントの責任者またはスーパーバイザーは、適切なチームと連携して、工場のフロアで報告されたインシデントを修正できます。

オペレーショナルテクノロジー と CSDM の要素

CSDM の要素があるビジネスアプリケーションの管理に関連する用語。

オペレーショナルテクノロジー用語

期間	定義
機器モデル	出力または製品を生産するために生産工程がどのように編成されているかを説明するサービスレコード。
製品プロセス	機器モデルエンティティと、原材料から最終製品までのワークフローのさまざまなステージとの関係。
サイト	親を持たない親機器モデルエンティティレコード。サイトにアサインされた OT デバイスに読み取りまたは書き込みレベルのアクセスをアサインするために使用される、特別な機器モデルエンティティレコードです。
OT デバイス (サイトのアサイン)	サイトのアサインは、OT デバイスのロールベースセキュリティ (RBAC) に必要です。OT デバイスは 1 つのサイトにのみ属することができるため、これは OT デバイスレコードの OT デバイスの詳細 (cmdb_ot_entity) テーブル部分の選択リスト参照フィールドとして実装されます。
OT デバイス (automates::automated)	「automates::automated by」関係は、OT デバイスが本番プロセスにどのように関連してい

オペレーショナルテクノロジー用語 (続く)

期間	定義
	るかを示します。本番プロセスには、複数の機器モデルエンティティが含まれることがあります。
Windows	OT と IT のどちらのネットワークでも、Windows サーバーは <code>cmdb_ci_win_server</code> サーバーで表されます。 さらに、OT ネットワーク内の Windows サーバーは、<code>[cmdb_ci_win_server.cmdb_ot_entity]</code> フィールドに参照があり、OT での機能とその他の OT 特性 (Purdue レベル、サイトなど) を記述する <code>cmdb_ot_entity</code> テーブル内のレコードを指しています。

オペレーショナルテクノロジー FAQ

CSDM フレームワークの実装時にいくつかの疑問点が生じることがあります。

生産プロセスと機器モデルエンティティの違いは何ですか？

機器モデルエンティティとは、出力または製品を生産するために生産工程がどのように編成されているかを説明するために使用されるサービスレコードのことです。生産プロセスは、生の入力から完成品への材料の流れとして機器モデルエンティティ間の関係を示します。

サイトとは何ですか？

サイトとは、それ自体が親を持たない親機器モデルエンティティレコードのことです。サイトにアサインされた OT デバイスに読み取りまたは書き込みレベルのアクセスをアサインするために使用される、特別な機器モデルエンティティレコードです。

OT デバイスにサイトアサインと「`automates::automated by`」の両方の関係があるのはなぜですか？

サイトアサインは、OT デバイスのロールベースセキュリティ (RBAC) に必要です。OT デバイスは 1 つのサイトにのみ属することができるため、これは OT デバイスレコードの OT デバイスの詳細 (`cmdb_ot_entity`) テーブル部分の選択リスト参照フィールドとして実装されます。

`automates::automated by` 関係は、OT デバイスが本番プロセスにどのように関連しているかを示します。本番プロセスには、複数の機器モデルエンティティが含まれることがあります。

OT ネットワーク上と IT ネットワーク上の Windows サーバーの違いは何ですか？

どちらのタイプのネットワークでも、Windows サーバーは `cmdb_ci_win_server` サーバーで表されます。さらに、OT ネットワーク内の Windows サーバーの `[cmdb_ci_win_server.cmdb_ot_entity]` フィールドにある参照は、OT での機能と、その他の OT 特性 (Purdue レベル、サイトなど) を記述する `cmdb_ot_entity` テーブル内のレコードに向けたものです。

オペレーショナルテクノロジー (OT) 拡張クラスのインストール

オペレーショナルテクノロジーマネージャー の基盤となる オペレーショナルテクノロジー (OT) 拡張クラスをインストールする必要があります。

OT 拡張クラスにアクセスするには、CMDB CI クラスモデル アプリケーションをインストールします。インストールの詳細については、「[CMDB CI クラスモデル](#)」を参照してください。

OT 拡張クラスモデルは、次の情報を含む 構成管理データベース (CMDB) クラス階層を拡張します。

- クラスの説明
- 識別ルール
- 識別子エントリ
- 該当する場合、依存関係

ディスカバリー や サービスグラフコネクタ などのアプリケーションは、これらのクラス拡張を使用して構成アイテム (CI) を入力し、さまざまなテクノロジーやソフトウェアを検出します。OT 拡張クラスの詳細については、「[オペレーショナルテクノロジー \(OT\) 拡張クラス](#)」を参照してください。

オペレーショナルテクノロジーマネージャー のインストール

管理者ロールをお持ちであれば、オペレーショナルテクノロジーマネージャー アプリケーションをインストールできます。このアプリケーションには、デモデータが含まれています。まだインストールされていない場合は、関連する ServiceNow Store アプリケーションとプラグインをインストールします。

始める前に

- アプリケーションとその関連するすべての ServiceNow Store アプリケーションに有効な ServiceNow エンタイトルメントがあることを確認してください。詳細については、次を参照してください。 [エンタイトルメントを取得する ServiceNow 製品またはアプリケーション](#)。

i 注: オペレーショナルテクノロジーマネージャーに必要なサブスクリプションの詳細については、「[オペレーショナルテクノロジー管理 \(OTM\) のサブスクリプション](#)」を参照してください。

必要なロール: admin

このタスクについて

オペレーショナルテクノロジーマネージャー とともに次のアイテムがインストールされます。

- プラグイン
- ストアアプリケーション
- ロール
- テーブル
- スクリプトインクルード

オペレーショナルテクノロジーマネージャーとともにインストールされているコンポーネントの表示の詳細については、「[オペレーショナルテクノロジーマネージャーとともにインストールされるコンポーネント](#)」を参照してください。

手順

1. 移動先 **すべて > システムアプリケーション > 利用可能なすべてのアプリケーション > すべて**。
2. フィルター基準と検索バーを使用して オペレーショナルテクノロジーマネージャー アプリケーションを検索します。

名前または ID でアプリケーションを検索できます。アプリケーションが見つからない場合は、ServiceNow Store への要求が必要になることがあります。

ServiceNow Store Web サイトにアクセスして利用可能なすべてのアプリを表示し、ストアにリクエストを送信する方法について確認してください。リリースされたすべてのアプリのリリースノート情報については、「**ServiceNow Storeバージョン履歴のリリースノート**」を参照してください。

3. アプリケーションのインストールダイアログボックスで、アプリケーションの依存関係を確認します。

依存するプラグインとアプリケーションがインストールされる場合、現在インストールされている場合、またはインストールする必要がある場合は、表示されます。インストールする必要があるプラグインまたはアプリケーションがある場合は、オペレーショナルテクノロジーマネージャー をインストールする前にインストールする必要があります。

4. オプション: 利用できるデモデータをインストールするには、[デモデータのロード] チェックボックスをオンにします。

デモデータは、一般的なユースケース向けのアプリケーション機能を説明するサンプルレコードです。開発またはテストインスタンスで初めてアプリケーションをインストールする場合は、デモデータを読み込みます。

5. **[Install (インストール)]** を選択します。

インストールされたスクリプトインクルード オペレーショナルテクノロジーマネージャー

オペレーショナルテクノロジーマネージャー プラグインは、次のスクリプトインクルードをインストールします。

名前	説明
ベースダオ	すべての DAO クラスが拡張する必要がある基本 DAO クラス。
NIDSUtil	cmdb_ci_nids デバイスのユーティリティ。
OTDevicesMigrationUtil	指定したクラスから更新されたクラステーブルにレコードを移行します。詳細については、次を参照してください。 オペレーショナルテクノロジー (OT) 拡張クラス 。
OT デバイス	[cmdb_ot_entity] テーブルおよび関連する [cmdb_ci] および [cmdb_rel_ci] テーブルに対して操作を実行するための実装クラス。
OTDeviceDAO	オペレーショナルテクノロジー (OT) ネットワークデバイスの IT ディスカバリーの使用を支援するユーティリティ。
OTBaseDAO	OT のすべての DAO クラスが拡張する必要がある基本 DAO クラス。
OTFoundationConstant	他のスクリプトインクルードによって使用される定数のコレクション。
OTUtil	OT ユーティリティメソッドのコレクション。
SGOTDeviceConstants	OT サービスグラフコネクタで使用される定数のコレクション。

名前	説明
SGOTDeviceTransformUtil	OT サービスグラフコネクタの変換ユーティリティメソッドのコレクション。
SGOTDataStreamBase	指定された入力で特定のデータストリームを呼び出すベースパターン。
SGOTTroubleShootHelper	サービスグラフコネクタ構成を検証するためのヘルパーメソッド。
OTAssetFilterAjax	産業用ワークスペース の [すべての OT デバイス] リストビューからアプリケーションレコードと OT コントロールモジュールを除外するユーティリティクライアントスクリプト。
OTBulkEditHandler	フローアクションとスケジュール済みジョブによってトリガーされる IT から OT への一括編集(変換) と OT デバイス詳細の一括編集を処理するサーバー側スクリプト。
拡張ポイント	
SGOTDeviceImportExtensionPoint	次の 2 つのメソッドを含む SG OT デバイスインポート拡張ポイント:1. getDeviceCMDBClassNameWithSysId;2. getComputerType。

オペレーショナルテクノロジーマネージャー ロールの割り当て

ユーザーにロールをアサインすると、オペレーショナルテクノロジーマネージャー アプリケーションの各機能やデータへのアクセスを制御できます。

始める前に

必要なロール: admin

このタスクについて

次のテーブルにリストされているロールを持つユーザーは、オペレーショナルテクノロジーマネージャー アプリケーションを使用できます。

サイト ユーザーを構成する場合は、機器モデル エンティティ サイト ユーザーのユーザー基準を作成して割り当てることができます。詳細については、「[アドミニストレーター以外の機器モデルサイトアクセスの割り当てまたは削除](#)」を参照してください。

ロール	説明
オペレーショナルテクノロジー ディスカバリー アドミニストレーター [ot_discovery_admin]	オペレーショナルテクノロジープロセスのディスカバリーを実行できますが、構成管理データベース (CMDB)にアクセスして、検出されたアイテムから作成された構成アイテム (CI) および関連 オペレーショナルテクノロジー (OT) エンティティを表示することはできません。詳細については、「 オペレーショナルテクノロジー ディスカバリースケジュールを作成し、ディスカバリープロセスを実行します 」を参照してください。
オペレーショナルテクノロジーマネージャー ビューアー [cmdb_ot_viewer]	オペレーショナルテクノロジー(OT) デバイスレコードへの読み取り専用アクセス。

ロール	説明
オペレーショナルテクノロジーマネージャー エディター [cmdb_ot_editor]	運用テクノロジー (OT) 拡張クラス の作成、読み取り、更新、および削除アクセス権。 注: cmdb_ot_editor ロールを割り当てられたユーザーは、OT 構成アイテム (CI) のみを編集および削除でき、IT CI を編集することはできません。
オペレーショナルテクノロジーマネージャー アドミン [cmdb_ot_admin]	オペレーショナルテクノロジー (OT) デバイスレコードの作成、読み取り、更新、および削除アクセス権。OT エンティティタイプ内の特定の構成を編集および管理することもできます。詳細については、「運用テクノロジー (OT) 拡張クラス」を参照してください。 注: cmdb_ot_admin ロールをアサインされたユーザーは、OT 構成アイテム (CI) のみを編集および削除でき、IT CI を編集することはできません。

手順

ServiceNow AI Platform ユーザー管理機能を使用して、ユーザーとグループにロールをアサインします。

タスク	ユーザー管理機能
ユーザーへのロールのアサイン	ユーザーへのロールの割り当て を参照してください。
グループへのロールのアサイン	グループへのロールのアサイン を参照してください。

オペレーショナルテクノロジーマネージャー 統合

オペレーショナルテクノロジーマネージャー アプリケーションには、サードパーティ統合のサポートが入っています。

現在、下記のサードパーティー統合をサポートしています。

- Claroty CTD のサービスグラフコネクタ統合
- サービスグラフ コネクタ Microsoft Defender for IoT (Azure)
- サービスグラフ Connector for Microsoft Defender for IoT (オンプレミス管理コンソール)

Claroty CTD のサービスグラフコネクタ統合

Claroty Continuous Threat Detection (CTD) を ServiceNow オペレーショナルテクノロジーマネージャー アプリケーションと統合して、検出されたデバイスと Claroty CTD サイト (センサーまたはネットワーク侵入検知システムアプライアンス) をインポートします。

ストアでアプリを要求する

ServiceNow Store Web サイトにアクセスして、利用可能なすべてのアプリを表示し、要求をストアに送信する方法について確認してください。リリースされたすべてのアプリのこれまでのリリースノート情報については、「**ServiceNow Store のバージョン履歴リリースノート**」を参照してください。

サポート対象のバージョン

Claroty CTDバージョン:

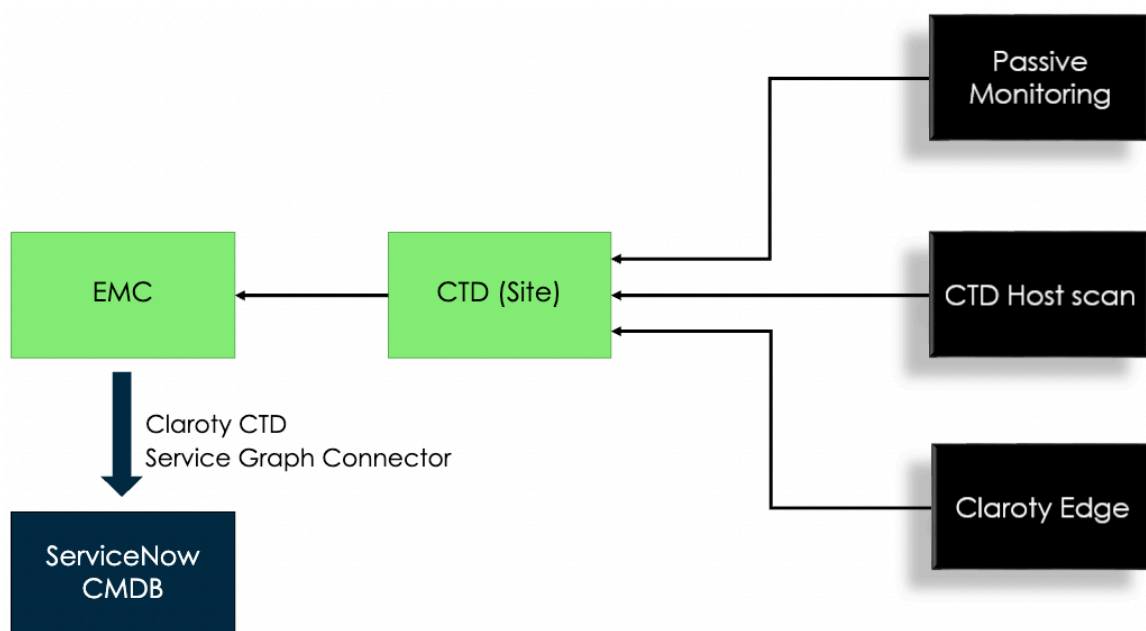
- 4.4.3 以降
- 5.1

ユースケース

オペレーショナルテクノロジーマネージャーアプリケーションでClaroty Continuous Threat Detection のサービスグラフコネクタ統合を使用して、次の情報をインポートします構成管理データベース (CMDB)

- 拠点
- 各サイトで検出されたデバイス
- 接続 (またはベースライン)
- インストール済みプログラム

次の図は、Claroty CTD データを CMDBにインポートするための検出方法を示しています。



ガイド付きセットアップ

Claroty CTD のサービスグラフコネクタ統合 のガイド付きセットアップでは、インスタンスの統合を構成するための、整理され順序の付いたタスクが用意されています。ガイド付きセットアップにアクセスするには、「**ガイド付きセットアップの構成**」を参照してください。

CMDB 統合ダッシュボード

CMDB 共通統合 ストアアプリは、インストールされているすべての統合のステータス、処理結果、および処理エラーを一元的に表示するダッシュボードを提供します。すべての統合実行のメトリクスを確認することができます。特定の CMDB 統合、特定の期間、または特定の統合実行に関してビューをフィルタリングすることもできます。CMDB 統合ダッシュボードでの統合の監視の詳細については、「[CMDB 共通統合](#)」を参照してください。

データマッピング

Claroty CTD データソースのデータは、強力な変換エンジン (RTE) を使用してマッピングされ、ServiceNow CMDB 構成アイテム (CI) クラス定義に変換されます。データは、識別および調整エンジン (IRE) を使用して ServiceNow CMDB に挿入されます。

次の表に、Claroty CTD のサービスグラフコネクタ統合に含まれるデータソースと、インポートされたデータがロードされる対応するステージングテーブルを示します。

Claroty CTD のデータソースとステージングテーブル

データソース	ステージングテーブル
SG-OT Claroty CTD デバイス	SG-OT Claroty CTD デバイスのインポート [sn_clarotyctdsgc_sg_ot_claroty_ctd_devices_import]
SG-OT Claroty CTD ベースライン	SG-OT Claroty CTD ベースラインのインポート [sn_clarotyctdsgc_sg_ot_claroty_ctd_baselines_import]
SG-OT Claroty CTD プログラム	SG-OT Claroty CTD プログラムのインポート [sn_clarotyctdsgc_sg_ot_claroty_ctd_programs_import]
SG-OT Claroty CTD サイト	SG-OT Claroty CTD サイトのインポート [sn_clarotyctdsgc_sg_ot_claroty_ctd_sites_import]

ステージングテーブルからインポートされたデータは、次のターゲットテーブルに挿入されます。

- コンピューター [cmdb_ci_computer]
- ハードウェア [cmdb_ci_hardware]
- IP アドレス [cmdb_ci_ip_address]
- ネットワークアダプタ [cmdb_ci_network_adapter]
- OT デバイスの詳細 [cmdb_ot_entity]
- OT コントロールモジュール [cmdb_ci_ot_control_module]
- OT コントロールシステム [cmdb_ci_ot_control]
- シリアル番号 [cmdb_serial_number]

詳細については、「[対象となる CMDB クラス](#)」を参照してください。

のデフォルトクエリパラメーター Claroty CTD のサービスグラフコネクタ統合

デフォルトでは、Claroty CTD のサービスグラフコネクタ統合はクエリパラメーターフィルターとともに出荷されます。これらの値は、統合ハブエンタープライズパッケージのエンタイトルメント ServiceNow に基づいて変更できます。

Claroty CTD からデータのインポートを開始すると、Claroty CTD のサービスグラフコネクタ統合は次のテーブルにリストされているデフォルトのクエリパラメーターフィルターを使用します。

デフォルトクエリパラメーターフィルター

クエリパラメーターフィルター	値	説明
approved_exact	true	approved_exactの値が true に設定されているため、Claroty CTD の未承認のデバイスはインポートされません。
valid_exact	true	valid_exactの値が true に設定されているため、Claroty CTD の無効なデバイスはインポートされません。
special_hint_exact	0	Claroty CTD で 0 (ユニキャスト) に設定されていないアドレスタイプはインポートされません。
ghost_exact	false	Claroty CTD にゴーストとして分類されるデバイスがある場合、デフォルト値が false に設定されているため、Claroty CTD のサービスグラフコネクタ統合ではインポートされません。

Claroty CTD のサービスグラフコネクタ統合の構成

Claroty CTD のサービスグラフコネクタ統合 のガイド付きセットアップを使用して、統合ステップを進めます。

始める前に

依存関係と要件：

- 自動的にインストールされる [CMDB 共通統合](#) ストアアプリ。
- 自動的にインストールされる [CMDB CI クラスモデル](#)。
- ITOMディスカバリーライセンスプラグイン (com.snc.itom.discovery.license)。このプラグインを有効にする必要があります。
- ITOM Licensing プラグイン (com.snc.itom.license)。詳細については、「[ディスカバリーの要求](#)」を参照してください。
- 自動的にインストールされる Datastream Action プラグイン (com.glide.hub.action_type.datastream)。
- Claroty CTDからServiceNowにデータを収集するために、次のユーザー権限の表示アクセスがClaroty CTDで有効になっていることを確認します。
 - ヴィジビリティ
 - 調査
- Industrial Core プラグイン。このプラグインを有効にする必要があります。

Claroty CTD のサービスグラフコネクタ統合のクラスマッピングテーブルにアクセスするには、Industrial Core プラグインが必要です。Industrial Core プラグインの詳細については、「[Industrial Core プラグイン](#)」を参照してください。

必要なロール：admin

- i** 注: Claroty CTD のサービスグラフコネクタ統合 の以前のバージョンを使用している場合は、古いコネクタからデータを移行しないでください。以前のバージョンをアンインストールし、新しい統合を実行する必要があります。

手順

1. アプリケーションピッカーを使用して、アプリケーションが Claroty CTD のサービスグラフコネクタ統合 に設定されていることを確認します。
詳細については、「[アプリケーションピッカー](#)」を参照してください。
2. 移動先 すべて > サービスグラフコネクタ **Claroty CTD** > ガイド付きセットアップ。
3. [はじめに] ページで、[開始] を選択します。
4. MID サーバーを設定するには、次の手順を実行します。
 - a. [接続と認証情報のセットアップ] セクションで、[MID サーバーの構成] タスクを選択します。
 - b. MID サーバーの構成が完了したら、[完了としてマーク] を選択します。
5. 接続レコードを設定するには、次の手順を実行します。
 - a. [接続と資格情報のセットアップ] セクションで、[接続の構成] タスクを選択します。
 - b. [Configure] を選択します。
 - c. 接続テーブルで Claroty CTD API レコードを開きます。
 - d. [接続 URL] フィールドに、Claroty CTD Enterprise 管理コンソール (EMC) の URL の名前を入力します。
<https://192.168.1.100> など。
 - e. MID サーバーを使用している場合は、レコードの **[MID サーバーを使用]** チェックボックスをオンにします。

i 注: MID サーバーを使用していない場合は、手順 5g に進みます。

 - f. [詳細設定 MID サーバー] 関連リストから、MID サーバー と [MID 選択] を選択します。
 - g. [Update (更新)] を選択します。
 - h. 手順 5a ~ 5h を繰り返して、**Claroty CTD EMC Base** 認証 レコードを更新します。
6. 認証情報レコードを設定するには、次の手順を実行します。
 - a. [接続と認証情報のセットアップ] セクションで、[認証情報の構成] タスクを選択します。
 - b. [Configure] を選択します。
 - c. 認証情報テーブルで Claroty CTD EMC Base 認証レコードを開きます。
 - d. [ユーザー名] フィールドに、Claroty CTD EMC へのログインに使用したユーザー名を入力します。
 - e. [パスワード] フィールドに、Claroty CTD EMC へのログインに使用したパスワードを入力します。
 - f. [Update (更新)] を選択します。
7. 接続をテストするには、次の手順を実行します。

- a. [接続と資格情報のセットアップ] セクションで、[接続のテスト/検証] タスクを選択します。
- b. センサーのデータソースレコードの関連リンクセクションから [テスト接続] UI アクションを選択します。
接続テストが完了したら、結果を表示します。テスト結果が「成功」を返すまで、推奨されるトラブルシューティング手順を実行する必要があります。
- c. 接続マネージャーに有効な証明書があることを確認してください。

本番環境には有効な証明書をインストールする必要があります。非本番インスタンスまたは概念実証 (POC) インスタンスの場合、接続マネージャーに有効な証明書がない場合に統合が機能するようにシステムプロパティを構成できます。次の表に、非本番環境で構成できるシステムプロパティを示します。

非本番環境のシステムプロパティ

プロパティ	値
com.glide.communications.httpclient.verify_certificate	false に設定します。
com.glide.communications.httpclient.verify_certificate	false に設定します。
	このシステムプロパティを追加する必要がある場合は、「 システムプロパティの追加 」を参照してください。
com.glide.communications.trustmanager_trustAll	true に設定します。

- d. MID セキュリティポリシーを確認します。
イントラネットレコードで、次の表の列に指定された値が表示されていることを確認します。

イントラネットレコード値

列	値
証明書チェーンチェック	誤り
ホスト名チェック	誤り
失効チェック	誤り

詳細については、「[MID サーバー証明書チェックポリシー](#)」を参照してください。

8. API リソースパス、ページネーションサイズ、および API キーの有効期限を構成するシステムプロパティを設定するには、次の手順を実行します。
 - a. [システムプロパティの構成] セクションで、[構成] を選択します。
 - b. 次のテーブルのシステムプロパティを構成します。

プロパティ	説明
sn_clarotyctdsgc.resourcepath.site	サイトのリソースパスを設定するプロパティ:

プロパティ	説明
	i 注: サイトのリソースパスは、CTD サイトおよびデバイスの Claroty CTD Enterprise 管理コンソール (EMC) V4.4.3 API バージョンにデフォルトで提供されます。 別の API バージョンを使用する場合は、パスを上書きできます。
sn_clarotyctdsgc.resourcepath.device	デバイスのリソースパスを設定するプロパティ: i 注: デバイスのリソースパスは、CTD サイトおよびデバイスの CTD EMC V4.4.3 API バージョンにデフォルトで提供されます。 別の API バージョンを使用する場合は、パスを上書きできます。
sn_clarotyctdsgc.pagesize.device	Claroty CTD EMC へのページネーション REST 呼び出しでフェッチするデバイスレコードの数を設定するプロパティ。デフォルト値は 1 ページあたり 500 レコードです。 i 注: ページあたりのデバイスの最大数は 500 です。
sn_clarotyctdsgc.resourcepath.baseline	ベースラインのリソースパスを設定するプロパティ: i 注: ベースラインのリソースパスは、CTD サイトおよびデバイスの CTD EMC V4.4.3 API バージョンにデフォルトで提供されます。 別の API バージョンを使用する場合は、パスを上書きできます。
sn_clarotyctdsgc.pagesize.baseline	Claroty CTD EMC へのページネーション REST 呼び出しでフェッチするベースラインレコードの数を設定するプロパティ。デフォルト値は 1 ページあたり 500 レコードです。
sn_clarotyctdsgc.get_all_baselines	ベースラインのすべてのレコードをフェッチするか、最後に成功したインポートの開始時刻以降の新しいレコードのみをフェッチするプロパティ。

プロパティ	説明
	i 注: ベースラインを初めてインポートすると、このプロパティの設定に関係なく、すべてのレコードがインポートされます。
sn_clarotyctdsgc.resourcepath.entity	エンティティのリソースパスを設定するプロパティ: i 注: エンティティのリソースパスは、CTD サイトおよびデバイスの CTD EMC V4.4.3 API バージョンにデフォルトで提供されます。別の API バージョンを使用する場合は、パスを上書きできます。
sn_clarotyctdsgc.resourcepath.program	インストール済みプログラムのリソースパスを設定するプロパティ: i 注: インストール済みプログラムのリソースパスは、CTD サイトおよびデバイスの CTD EMC V4.4.3 API バージョンにデフォルトで提供されます。 別の API バージョンを使用する場合は、パスを上書きできます。
sn_clarotyctdsgc.pagesize.entity	Claroty CTD EMC へのページネーション REST 呼び出しでフェッチするエンティティレコードの数を設定するプロパティ。デフォルト値は 1 ページあたり 500 レコードです。
sn_clarotyctdsgc.pagesize.program	Claroty CTD EMC へのページネーション REST 呼び出しでフェッチするプログラムレコードの数を設定するプロパティ。デフォルト値は 1 ページあたり 500 レコードです。
sn_clarotyctdsgc.api_token_life_in_minutes	API がアクティブと見なされる時間を分単位で設定するプロパティ。時間が経過すると、サービスグラフコネクタは次のインポート時に新しい API キーをフェッチします。デフォルト値は 0 で、REST 呼び出しごとに新しいトークンがフェッチされます。 i 注: 同じトークンを最大 24 時間保持するように値を変更して、REST コールの数を減らすことができます。

プロパティ	説明
sn_clarotyctdsgc.classify_based_on_os	Claroty CTD のサービスグラフコネクタ統合の一部として OS による分類をサポートするクラスのリストを提供するプロパティ。 フラグが True に設定されている場合、OS 別の分類がサポートされます。False に設定すると、サービスグラフコネクタは OS 別に分類されなくなります。たとえば、次のようになります。 <pre>{ "cmdb_ci_ip_switch":true, "cmdb_ci_nids":false }</pre>
sn_clarotyctdsgc.filter.asset_type_code	区切り文字 (\$) で区切られたデバイスタイプのコードのリストを提供するプロパティ。 Claroty のタイプとコードの詳細については、「対象となる CMDB クラス」を参照してください。たとえば、PLC および HMI デバイスタイプのみをインポートするには、Claroty タイプコードを 0\$1 として入力します。
sn_clarotyctdsgc.filter.asset_purdue_level	区切り文字 (\$) で区切られた Purdue レベルのリストを提供するプロパティ。たとえば、Purdue レベル 1 と 2 のデバイスのみをフィルター処理するには、Purdue レベル 1 と 2 のデバイスのみをフィルター処理するには、値を 1.0\$2.0 に設定します。

c. **[Save (保存)]** を選択します。

9. CTD サイトをインポートするには、次の手順を実行します。

- a. [CTD サイトを構成] セクションで、[CTD サイトをインポート] タスクを選択します。
- b. **[Configure]** を選択します。
- c. [今すぐ実行] ボタンを選択します。

10. ネットワーク侵入検知システム (NIDS) を構成するには、次の手順を実行します。

- a. [CTD サイトの構成 (Configure CTD sites)] セクションで、[NIDS の構成 (Configure NIDS)] タスクを選択します。
- b. Claroty CTD からデバイスを取得するために使用する NIDS をセットアップしたら、「完了としてマーク」を選択します。

11. サイト、デバイス、ベースライン、およびインストール済みプログラムを実行するようにインポートスケジュールを設定するには、次の手順を実行します。

i 注: PLC に関連付けられている空のラックスロットは、構成管理データベース (CMDB) にインポートされなくなりました。

- a. [インポートスケジュールの構成] セクションで、[サイトインポートスケジュールの構成] タスクを選択します。

b. **[Configure]** を選択します。

- c. [予定されているデータインポート] テーブルで、[**SG-OT CTD** サイトのスケジュール済みインポート] を選択します。
- デフォルトでは、サイトインポートスケジュールは毎日深夜に実行されるように構成されています。
 - デバイスをインポートする前に、CTD サイトをインポートして検証する必要があります。
- d. 必要に応じて次のアクションを実行し、必要に応じてインポートスケジュールを確認または変更します。

アクション	説明
条件付きスクリプトを入力	[条件付き] を選択して、スケジュール済みインポートを実行するかどうかを決定する条件スクリプトを入力します。
デフォルトのインポートスケジュールを変更する	必要に応じて [実行] フィールドを設定して、デフォルトのインポートスケジュールを変更します。
ユーザーテーブルでのユーザーの参照	[実行方法] フィールドでユーザーを選択して、[ユーザー] テーブルでユーザーを参照します。 i 注: デフォルトでは、このフィールドは [システムアドミニストレーター] に設定されています。インポートを成功させるには、選択したユーザーに admin ロールがアサインされている必要があります。空のままの場合、インポートスケジュールはログインしているユーザーのロールを使用します。
インポートを実行	[今すぐ実行] を選択してインポートを実行します。構成されたシステムプロパティに基づいて、すべてのレコードまたは前回成功したインポートの開始時刻以降の新しいレコードのみをインポートできます。詳細については、「 ガイド付きセットアップの構成 」を参照してください。
インポートを有効にする	[アクティブ] チェックボックスをオンにして、インポートをアクティブ化します。
スケジュールの変更の保存	[更新] を選択して、スケジュールの変更を保存します。

- e. [インポートスケジュールの構成 (Configure Import Schedules)] セクションで、[デバイスインポートスケジュールの構成 (Configure Devices Import Schedule)] タスクを選択します。
- f. [Configure] を選択します。

- g. [予定されているデータインポート] テーブルで、[**SG-OT CTD** デバイスのスケジュール済みインポート] を選択して、デバイスのインポートスケジュールを確認または変更します。
- デフォルトでは、デバイスのインポートスケジュールは毎日深夜に実行されるように設定されています。
 - デバイスは CTD サイトによって照会されます。サービスグラフコネクタは、検証済みの CTD サイトによって検出されたデバイスのみクエリを実行します。
- h. 必要に応じて次のアクションを実行し、必要に応じてインポートスケジュールを確認または変更します。

アクション	説明
条件付きスクリプトを入力	[条件付き] を選択して、スケジュール済みインポートを実行するかどうかを決定する条件スクリプトを入力します。
デフォルトのインポートスケジュールを変更する	必要に応じて [実行] フィールドを設定して、デフォルトのインポートスケジュールを変更します。
ユーザーテーブルでのユーザーの参照	[実行方法] フィールドでユーザーを選択して、[ユーザー] テーブルでユーザーを参照します。 i 注: デフォルトでは、このフィールドは [システムアドミニストレーター] に設定されています。インポートを成功させるには、選択したユーザーに admin ロールがアサインされている必要があります。空のままの場合、インポートスケジュールはログインしているユーザーのロールを使用します。
インポートを実行	[今すぐ実行] を選択してインポートを実行します。構成されたシステムプロパティに基づいて、すべてのレコードまたは前回成功したインポートの開始時刻以降の新しいレコードのみをインポートできます。詳細については、「 ガイド付きセットアップの構成 」を参照してください。
インポートを有効にする	[アクティブ] チェックボックスをオンにして、インポートをアクティブ化します。
スケジュールの変更の保存	[更新] を選択して、スケジュールの変更を保存します。

- i. [インポートスケジュールの構成] セクションで、[ベースラインインポートスケジュールの構成] タスクを選択します。

- j. [Configure] を選択します。

- k. [スケジュール設定済みデータインポート] テーブルで、[**SG-OT CTD** ベースラインのインポートスケジュール済みインポート] を選択して、ベースラインのインポートスケジュールを確認または変更します。
デフォルトでは、ベースラインインポートスケジュールは、親 OT コントロールシステムの実行後に実行されるように構成されています。
- l. 必要に応じて次のアクションを実行し、必要に応じてインポートスケジュールを確認または変更します。

アクション	説明
条件付きスクリプトを入力	[条件付き] を選択して、スケジュール済みインポートを実行するかどうかを決定する条件スクリプトを入力します。
デフォルトのインポートスケジュールを変更する	必要に応じて [実行] フィールドを設定して、デフォルトのインポートスケジュールを変更します。
ユーザーテーブルでのユーザーの参照	[実行方法] フィールドでユーザーを選択して、[ユーザー] テーブルでユーザーを参照します。 <i>i</i> 注: デフォルトでは、このフィールドは [システムアドミニストレーター] に設定されています。インポートを成功させるには、選択したユーザーに admin ロールがアサインされている必要があります。空のままの場合、インポートスケジュールはログインしているユーザーのロールを使用します。
インポートを実行	[今すぐ実行] を選択してインポートを実行します。構成されたシステムプロパティに基づいて、すべてのレコードまたは前回成功したインポートの開始時刻以降の新しいレコードのみをインポートできます。詳細については、「 ガイド付きセットアップの構成 」を参照してください。
インポートを有効にする	[アクティブ] チェックボックスをオンにして、インポートをアクティブ化します。
スケジュールの変更の保存	[更新] を選択して、スケジュールの変更を保存します。

- m. [インポートスケジュールの構成 (Configure Import Schedules)] セクションで、[サイトのインストール済みプログラムのインポートスケジュールの構成 (Configure Sites Installed Programs Import Schedule)] タスクを選択します。
- n. [Configure] を選択します。

- o. [予定されているデータインポート] テーブルで、[**SG-OT CTD** インストール済みプログラムのインポートスケジュール] を選択して、インストール済みプログラムのインポートのスケジュールを確認または変更します。
デフォルトでは、インストール済みプログラムのインポートスケジュールは、毎日深夜に実行されるように設定されています。
- p. 必要に応じて次のアクションを実行し、必要に応じてインポートスケジュールを確認または変更します。

アクション	説明
条件付きスクリプトを入力	必要に応じて [実行] フィールドを設定して、デフォルトのインポートスケジュールを変更します。
デフォルトのインポートスケジュールを変更する	必要に応じて [実行] フィールドを設定して、デフォルトのインポートスケジュールを変更します。
ユーザーテーブルでのユーザーの参照	[実行方法] フィールドでユーザーを選択して、[ユーザー] テーブルでユーザーを参照します。 i 注: デフォルトでは、このフィールドは [システムアドミニストレーター] に設定されています。インポートを成功させるには、選択したユーザーに admin ロールがアサインされている必要があります。空のままの場合、インポートスケジュールはログインしているユーザーのロールを使用します。
インポートを実行	[今すぐ実行] を選択してインポートを実行します。構成されたシステムプロパティに基づいて、すべてのレコードまたは前回成功したインポートの開始時刻以降の新しいレコードのみをインポートできます。詳細については、ステップ 7c を参照してください。
インポートを有効にする	[アクティブ] チェックボックスをオンにして、インポートをアクティブ化します。
スケジュールの変更の保存	[更新] を選択して、スケジュールの変更を保存します。

12. オプション: CMDBで構成アイテム (CI) が作成されると、資産レコードが作成されます。資産レコードには、CI のモデルカテゴリが含まれています。オペレーショナルテクノロジー (OT) のモデルカテゴリの詳細については、「[のモデルカテゴリ オペレーショナルテクノロジー](#)」を参照してください。OT デバイスのモデルカテゴリを表示するには、次の手順を実行します。
- a. 移動先 **すべて > オペレーショナルテクノロジー (OT) > すべての OT デバイス**。
- b. 資産レコードを表示する OT デバイスを選択します。

c. [資産] フィールドの横にある [このレコードをプレビュー] アイコン () を選択します。

d. [レコードを開く (**Open Record**)] を選択します。

13. オプション: Claroty CTD のサービスグラフコネクタ統合のトラブルシューティングを行うには、次の手順を実行します。

a. [オプション] Claroty CTD のサービスグラフコネクタのトラブルシューティングセクションを選択します。

b. [検証スケジュール済みジョブを実行] タスクで、[構成] を選択します。

c. **[Execute Now (今すぐ実行)]** を選択します。

このジョブは、SGC の構成と Claroty CTD への接続を検証するタスクを実行します。構成の問題が見つかった場合、検証結果に問題が報告され、トラブルシューティング手順が提案されます。スケジュール済みジョブが終了するまで待ちます。

d. スケジュール済みジョブが完了したら、「[オプション] Claroty CTD のサービスグラフコネクタのトラブルシューティング」セクションに戻ります。

e. [検証結果のレビュー] タスクで、[構成] を選択します。

このステップでは、前回のトラブルシューティング実行の実行ログと提案が開き、表示されます。

f. 必要に応じて提案に対処します。

 注: スケジュール設定済みスクリプトは、Claroty CTD のサービスグラフコネクタ統合の初期構成後であればいつでも使用できます。検証をトリガーするには、次に移動します: すべて > **Claroty CTD** のサービスグラフコネクタ > トラブルシューティング > トラブルシューティングの実行. 検証結果を表示するには、次に移動します: すべて > **Claroty CTD** のサービスグラフコネクタ > トラブルシューティング > 結果.

Claroty CTD のサービスグラフコネクタ統合使用中の問題のトラブルシューティングの詳細については、以下を参照してください。 [Claroty CTD \(KB1502041\) のサービスグラフコネクタ統合のトラブルシューティングシナリオ](#)  .

NIDS センサーの検証

インポートされたネットワーク IDS (NIDS) センサーを検証して、デバイスのインポートに備えます。センサーはデバイスインポートの対象ではないため、センサーはラーニングモードでない場合にのみ検証に合格できます。

始める前に

CSDM プラグインをインストールすることをお勧めします。サービスグラフコネクタは、CMDB 標準に従ってライフサイクルデータモデルに適合します。詳細については、「[CSDM フレームワークを段階的に実装する](#)  」を参照してください。

必要なロール:cmdb_nids_admin

このタスクについて

[ライフサイクルステージ] フィールドと [ライフサイクルステージステータス] フィールドは、センサーの学習モードをキャプチャするために使用されます。[ライフサイクルステージ] フィールドが [運用] に設定され、かつ [ライフサイクルステージステータス] が [学習モード] に設定されている場合、検証は失敗します。[ライフサイクルステージステータス] フィールドが [使用中] に設定されている場合、検証は成功しています。

手順

1. 移動先 **すべて > ネットワーク IDS アプライアンス (NIDS) > センサー**。
2. 検証するセンサーレコードを選択します。
3. [NIDS アサインメタデータ (NIDS Assigned Meta Data)] セクションで、検出されたデバイスに割り当てたセンサーの値を追加します。
4. [NIDS アドミン構成] セクションで、[ライフサイクルステータス] フィールドの値が [学習モード] でないことを確認します。
それ以外の場合、検証は失敗します。
5. [**NIDS ネットワークタイプ**] フィールドが NIDS ネットワークの場所に基いて設定されていることを確認します。
たとえば、NIDS のデータセンター展開の場合は **NIDS ネットワークタイプ** の IT を選択し、産業用/OT ネットワークでの産業用展開の場合は **NIDS ネットワークタイプ** の OT を選択できます。

[OT] を選択すると、すべてのデバイスに対して OT デバイスの詳細が作成されます。
6. 属性が正しく入力されたら、[検証] を選択します。

i 注:

注意: センサーからデバイスに渡される属性は、sn_cmdb_ci_class.nids_map_fields システムプロパティで定義されます。次のリストは、属性のデフォルトのリストです。

- assigned_to
- 場所
- 会社
- owned_by
- managed_by
- supported_by
- change_control
- support_group
- managed_by_group
- assignment_group
- ゾーン
- isa_entity_site (製造業プロセスマネージャー アプリケーションがインストールされている場合のみ利用可能)

の接続の詳細へのアクセス **Claroty CTD** のサービスグラフコネクタ統合

CMDB 共通統合 (sn_cmdb_int_util) ストアアプリに含まれる共通接続フレームワーク (CCF) を使用して、単一のビューで Claroty CTD のサービスグラフコネクタ統合の接続の詳細にアクセスできます。

CCF を使用すると、Claroty CTD のサービスグラフコネクタ統合 で使用されるすべての接続にアクセスできます。接続の詳細には、接続エイリアス、接続のプロパティ、データソース、および接続に関連付けられたスケジュール設定済みデータインポートが含まれます。接続をテストすることもできます。詳細については、「[サービスグラフコネクタの接続の詳細へのアクセス](#)」を参照してください。

Claroty CTD 接続の詳細へのアクセス

Claroty CTD のサービスグラフコネクタ統合用に構成された Claroty CTD 接続の詳細にアクセスします。

始める前に

必要なロール：admin

このタスクについて

Claroty CTD のサービスグラフコネクタ統合データソース、システムプロパティ、およびスケジュール設定済みデータインポートに個別に移動するためのアプリケーションモジュールがあります。ただし、共通接続フレームワーク (CCF) を使用すると、Claroty CTD 用に作成されたすべての関連データソースとスケジュール設定済みデータインポートを 1 か所に集めることができます。関連リンクセクションを使用して、ソース (Claroty CTD) への接続をテストすることもできます。

手順

1. アプリケーションピッカーを使用して、アプリケーションスコープが **Claroty CTD** のサービスグラフコネクタ統合 アプリケーションに設定されていることを確認します。
2. 移動先 **すべて > Claroty CTD のサービスグラフコネクタ > Claroty CTD SGC 接続**.
3. [サービスグラフ接続] ページで、[**SG-OT Claroty CTD デフォルト接続 (SG-OT Claroty CTD Default Connection)**] を選択します。
4. オプション: システムのプロパティにアクセスするには、[サービスグラフ接続のプロパティ] タブを選択します。
5. オプション: データソースにアクセスするには、[サービスグラフ接続データソース] タブを選択します。
6. オプション: 予定されているデータインポートにアクセスするには、[サービスグラフ接続の予定されているデータインポート] タブを選択します。
7. オプション: Claroty CTD プラットフォームとの接続をテストするには、[テスト接続] 関連リンクを選択します。
接続はいつでもテストできます。接続テストが完了すると、同じページの [ステータス] と [提案] に、失敗したステップのトラブルシューティングのためのステータスと提案がそれぞれ表示されます。

CMDB での対象となるクラス **Claroty CTD** のサービスグラフコネクタ統合

セットアップタスクを完了したら、Claroty CTD からデータをプルするように統合を定期的に構成できます。データは、構成アイテム [cmdb_ci] テーブルから拡張されたテーブルに保存されます。

クラスマッピングの表示

Claroty CTD のサービスグラフコネクタ統合に利用可能なクラスマッピングを表示するには、次に移動します: **すべて > サービスグラフコネクタ Claroty CTD > クラスマッピング**. クラスマッピングテーブルでは、次の属性を表示できます。

クラスマッピング属性

フィールド	説明
ソースクラス	ソース CI のクラス。
ターゲット CMDB クラス	CI に予期される ServiceNow クラス。
OT デバイスタイプ	OT デバイスが分類されるカテゴリタイプ。デバイスタイプは、デバイスが OT ネットワーク上

クラスマッピング属性 (続く)

フィールド	説明
	で果たす機能でもあります。たとえば、次のようになります。 サーバーなどのIT機器はOT機器に変換でき、ネットワーク上で果たす機能はHMIです。したがって、そのクラスは server で、デバイスタイプは HMI です。 i 注: 場合によっては、OT 機能を持たない OT デバイスや、デバイスタイプが不明な OT デバイスがあります。OT 機能のない OT デバイスの場合は、[OT 機能なし] を選択します。デバイスタイプが不明な OT デバイスの場合は、[不明] を選択します。
OS 分類を許可	True に設定すると、CI でオペレーティングシステムが見つかった場合、ターゲットはターゲットの CMDB クラスからその OS に一致する ServiceNow クラスに切り替えられます。
アクティブ	オンにすると、クラスマッピングがアクティブに設定されます。

Claroty CTD のサービスグラフコネクタ統合 は Claroty のタイプとコードも使用します。詳細については、を参照してください。 [デフォルトのクラスマッピング](#) テーブルの AJAX 機能を提供します。

コンピューター [cmdb_ci_computer]

コンピューター [cmdb_ci_computer] テーブルの次の属性は、収集されたデータによって設定されます。

属性ラベル	属性の名前
最新のディスカバリー	last_discovered
オペレーティングシステム	os
OS バージョン	os_version

外部システムメタデータ [cmdb_key_value_v2]

外部システムメタデータ [cmdb_key_value_v2] テーブルの次の属性は、収集されたデータによって設定されます。

属性ラベル	属性の名前
ディスカバリーソース	discovery_source
キー	キー
ソースキー	source_key

属性ラベル	属性の名前
URL 値	url_value
値のタイプ	value_type

ファームウェアのインストール [cmdb_firmware_install]

ファームウェアインストール [cmdb_firmware_install] テーブルの次の属性は、収集されたデータによって設定されます。

属性ラベル	属性の名前
ソースネイティブキー	firmware_version_snk
IRE 基準属性	firmware_ire_criterion_key
検出されたバージョン	firmware_version_cleansed
ディスカバリーソース	firmware_version_discovery_source

ハードウェア [cmdb_ci_hardware]

ハードウェア [cmdb_ci_hardware] テーブルの次の属性は、収集されたデータによって設定されます。

属性ラベル	属性の名前
変更グループ	assignment_group
サポートグループ	support_group
会社	会社
ベンダー	ベンダー
名前	name
シリアル番号	serial_number
クラス	sys_class_name
最初の検出	first_discovered
場所	場所
モデル番号	model_number
最新検出日	last_discovered
サポート担当者	supported_by
アサイン先	assigned_to
グループによる管理	managed_by_group
管理担当者	managed_by
モデル ID	model_id
承認グループ	change_control
所有者	owned_by
メーカー	manufacturer

ハードウェアに対して作成された関係

親クラス	関係性タイプ	子クラス
ハードウェア [cmdb_ci_hardware]	Owens::Owned by	ネットワークアダプタ [cmdb_ci_network_adapter]
ハードウェア [cmdb_ci_hardware]	Owens::Owned by	IP アドレス [cmdb_ci_ip_address]
ハードウェア [cmdb_ci_hardware]	参照	OT デバイス [cmdb_ot_entity]
ハードウェア [cmdb_ci_hardware]	参照	外部システムメタデータ [cmdb_key_value_v2]
ハードウェア [cmdb_ci_hardware]	参照	ソフトウェアインストール [cmdb_sam_sw_install]

IP アドレス [cmdb_ci_ip_address]

IP アドレス [cmdb_ci_ip_address] テーブルの次の属性は、収集されたデータによって設定されます。

属性ラベル	属性の名前
構成アイテムによって所有されている	owned_by_cmdb_ci
IP アドレス	ip_address
IP バージョン	ip_version

IP アドレス用に作成された関係

親クラス	関係性タイプ	子クラス
IP アドレス [cmdb_ci_ip_address]		ネットワーク侵入検知システム [cmdb_ci_nids]
IP アドレス [cmdb_ci_ip_address]		ハードウェア [cmdb_ci_hardware]

ネットワークアダプタ [cmdb_ci_network_adapter]

ネットワークアダプタ [cmdb_ci_network_adapter] テーブルの次の属性は、収集されたデータによって設定されます。

属性ラベル	属性の名前
MAC アドレス	mac_address
名前	名前

ネットワークアダプタ用に作成された関係

親クラス	関係性タイプ	子クラス
ネットワークアダプタ [cmdb_ci_network_adapter]	参照	ハードウェア [cmdb_ci_hardware]

ネットワーク侵入検知システム [cmdb_ci_nids]

ネットワーク侵入検知システム [cmdb_ci_nids] テーブルの次の属性は、収集されたデータによって設定されます。

属性ラベル	属性の名前
メーカー	manufacturer
名前	name
相関 ID	correlation_id
説明	short_description
ファームウェアバージョン	firmware_version
NIDS マネージャー接続ステータス	connection_state
ライフサイクルステージステータス	life_cycle_stage_status
Life Cycle Stage (ライフサイクルステージ)	life_cycle_stage
検証済み	検証済み

NIDS 用に作成された関係

親クラス	関係性タイプ	子クラス
ネットワーク侵入検知システム [cmdb_ci_nids]	Owns::Owned by	IP アドレス [cmdb_ci_ip_address]
ネットワーク侵入検知システム [cmdb_ci_nids]	検出::Detected	ハードウェア [cmdb_ci_hardware]

オペレーショナルテクノロジー (OT) [cmdb_ci_ot]

オペレーショナルテクノロジー (OT) [cmdb_ci_ot] テーブルの次の属性は、収集されたデータによって設定されます。

属性ラベル	属性名
ファームウェアバージョン	firmware_version
最新検出日	last_discovered

OT デバイス [cmdb_ot_entity]

OT デバイス [cmdb_ot_entity] テーブルの次の属性は、収集されたデータによって設定されます。

属性ラベル	属性の名前
Purdue レベル	purdue_level
ISA エンティティサイト	isa_entity_site
OT ディスカバリーソース ID	ot_correlation_id
デバイスの重要度	business_criticality
ゾーン	ゾーン
OT デバイスタイプ	ot_asset_type
IRE 基準属性	ire_criterion_attribute

OT コントロールモジュール [cmdb_ci_ot_control_module]

OT コントロールモジュール [cmdb_ci_ot_control_module] テーブルの次の属性は、収集されたデータによって設定されます。

属性ラベル	属性の名前
場所	場所
サポート担当者	supported_by
名前	name
シリアル番号	serial_number
スロット番号	slot_number
メーカー	メーカー
ファームウェアバージョン	firmware_version
承認グループ	change_control
アサイン先	assigned_to
最新のディスカバリー	last_discovered
モデル ID	model_id
モデル番号	model_number
会社	会社
所有者	owned_by
管理担当者	managed_by
サポートグループ	support_group
グループによる管理	managed_by_group
変更グループ	assignment_group
ベンダー	ベンダー

OT コントロールモジュール用に作成された関係

親クラス	関係性タイプ	子クラス
OT コントロールモジュール [cmdb_ci_ot_control_module]	参照	OT デバイス [cmdb_ot_entity]

OT コントロールシステム [cmdb_ci_ot_control]

OT コントロールシステム [cmdb_ci_ot_control] テーブルの次の属性は、収集されたデータによって設定されます。

属性ラベル	属性の名前
モジュールあり	has_module
最新検出日	last_discovered

OT コントロールシステム用に作成された関係

親クラス	関係性タイプ	子クラス
OT コントロールシステム [cmdb_ci_ot_control]	Owens::Owned by	OT コントロールモジュール [cmdb_ci_ot_control_module]

シリアル番号 [cmdb_serial_number]

シリアル番号 [cmdb_serial_number] テーブルの次の属性は、収集されたデータによって設定されます。

- i** 注: サービスグラフコネクタからsys_object_sourceテーブルにインポートされたシリアル番号 [cmdb_serial_number] レコードをクリーンアップするために、修正スクリプトが自動的に適用されます。このスクリプトにより、シリアル番号と MAC アドレスが同じ場合に null ポインター例外が発生しないようにします。

この修正スクリプトは、Claroty CTD のサービスグラフコネクタ統合 のアップグレード中に一度だけ実行されますが、zboot インスタンスまたは新規インストールでは実行されません。これにより、機能に影響したり、データが失われたりすることはありません。

属性ラベル	属性の名前
シリアル番号	serial_number
シリアル番号タイプ	serial_number_type
有効	valid

シリアル番号用に作成された関係

親クラス	関係性タイプ	子クラス
シリアル番号 [cmdb_serial_number]	参照	ハードウェア [cmdb_ci_hardware]

ソフトウェア [cmdb_ci_spkg]

ソフトウェア [cmdb_ci_spkg] テーブルの次の属性は、収集されたデータによって設定されます。

属性ラベル	属性の名前
キー	key
バージョン	version
メーカー	manufacturer
名前	名前

ソフトウェア用に作成された関係

親クラス	関係性タイプ	子クラス
ソフトウェア [cmdb_ci_spkg]	参照	ソフトウェアインスタンス [cmdb_software_instance]

ソフトウェアインスタンス [cmdb_software_instance]

ソフトウェアインスタンス [cmdb_software_instance] テーブルの次の属性は、収集されたデータによって設定されます。

属性ラベル	属性の名前
インストール日	install_date
インストール先	installed_on
名前	name

ソフトウェアインスタンス用に作成された関係

親クラス	関係性タイプ	子クラス
ソフトウェアインスタンス [cmdb_software_instance]	参照	ハードウェア [cmdb_ci_hardware]

ソフトウェアインストール [cmdb_sam_sw_install]

ソフトウェアインストール [cmdb_sam_sw_install] テーブルの次の属性は、収集されたデータによって設定されます。

属性ラベル	属性の名前
表示名	display_name
バージョン	version
ディスカバリーソース	discovery_source

ソフトウェアインストール用に作成された関係

親クラス	関係性タイプ	子クラス
ソフトウェアインスタンス [cmdb_software_instance]	参照	ハードウェア [cmdb_ci_hardware]

デフォルトのクラスマッピング

デフォルトのクラスマッピングは、Claroty CTD のサービスグラフコネクタ統合 アプリケーションに付属しています。

i 注: クラスマッピングは **sn_clarotyctdsgc**にあります。SGOTClarotyCTDConstants スクリプト。

Claroty CTD タイプ	ServiceNow のタイプ	クラス	OT エンティティタイプ	Claroty のタイプとコード
eAAAサーバー (eAAAServer)	(空)	cmdb_ci_server		eAAAServer = 61
eアクセスコントロール	(空)	cmdb_ci_iot		eAccessControl = 50
eアクセスポイント	(空)	cmdb_ci_ip_switch		eAccessPoint = 60
eADServer	(空)	cmdb_ci_server		eADServer = 33
eAutonomousVehicle	OT フィールドデバイス	cmdb_ci_ot_field_device	ot_field_device	eAutonomousVehicle = 58
eAVServer	(空)	cmdb_ci_server		eAVServer = 32
eバーコードスキャナー	OT フィールドデバイス	cmdb_ci_ot_field_device	ot_field_device	eBarcodeScanner = 48
eBluetoothデバイス	(空)	cmdb_ci_iot		eBluetoothデバイス = 41
eブロードキャスト	(空)	cmdb_ci_netgear		eブロードキャスト = 4
eカメラ	OT フィールドデバイス	cmdb_ci_ot_field_device	ot_field_device	eCamera = 42
eクリーニングデバイス	OT フィールドデバイス	cmdb_ci_ot_field_device	ot_field_device	eクリーニングデバイス = 55
eコントローラー	OT コントロールシステム	cmdb_ci_ot_control_system	ot_control_system	eコントローラー = 20
eDataLogger	OT コントロールシステム	cmdb_ci_ot_control_system	ot_control_system	eDataLogger = 66
eDBServer	(空)	cmdb_ci_server		eDBServer = 35
eドメインコントローラー	(空)	cmdb_ci_server		eDomainController = 5
e電気駆動ドライブ	産業用ドライブ	cmdb_ci_ot_industrial_drive	ot_industrial_drive	eElectricalDrive = 68

Claroty CTD タイプ	ServiceNow のタイプ	クラス	OT エンティティタイプ	Claroty のタイプとコード
eエンドポイント	オペレーショナルテクノロジーデバイス	cmdb_ci_ot	ot_base	eEndpoint = 2
eエンジニアリングステーション	EWS	cmdb_ci_ot_ews	ews	eEngineeringStation = 14
eファイルサーバー	(空)	cmdb_ci_server		eFileServer = 10
eファイアウォール	(空)	cmdb_ci_ip_firewall		eファイアウォール = 31
eFrontEndProcessor	OT コントロールシステム	cmdb_ci_ot_control_system	ot_control_system	eFrontEndProcessor = 26
eゲートウェイ	(空)	cmdb_ci_ip_switch		eGateway = 15
eGPSClock	オペレーショナルテクノロジーデバイス	cmdb_ci_ot	ot_base	eGPSClock = 37
eGPSDevice	オペレーショナルテクノロジーデバイス	cmdb_ci_ot	ot_base	eGPSDevice = 62
eヒストリアン	履歴担当者	cmdb_ci_ot_historian	historian	eHistorian = 9
eHMIの	HMI	cmdb_ci_ot_hmi	hmi	eHMI = 1
eHomeアシスタント	(空)	cmdb_ci_iot		eHomeアシスタント = 53
eIED	IED	cmdb_ci_ot_ied	ied	eIED = 19
eインフュージョンポンプ	(空)	cmdb_ci_iot		eInfusionPump = 46
eMediaServer	(空)	cmdb_ci_server		eMediaServer = 54
e医療デバイス	(空)	cmdb_ci_iot		eMedicalデバイス = 47
電子顕微鏡	(空)	cmdb_ci_iot		eマイクロスコープ = 49
eモデム	(空)	cmdb_ci_netgear		eModem = 27
eモータースターター	産業用ドライブ	cmdb_ci_ot_industrial_drive	industrial_drive	eMotorStarter = 69
eNetworkAccessストレージ	(空)	cmdb_ci_server		eNetworkAccessStorage = 30
eネットワークキング	(空)	cmdb_ci_netgear		eネットワークキング = 3
eNTPServer	(空)	cmdb_ci_server		eNTPServer = 21
eOPCServer	OPC サーバー	cmdb_ci_ot_opc_server	opc_server	eOPCServer = 16

Claroty CTD タイプ	ServiceNow のタイプ	クラス	OT エンティティタイプ	Claroty のタイプとコード
eOT	オペレーショナルテクノロジーデバイス	cmdb_ci_ot	ot_base	eOT = 17
ePLC	PLC	cmdb_ci_ot_plc	plc	ePLC = 0
eプリンター	(空)	cmdb_ci_printer		eプリンター = 6
eProxyServer	(空)	cmdb_ci_netgear		eProxyServer = 28
eリモートIO	OT フィールドデバイス	cmdb_ci_ot_field_device	ot_field_device	eRemoteIO = 13
eReverseProxyServer	(空)	cmdb_ci_netgear		eReverseProxyServer = 29
eロボット	産業用ロボット	cmdb_ci_ot_industrial_robot	industrial_robot	eロボット = 57
eルーター	ルーター	cmdb_ci_ip_router		eRouter = 11
eRTU	RTU	cmdb_ci_ot_rtu	RTU	eRTU = 18
エスカダクライアント	SCADA クライアント	cmdb_ci_ot_scada_client	scada_client	エスカダクライアント = 7
eSCADAMaster	SCADA サーバー	cmdb_ci_ot_scada_server	scada_server	エスカダマスター = 38
eSCADAServer	SCADA サーバー	cmdb_ci_ot_scada_server	scada_server	eSCADAServer = 8
eセンサー	産業用センサー	cmdb_ci_ot_industrial_sensor	industrial_sensor	eSensor = 67
eスマートライト	(空)	cmdb_ci_iiot		eSmartLight = 51
eスマートフォン	(空)	cmdb_ci_iiot		eスマートフォン = 44
eスマートウォッチ	(空)	cmdb_ci_iiot		eSmartWatch = 45
eStorageArray	(空)	cmdb_ci_server		eStorageArray = 36
eストリーマー	(空)	cmdb_ci_iiot		eストリーマー = 52
eスイッチ	(空)	cmdb_ci_ip_switch		eSwitch = 12
eSyslogサーバー	(空)	cmdb_ci_server		eSyslogServer = 25
eTerminalServer	(空)	cmdb_ci_server		eTerminalServer = 24
eTVScreen	(空)	cmdb_ci_iiot		eTVScreen = 40
eUPS	(空)	cmdb_ci_ups		eUPS = 63
eUserConsole	HMI	cmdb_ci_ot_hmi	hmi	eUserConsole = 22

Claroty CTD タイプ	ServiceNow のタイプ	クラス	OT エンティティタイプ	Claroty のタイプとコード
eUserWorkstation	HMI	cmdb_ci_ot_hmi	hmi	eUserWorkstation = 23
eVendingマシン	(空)	cmdb_ci_iot		eVendingMachine = 43
eビデオレコーダー	(空)	cmdb_ci_server		eVideoRecorder = 64
eVirtualizationサーバー	(空)	cmdb_ci_server		eVirtualizationServer = 65
eVoipフォン	(空)	cmdb_ci_comm_hardware		eVoipPhone = 39
eVoipServer	(空)	cmdb_ci_server		eVoipServer = 56
eWeb サーバー	(空)	cmdb_ci_server		eWebServer = 34
eワイヤレスLANコントローラー	(空)	cmdb_ci_netgear		eWirelessLanController = 59
電子バーコードリーダー	(空)	cmdb_ci_iot		eBarcodeReader = 77
eバイオメトリックスキャナー	(空)	cmdb_ci_iot		eBiometricScanner = 74
eDNSServer	(空)	cmdb_ci_server		eDNSServer = 75
eSNMPScanner	(空)	cmdb_ci_server		eSNMPScanner = 73
eSNMPServer	(空)	cmdb_ci_server		eSNMPServer = 72
eVisionカメラ	OT フィールドデバイス	cmdb_ci_ot_field_device	ot_field_device	eVisionCamera = 76
eVisionController	OT コントロールシステム	cmdb_ci_ot_control_system	ot_control_system	eVisionController = 78
eビジョンセンサー	OT フィールドデバイス	cmdb_ci_ot_field_device	ot_field_device	eVisionSensor = 79
eVOIPAccessPoint	(空)	cmdb_ci_ip_switch		eVOIPAccessPoint = 71
e脆弱性スキャナー	(空)	cmdb_ci_server		eVulnerabilityScanner = 70

サービスグラフ コネクタ **Microsoft Defender for IoT (Azure)**

Microsoft Defender for IoT を ServiceNow オペレーショナルテクノロジーマネージャー アプリケーションと統合して、OT デバイスとセンサーアプライアンスのインポートを自動化します。

ストアでアプリを要求する

ServiceNow Store Web サイトにアクセスして、利用可能なすべてのアプリを表示し、要求をストアに送信する方法について確認してください。リリースされたすべてのアプリのこれまでのリリースノート情報については、「**ServiceNow Store のバージョン履歴リリースノート**」を参照してください。

サポート対象のバージョン

Microsoft Defender for IoTセンサーバージョンをサポートします。

- 22.2.3.22
- 22.2.5.9

ユースケース

ServiceNow オペレーショナルテクノロジーマネージャー アプリケーションで サービスグラフ Connector for Microsoft Defender for IoT (Azure) を使用して、OT デバイスとセンサーアプライアンスをインポートできます。

ガイド付きセットアップ

サービスグラフ Connector for Microsoft Defender for IoT (Azure) のガイド付きセットアップでは、インスタンスで統合を構成するための整理された一連のタスクが提供されます。ガイド付きセットアップにアクセスするには、「**ガイド付きセットアップの構成**」を参照してください。

CMDB 統合ダッシュボード

CMDB 共通統合 ストアアプリは、インストールされているすべての統合のステータス、処理結果、および処理エラーを一元的に表示するダッシュボードを提供します。すべての統合実行のメトリクスを確認することができます。特定の CMDB 統合、特定の期間、または特定の統合実行に関してビューをフィルタリングすることもできます。CMDB 統合ダッシュボードでの統合の監視の詳細については、「**CMDB 共通統合**」を参照してください。

データマッピング

Microsoft Defender for IoT (Azure) データソースのデータは、強力な変換エンジン (RTE) を使用してマッピングされ、ServiceNow CMDB 構成アイテム (CI) クラス定義に変換されます。データは、識別および調整エンジン (IRE) を使用して ServiceNow CMDB に挿入されます。

セットアップが完了したら、Microsoft Defender for IoT (Azure) アプリケーションから定期的にデータをプルするように統合を構成できます。

次の表に、Microsoft Defender for IoT (Azure) プロジェクトに含まれるデータソースと、インポートされたデータがロードされる対応するステージングテーブルを示します。

Microsoft Defender for IoT (Azure) のデータソースとステージングテーブル

データソース	ステージングテーブル
SG-OT Azure D4IoT デバイスインポート	SG-OT Azure D4IoT デバイスインポート [sn_msftd4iotazsgc_sg_ot_azure_d4iot_devices_import]
SG-OT Azure D4IoT センサーインポート	SG-OT Msft D4IoT センサーインポート [sn_msftd4iotazsgc_sg_ot_azure_d4iot_sensors_import]

ステージングテーブルからインポートされたデータは、次のターゲットテーブルに挿入されます。

- AIX サーバー [cmdb_ci_aix_server]
- コンピューター [cmdb_ci_computer]
- 構成アイテム (CI) [cmdb_ci]
- DCS [cmdb_ci_ot_dcs]
- ESX サーバー [cmdb_ci_esx_server]
- EWS [cmdb_ci_ot_ews]
- 外部システムメタデータ [cmdb_key_value_v2]
- ゲームコンソール [cmdb_ci_game_console]
- ハンドヘルドコンピューティングデバイス [cmdb_ci_handled_computing]
- 履歴担当者 [cmdb_ci_ot_historian]
- HMI [cmdb_ci_ot_hmi]
- HP-UX サーバー [cmdb_ci_hpux_server]
- HVAC機器 [cmdb_ci_hvac]
- HyperV サーバー [cmdb_ci_hyper_v_server]
- IED [cmdb_ci_ot_ied]
- 産業用アクチュエーター [cmdb_ci_ot_industrial_actuator]
- 産業用ドライブ [cmdb_ci_ot_industrial_drive]
- 産業用ロボット [cmdb_ci_ot_industrial_robot]
- 産業用センサー [cmdb_ci_ot_industrial_sensor]
- IoT デバイス [cmdb_ci_iot]
- IP アドレス [cmdb_ci_ip_address]
- IP カメラ [cmdb_ci_ip_camera]
- IP ファイアウォール [cmdb_ci_ip_firewall]
- IP フォン [cmdb_ci_ip_phone]
- Linux サーバー [cmdb_ci_linux_server]
- ネットギア [cmdb_ci_netgear]
- ネットワークアダプタ [cmdb_ci_network_adapter]
- ネットワーク侵入検知システム [cmdb_ci_nids]
- オペレーショナルテクノロジー (OT) [cmdb_ci_ot]
- OSX サーバー [cmdb_ci_osx_server]
- OT コントロールモジュール [cmdb_ci_ot_control_module]
- OT コントロールシステム [cmdb_ci_ot_control]
- OT デバイスの詳細 [cmdb_ot_entity]
- OT フィールドデバイス [cmdb_ci_ot_field_device]
- PLC [cmdb_ci_ot_plc]
- プリンター [cmdb_ci_printer]
- RTU [cmdb_ci_ot_rtu]

- シリアル番号 [cmdb_serial_number]
- サーバー [cmdb_ci_server]
- サーバー [cmdb_ci_server]
- Solaris サーバー [cmdb_ci_solaris_server]
- ソース [sys_object_source]
- Unix Servercmdb_ci_unix_server]
- 無停電電源装置 (UPS) [cmdb_ci_ups]
- 無線アクセスポイント [cmdb_ci_wap_network]

Microsoft Defender for IoT (Azure) プロジェクトからデータをプルするときにデータが保存される場所の詳細については、「[対象となる CMDB クラス](#)」を参照してください。

Microsoft Defender for IoT (Azure) の サービスグラフ コネクタの構成

Microsoft Defender for IoT (Azure) の サービスグラフ コネクタのガイド付きセットアップを使用して、統合ステップを進めます。

始める前に

依存関係と要件：

- 自動的にインストールされる [CMDB 共通統合](#) ストアアプリ。
- 自動的にインストールされる [CMDB CI クラスモデル](#)。
- ITOMディスカバリーライセンスプラグイン (com.snc.itom.discovery.license)。このプラグインを有効にする必要があります。
- ITOM Licensing プラグイン (com.snc.itom.license)。詳細については、「[ディスカバリーの要求](#)」を参照してください。
- 自動的にインストールされる Datastream Action プラグイン (com.glide.hub.action_type.datastream)。
- Industrial Core プラグイン。このプラグインを有効にする必要があります。

Microsoft Defender for IoT (Azure) のサービスグラフコネクタのクラスマッピングテーブルにアクセスするには、Industrial Core プラグインが必要です。Industrial Core プラグインの詳細については、「[Industrial Core プラグイン](#)」を参照してください。

必要なロール：admin

- i** 注：以前のバージョンの サービスグラフ Connector for Microsoft Defender for IoT (Azure) を使用している場合は、古いコネクタからデータを移行しないでください。以前のバージョンをアンインストールし、新しい統合を実行する必要があります。

手順

1. アプリケーションピッカーを使用して、アプリケーションスコープが サービスグラフ Connector for Microsoft Defender for IoT (Azure) アプリケーションに設定されていることを確認します。
詳細については、「[アプリケーションピッカー](#)」を参照してください。
2. 移動先 すべて > **MSFT D4IoT (Azure)** の サービスグラフ > ガイド付きセットアップ。
3. [はじめに] ページで、[開始] を選択します。
4. Azureリソースにアクセスするには、次の手順を実行します。

- a. [Azure リソースへのアクセス] タスクを選択します。
 - b. 説明の手順を完了したら、[完了としてマーク] を選択します。
5. 接続と認証情報を設定するには、次の手順を実行します。
- a. [接続と資格情報の構成] セクションで、[接続と資格情報のセットアップ] タスクを選択します。
 - b. [Configure] を選択します。
 - c. **SG-OT Azure** 接続レコードを選択します。
 - d. [新しい接続および資格情報の作成] 関連リンクを選択します。
 - e. [接続と資格情報を作成] ウィンドウで、次のフィールドに入力します。

フィールド	説明
接続名	接続レコードの表示名
接続 URL	Azure URL
OAuth クライアント ID	クライアント ID (アプリケーション ID) またはサービスプリンシパル ID
OAuth クライアントシークレット	サービスプリンシパルに関連付けられたクライアントシークレットキー
OAuth トークン URL	認証トークンをフェッチするための URL。URL の <tenantid> をテナント ID の値に置き換えます。

i 注: トークンの生成が成功すると、新しいウィンドウに成功メッセージが表示されます。トークンの生成が成功しなかった場合、新しいウィンドウに「 OAuth フローに失敗しました」というエラーメッセージが表示されます。表示された詳細を確認し、作成したレコードを編集してもう一度お試しください。

- f. [**OAuth** トークンを作成して取得] を選択します。
6. 接続をテストするには、次の手順を実行します。
- a. [接続と資格情報のセットアップ] セクションで、[接続のテスト/検証] タスクを選択します。
 - b. センサーのデータソースレコードの関連リンクセクションから [テスト接続] UI アクションを選択します。
接続テストが完了したら、結果を表示します。テスト結果が「成功」を返すまで、推奨されるトラブルシューティング手順を実行する必要があります。
7. システムプロパティを設定するには、次の手順を実行します。
- a. [システムプロパティの構成] セクションで、[構成] を選択します。
 - b. 次のシステムプロパティを構成します。

プロパティ	説明
sn_msft4iotazsgc.resource_path	リソースパスプロパティを設定します。 ARG REST API バージョン 2021-03-01 の既定のリソース パスは /providers/Microsoft.ResourceGraph/resources です。
sn_msft4iotazsgc.pagesize.sensor	センサーのページサイズプロパティを設定します。 - Azure ARG REST API はページネーションをサポートしているため、API ごとにページあたりのレコード数を選択できます。 - デフォルトは 1 ページあたり 1000 レコードです。 i 注: 1000 は、ページあたりの最大レコード数でもあります。
sn_msft4iotazsgc.pagesize.device	デバイスのページサイズプロパティを設定します。 - Azure ARG REST API はページネーションをサポートしているため、API ごとにページあたりのレコード数を選択できます。 - デフォルトは 1 ページあたり 1000 レコードです。 i 注: 1000 は、ページあたりの最大レコード数でもあります。
sn_msft4iotazsgc.get_all_devices	- デバイスの場合は、すべてのレコードのフェッチ (チェックボックスをオン) またはデルタフェッチ (ボックスをオフ) を選択できます。 - デルタでは、CMDBで前回成功したインポートの開始時刻以降に作成または更新されたすべてのレコードをフェッチします。 i 注: デバイス統合を初めて実行すると、すべてのレコードがこのプロパティとは独立してインポートされます。
sn_msft4iotazsgc.convert_sensor_names_to_lowercase	インポートの場合は、このプロパティを設定します。

プロパティ	説明
	- このシステムプロパティは、デバイスのインポート時に Microsoft Azure によって提供されるセンサー名を小文字に変換するために使用されます。 - Microsoft Azureはクエリのデータが小文字形式であることが想定されるため、これが必要です。
sn_msftd4iotazsgc.filter.device_sub_types	デバイスのインポート中にサブタイプ別にデバイスをフィルタリングするには、このプロパティを設定します。 - デバイスをフィルタリングするための Microsoft Azure サブタイプのカンマ区切りリスト。 - たとえば、PLC とサーバーのみをインポートするには、Microsoft Azure の DeviceSubType 属性の値を Server, PLC として指定します。
sn_msftd4iotazsgc.filter.device_tags	デバイスのインポート中にデバイスタグでデバイスをフィルタリングするには、このプロパティを設定します。 - デバイスのフィルタリングに必要なタグのカンマ区切りリスト (大文字と小文字を区別する)。 - 例:特定のタグを持つデバイスをインポートするには、Microsoft Azure の DeviceTags 属性の値のリストを指定します。
sn_msftd4iotazsgc.filter.custom_query	デバイスサブタイプおよびデバイスタグフィルターとは別にデバイスインポートのフィルターを追加するには、このプロパティを設定します。 - 他の属性に基づいてフィルタリングするクエリ。 - これにより、他の属性のフィルタリングが可能になります。詳細については、「Azure クエリ言語」を参照してください。
sn_msftd4iotazsgc.azure_d4iot_site_map_fields	Microsoft Defender for IoT (Azure) サイトマップのフィールドのオブジェクト。フィールドが True に設定されている場合、Microsoft Defender for IoT (Azure) のサービスグラフコネクタは [サイトマップ] フィールドの値を、Azure サイトの統合によって検出された各 CI の対応するフィールドに渡します。 False に設定されている場合、またはサイトマップレコードで設定されていない場合、Azure サイトに関連付けられているイン

プロパティ	説明
	ポート済み CI では、このフィールドが設定されません。 NIDS フレームワークを使用する他の統合との整合性を保つために、このシステムプロパティを確認してください。デフォルトでは、場所 と equipment_model_entity のみが True に設定されています。
sn_msftd4iotazsgc.devices_fetch_type	デバイスがセンサーごと、アクティブスキャンデバイスごと、またはその両方ごとにフェッチされるかどうかを示します。
sn_msftd4iotazsgc.active_scan_get_all_devices	すべてのアクティブスキャンデバイスをインポートするには、このシステムプロパティを設定します。オフにすると、前回の正常なインポート以降に作成または更新されたアクティブスキャンデバイスのみがインポートされます。デフォルト値は [なし] です。
sn_msftd4iotazsgc.filter.active_scan.device_sub_type	アクティブスキャンデバイスをフィルタリングする Azure サブタイプのカンマ区切りリスト。たとえば、PLC とサーバーのみをインポートするには、Device SubType 属性の値を Server, PLC in Azure に指定します。
sn_msftd4iotazsgc.filter.active_scan.device_tags	アクティブスキャンデバイスのフィルタリングに必要なタグのカンマ区切りリスト (大文字と小文字を区別する)。たとえば、特定のタグを持つアクティブスキャンデバイスをインポートするには、Azure の DeviceTags 属性の値のリストを指定します。
sn_msftd4iotazsgc.filter.active_scan.custom_query	アクティブスキャンデバイスの他の属性をフィルタリングするクエリ。たとえば、他の属性のフィルタリングを許可します。 Azure クエリ言語の詳細については、「Azure クエリ言語」を参照してください。

c. **[Save (保存)]** を選択します。

8. センサーをインポートするには、次の手順を実行します。

- a. [センサーの構成 (NIDS)] セクションで、[センサーのインポート] タスクを選択します。
- b. **[Configure]** を選択します。
- c. [アクティブ] を選択して、スケジュール設定済みデータインポートジョブをアクティブにします。

9. NIDS を構成するには、次の手順を実行します。

- a. [センサーの構成 (NIDS)] セクションで、[センサーのインポート] タスクを選択します。
- b. 説明にリンクされている NIDS 構成を完了したら、[完了としてマーク (**Mark as complete**)] を選択します。

10. インポートスケジュールを設定するには、次の手順を実行します。

- a. [インポートスケジュールの構成] セクションで、[構成] を選択します。
- b. **[SG-OT Microsoft D4IoT Azure センサースケジュール済みインポート]** を選択して、必要に応じてセンサーインポートスケジュールを確認または変更します。
 - i. [アクティブ] を選択して、センサーインポートスケジュールをアクティブにします。
 - ii. デフォルトでは、センサーのインポートスケジュールは毎日深夜に実行されるように設定されています。[実行] フィールドと [時間] フィールドを使用してスケジュールを変更します。
 - iii. このスケジュールを条件付きにするには、[条件付き] チェックボックスをオンにします。
 - iv. [今すぐ実行] を選択して、手動インポートを開始します。
- c. **[SG-OT Microsoft D4IoT デバイスのスケジュール済みインポート]** を選択し、必要に応じてデバイスのインポートスケジュールを確認または変更します。
 - i. [アクティブ] を選択して、センサーインポートスケジュールをアクティブにします。
 - ii. デフォルトでは、センサーのインポートスケジュールは毎日深夜に実行されるように設定されています。[実行] フィールドと [時間] フィールドを使用してスケジュールを変更します。
 - iii. このスケジュールを条件付きにするには、[条件付き] チェックボックスをオンにします。
 - iv. [今すぐ実行] を選択して、手動インポートを開始します。

 注: デバイスはセンサーごとにクエリされます。サービスグラフコネクタは、検証済みのセンサーによって検出されたデバイスのみクエリします。詳細については、ステップ 9 を参照してください。

11. オプション: CMDBで構成アイテム (CI) が作成されると、資産レコードが作成されます。資産レコードには、CI のモデルカテゴリが含まれています。オペレーショナルテクノロジー (OT) のモデルカテゴリの詳細については、「[のモデルカテゴリ オペレーショナルテクノロジー](#)」を参照してください。OT デバイスのモデルカテゴリを表示するには、次の手順を実行します。

- a. 移動先 **すべて > オペレーショナルテクノロジー (OT) > すべての OT デバイス**。
- b. 資産レコードを表示する OT デバイスを選択します。
- c. [資産] フィールドの横にある [このレコードをプレビュー] アイコン () を選択します。
- d. [レコードを開く (**Open Record**)] を選択します。

12. オプション: サービスグラフ Connector for Microsoft Defender for IoT(Azure)のトラブルシューティングを行うには、次の手順に従います。

- a. [オプション] Microsoft Defender for IoT (Azure) のサービスグラフコネクタのトラブルシューティング セクションを選択します。
- b. [検証スケジュール済みジョブを実行] タスクで、[構成] を選択します。

c. **[Execute Now (今すぐ実行)]** を選択します。

このジョブは、SGC の構成と Microsoft Azure への接続を検証するタスクを実行します。構成の問題が見つかった場合、検証結果に問題が報告され、トラブルシューティング手順が提案されます。スケジュール済みジョブが終了するまで待ちます。

- d. スケジュール済みジョブが完了したら、「[オプション] Microsoft Defender for IoT (Azure) のサービスグラフコネクタのトラブルシューティング」セクションに戻ります。
- e. [検証結果のレビュー] タスクで、[構成] を選択します。
このステップでは、前回のトラブルシューティング実行の実行ログと提案が開き、表示されます。
- f. 必要に応じて提案に対処します。

i 注: スケジュール設定済みスクリプトは、Claroty CTD のサービスグラフコネクタ統合の初期構成後であればいつでも使用できます。検証をトリガーするには、次に移動します: すべて > **MSFT D4IoT (Azure)** のサービスグラフ > トラブルシューティング > トラブルシューティングの実行. 検証結果を表示するには、次に移動します: すべて > **MSFT D4IoT (Azure)** のサービスグラフ > トラブルシューティング > 結果.

次のタスク

これで、Microsoft Defender for IoT (Azure) を ServiceNow サービスグラフ Connector for Microsoft Defender for IoT (Azure) に接続できるようになりました。詳細については、次を参照してください。 [Microsoft Defender for IoT \(Azure\) サブスクリプションを Microsoft Defender for IoT \(Azure\) の ServiceNow サービスグラフコネクタに接続する \(KB1587770\)](#)。

NIDS センサーの検証

インポートされたネットワーク IDS (NIDS) センサーを検証して、デバイスのインポートに備えます。センサーはデバイスインポートの対象ではないため、センサーはラーニングモードでない場合にのみ検証に合格します。

始める前に

CSDM プラグインをインストールすることをお勧めします。サービスグラフコネクタは、CMDB 標準に従ってライフサイクルデータモデルに適合します。詳細については、「[CSDM フレームワークを段階的に実装する](#)」を参照してください。

必要なロール:cmdb_nids_admin

i 注: ServiceNow の NIDS アプライアンスは、Microsoft Defender for IoT (Azure) センサーを表します。

このタスクについて

[ライフサイクルステージ] フィールドと [ライフサイクルステージステータス] フィールドは、センサーの学習モードをキャプチャするために使用されます。[ライフサイクルステージ] フィールドが [運用] に設定され、かつ [ライフサイクルステージステータス] が [学習モード] に設定されている場合、検証は失敗します。[ライフサイクルステージステータス] フィールドが [使用中] に設定されている場合、検証は成功しています。

手順

1. 移動先 すべて > ネットワーク **IDS** アプライアンス (**NIDS**) > センサー.
2. 検証するセンサーレコードを選択します。
3. [NIDS アサインメタデータ (NIDS Assigned Meta Data)] セクションで、検出されたデバイスに割り当てたセンサーの値を追加します。
4. [NIDS アドミン構成] セクションで、[ライフサイクルステージステータス] フィールドの値が [学習モード] でないことを確認します。
それ以外の場合、検証は失敗します。

5. [**NIDS** ネットワークタイプ] フィールドが NIDS ネットワークの場所に基づいて設定されていることを確認します。
 たとえば、NIDS のデータセンター展開の場合は **NIDS** ネットワークタイプの IT を選択し、産業用/OT ネットワークでの産業用展開の場合は **NIDS** ネットワークタイプの OT を選択できます。
- [OT] を選択すると、すべてのデバイスに対して OT デバイスの詳細が作成されます。
6. 属性が正しく入力されたら、[検証] を選択します。

i 注:

注意: センサーからデバイスに渡される属性は、sn_cmdb_ci_class.nids_map_fields システムプロパティで定義されます。次のリストは、属性のデフォルトのリストです。

- assigned_to
- 場所
- 会社
- owned_by
- managed_by
- supported_by
- change_control
- support_group
- managed_by_group
- assignment_group
- ゾーン
- isa_entity_site (製造業プロセスマネージャー アプリケーションがインストールされている場合のみ利用可能)

の接続の詳細へのアクセス **Microsoft Defender for IoT (Azure)** のサービスグラフコネクタ

CMDDB 共通統合 (sn_cmdb_int_util) ストアアプリに含まれる共通接続フレームワーク (CCF) を使用して、単一のビューで Microsoft Defender for IoT (Azure) のサービスグラフコネクタの接続の詳細にアクセスできます。

CCF を使用すると、Microsoft Defender for IoT (Azure) のサービスグラフコネクタ で使用されるすべての接続にアクセスできます。接続の詳細には、接続エイリアス、接続のプロパティ、データソース、および接続に関連付けられたスケジュール設定済みデータインポートが含まれます。接続をテストすることもできます。詳細については、「[サービスグラフコネクタの接続の詳細へのアクセス](#)」を参照してください。

Microsoft Defender for IoT (Azure) 接続の詳細へのアクセス

Claroty CTD のサービスグラフコネクタ統合用に構成された Microsoft Defender for IoT (Azure) 接続の詳細にアクセスします。

始める前に

必要なロール: admin

このタスクについて

サービスグラフ Connector for Microsoft Defender for IoT (Azure) のデータソース、システムプロパティ、およびスケジュール設定済みデータインポートに個別に移動できるアプリケーションモジュールがあります。ただし、共通接続フレームワーク (CCF) を使用すると、Microsoft Defender for IoT (Azure) 用に作成されたすべての関連データソースとスケジュール設定済み

データインポートを 1 か所に集めることができます。関連リンクセクションを使用して、ソース (Microsoft Defender for IoT (Azure)) への接続をテストすることもできます。

手順

1. アプリケーションピッカーを使用して、アプリケーションスコープが サービスグラフ Connector for Microsoft Defender for IoT (Azure) アプリケーションに設定されていることを確認します。
2. 移動先 すべて > **MSFT D4IoT (Azure)** のサービスグラフ > **Azure SGC** の接続。
3. [サービスグラフ接続] ページで、[**SG-OT Azure SGC デフォルト接続 (SG-OT Azure SGC Default Connection)**] レコードを選択します。
4. オプション: システムのプロパティにアクセスするには、[サービスグラフ接続のプロパティ] タブを選択します。
5. オプション: データソースにアクセスするには、[サービスグラフ接続データソース] タブを選択します。
6. オプション: 予定されているデータインポートにアクセスするには、[サービスグラフ接続の予定されているデータインポート] タブを選択します。
7. オプション: Microsoft Azure プラットフォームとの接続をテストするには、[テスト接続] 関連リンクを選択します。
接続はいつでもテストできます。接続テストが完了すると、同じページの [ステータス] と [提案] に、失敗したステップのトラブルシューティングのためのステータスと提案がそれぞれ表示されます。

標準検出モードを使用して **OT** デバイスをインポート

Microsoft Defender for IoT (Azure) のサービスグラフコネクタを使用して、標準検出モードで検出された オペレーショナルテクノロジー (OT) デバイスを Microsoft Defender for IoT からインポートします。

始める前に

必要なロール: admin

このタスクについて

標準モードでは、アクティブな検索を使用して、識別された OT デバイスに関する追加情報を検出し、既存のデバイス情報を補足します。標準モードで識別されたデバイスは、パッシブセンサーに関連付けられていません。これらのデバイスをインポートしてサイトに割り当てるには、サイトマッピングテーブルを使用します。テーブルは、自動スケジュール済みジョブを使用して入力されます。スケジュール済みジョブが実行されると、ソースシステムからテーブルにサイトが入力されます。

[サイトマッピング] テーブルを使用すると、アドミンは、このデータが存在する Microsoft Defender for IoT (Azure) サイトと ServiceNow ISA エンティティサイト [cmdb_ci_ot_isa_entity] の間でサイトマッピングを実行できます。データが Microsoft Defender for IoT (Azure) のサービスグラフコネクタ を介してインポートされると、デバイスは ISA エンティティサイト [cmdb_ci_ot_isa_entity] の正しいサイトに割り当てられます。

手順

1. 移動先 すべて > **MSFT D4IoT (Azure)** のサービスグラフ > サイトマッピング。
2. [New (新規)] を選択します。
3. フォームで次のフィールドに入力します。

SG-OT Azure D4IoT サイトマップのフィールド

フィールド	説明
ISA エンティティサイト	ISA エンティティサイトのサイト名。
Azure D4IoT サイト	Azure D4IoT サイトのサイト名。
場所	Azure D4IoT サイトの場所
承認グループ	サイトに関連する要求を承認できるグループ。
Azure D4IoT サイト URL	
アサイン先	サイトが割り当てられているユーザー。
変更グループ	サイトに関連する変更要求がアサインされているグループ。
会社	サイトを運営する会社。
管理担当者	サイトを管理するユーザー。
管理担当者グループ	サイトを管理するグループ。
所有者	サイトを所有するユーザー。
サポートグループ	問題が発生したときに連絡を受けるグループ。
サポート担当者	問題が発生したときに連絡を受けるユーザー。
ネットワークタイプ	サイトのネットワークタイプ。例:OT。
関連 ID	ローカルシステム上の関連を識別する一意の ID。

4. [Submit (送信)] を選択します。

結果

サイトマッピングレコードが作成され、デバイスのインポートを実行すると、センサーとアクティブスキャンによってデバイスがインポートされます。その後、デバイスは ServiceNow の ISA エンティティ [cmdb_ci_ot_isa_entity] サイトにアサインされます。

- i** 注: [アサイン先] や [オーナー] などのサイトレコードのメタデータ情報は、サービスグラフコネクタのシステムプロパティを使用してインポートされたデバイスにコピーされます。Microsoft Defender for IoT (Azure) のサービスグラフコネクタのシステムプロパティの詳細については、「[ガイド付きセットアップの構成](#)」を参照してください。

CMDB での対象となるクラス Microsoft Defender for IoT (Azure) のサービスグラフコネクタ

ガイド付きセットアップを完了したら、Microsoft Defender for IoT (Azure) のサービスグラフコネクタ (Azure) プロジェクトから定期的にデータをプルするように統合を構成できます。データは、構成アイテム [cmdb_ci] テーブルから拡張されたテーブルに保存されます。

クラスマッピングの表示

Microsoft Defender for IoT (Azure) のサービスグラフコネクタに利用可能なクラスマッピングを表示するには、次に移動します: すべて > **MSFT D4IoT (Azure)** のサービスグラフ > クラスマッピング。クラスマッピングテーブルでは、次の属性を表示できます。

クラスマッピング属性

フィールド	説明
ソースクラス	ソースシステム (Azure) のデバイスタイプ。
ターゲット CMDB クラス	CI に予期される ServiceNow クラス。
OT デバイスタイプ	OT デバイスが分類されるカテゴリタイプ。デバイスタイプは、デバイスが OT ネットワーク上で果たす機能でもあります。たとえば、次のようになります。 サーバーなどのIT機器はOT機器に変換でき、ネットワーク上で果たす機能はHMIです。したがって、そのクラスは server で、デバイスタイプは HMI です。 i 注: 場合によっては、OT 機能を持たない OT デバイスや、デバイスタイプが不明な OT デバイスがあります。OT 機能のない OT デバイスの場合は、[OT 機能なし] を選択します。デバイスタイプが不明な OT デバイスの場合は、[不明] を選択します。
OS 分類を許可	True に設定すると、CI でオペレーティングシステムが見つかった場合、ターゲットはターゲットの CMDB クラスからその OS に一致する ServiceNow クラスに切り替えられます。
アクティブ	オンにすると、クラスマッピングがアクティブに設定されます。

コンピューター [cmdb_ci_computer]

コンピューター [cmdb_ci_computer] テーブルの次の属性は、収集されたデータによって設定されます。

コンピューター [cmdb_ci_computer] 属性

属性ラベル	属性の名前
最新のディスカバリー	last_discovered
オペレーティングシステム	os
OS アドレス幅 (ビット)	os_address_width
OS ドメイン	os_domain
OS バージョン	os_version

外部システムメタデータ [cmdb_key_value_v2]

外部システムメタデータ [cmdb_key_value_v2] テーブルの次の属性は、収集されたデータによって設定されます。

外部システムメタデータ [cmdb_key_value_v2] 属性

属性ラベル	属性の名前
ディスカバリーソース	discovery_source
キー	キー
ソースキー	source_key
文字列値	string_value
URL 値	url_value
値のタイプ	value_type

ハードウェア [cmdb_ci_hardware]

ハードウェア [cmdb_ci_hardware] テーブルの次の属性は、収集されたデータによって設定されます。

ハードウェア [cmdb_ci_hardware] 属性

属性ラベル	属性の名前
クラス	sys_class_name
モデル番号	model_number
最新検出日	last_discovered
場所	場所
モデル ID	model_id
メーカー	メーカー
最初の検出	first_discovered
所有者	owned_by
承認グループ	change_control
グループによる管理	managed_by_group
管理担当者	managed_by
名前	名前
会社	会社
サポートグループ	support_group
変更グループ	assignment_group
アサイン先	assigned_to
サポート担当者	supported_by

ハードウェアに対して作成された関係

親クラス	関係性タイプ	子クラス
ハードウェア [cmdb_ci_hardware]	Owns::Owned by	IP アドレス [cmdb_ci_ip_address]

ハードウェアに対して作成された関係 (続く)

親クラス	関係性タイプ	子クラス
ハードウェア [cmdb_ci_hardware]	Owns::Owned by	ネットワークアダプタ [cmdb_ci_network_adapter]
ハードウェア [cmdb_ci_hardware]	参照	外部システムメタデータ [cmdb_key_value_v2]
ハードウェア [cmdb_ci_hardware]	参照	OT デバイス [cmdb_ot_entity]

IP アドレス [cmdb_ci_ip_address]

IP アドレス [cmdb_ci_ip_address] テーブルの次の属性は、収集されたデータによって設定されます。

IP アドレス [cmdb_ci_ip_address] 属性

属性ラベル	属性の名前
IP アドレス	ip_address
IP バージョン	ip_version
構成アイテムが所有	owned_by_cmdb_ci

IP アドレス用に作成された関係

親クラス	関係性タイプ	子クラス
IP アドレス [cmdb_ci_ip_address]	参照	ネットワーク侵入検知システム [cmdb_ci_nids]
IP アドレス [cmdb_ci_ip_address]	参照	ハードウェア [cmdb_ci_hardware]

ネットワークアダプタ [cmdb_ci_network_adapter]

ネットワークアダプタ [cmdb_ci_network_adapter] テーブルの次の属性は、収集されたデータによって設定されます。

ネットワークアダプタ [cmdb_ci_network_adapter] 属性

属性ラベル	属性の名前
MAC アドレス	mac_address
名前	name
ディスカバリーソース	discovery_source

ネットワークアダプタ用に作成された関係

親クラス	関係性タイプ	子クラス
ネットワークアダプタ [cmdb_ci_network_adapter]	参照	ネットワーク侵入検知システム [cmdb_ci_nids]

ネットワークアダプタ用に作成された関係 (続く)

親クラス	関係性タイプ	子クラス
ネットワークアダプタ [cmdb_ci_network_adapter]	参照	ハードウェア [cmdb_ci_hardware]

ネットワーク侵入検知システム [cmdb_ci_nids]

ネットワーク侵入検知システム [cmdb_ci_nids] テーブルの次の属性は、収集されたデータによって設定されます。

ネットワーク侵入検知システム [cmdb_ci_nids] 属性

属性ラベル	属性の名前
最初の検出	first_discovered
NIDS ソース名	source_name
ライフサイクルステージ	life_cycle_stage
Life Cycle Stage Status (ライフサイクルステータス)	life_cycle_stage_status
名前	name
相関 ID	correlation_id
ファームウェアバージョン	firmware_version
完全修飾ドメイン名	fqdn
NIDS アサインゾーン	ゾーン
NIDS マネージャー接続ステータス	connection_state
検証済み	検証済み
メーカー	メーカー

NIDS 用に作成された関係

親クラス	関係性タイプ	子クラス
ネットワーク侵入検知システム [cmdb_ci_nids]	検出::Detected	ハードウェア [cmdb_ci_hardware]
ネットワーク侵入検知システム [cmdb_ci_nids]	Owns::Owned by	IP アドレス [cmdb_ci_ip_address]
ネットワーク侵入検知システム [cmdb_ci_nids]	Owns::Owned by	ネットワークアダプタ [cmdb_ci_network_adapter]

オペレーショナルテクノロジー (OT) [cmdb_ci_ot]

オペレーショナルテクノロジー (OT) [cmdb_ci_ot] テーブルの次の属性は、収集されたデータによって設定されます。

オペレーショナルテクノロジー (OT) [cmdb_ci_ot] 属性

属性ラベル	属性の名前
最新のディスカバリー	last_discovered

OT コントロールモジュール [cmdb_ci_ot_control_module]

OT コントロールモジュール [cmdb_ci_ot_control_module] テーブルの次の属性は、収集されたデータによって設定されます。

OT コントロールモジュール [cmdb_ci_ot_control_module] 属性

属性ラベル	属性の名前
ベンダー	ベンダー
サポートグループ	support_group
シリアル番号	serial_number
クラス	sys_class_name
最初の検出	first_discovered
承認グループ	change_control
管理担当者	managed_by
グループによる管理	managed_by_group
変更グループ	assignment_group
会社	会社
ラック番号	rack_number
スロット番号	slot_number
場所	場所
名前	名前
ファームウェアバージョン	firmware_version
最新検出日	last_discovered
アサイン先	assigned_to
所有者	owned_by
サポート担当者	supported_by
モデル ID	model_id

OT コントロールモジュール用に作成された関係

親クラス	関係性タイプ	子クラス
OT コントロールモジュール [cmdb_ci_ot_control_module]	参照	OT デバイス [cmdb_ot_entity]

OT コントロールシステム [cmdb_ci_ot_control]

OT コントロールシステム [cmdb_ci_ot_control] テーブルの次の属性は、収集されたデータによって設定されます。

OT コントロールシステム [cmdb_ci_ot_control] 属性

属性ラベル	属性の名前
モジュールあり	has_module
最新検出日	last_discovered

OT コントロールシステム用に作成された関係

親クラス	関係性タイプ	子クラス
OT コントロールシステム [cmdb_ci_ot_control]	Owens::Owned by	OT コントロールモジュール [cmdb_ci_ot_control_module]

OT デバイス [cmdb_ot_entity]

OT デバイス [cmdb_ot_entity] テーブルの次の属性は、収集されたデータによって設定されます。

OT デバイス [cmdb_ot_entity] 属性

属性ラベル	属性の名前
ISA エンティティサイト	isa_entity_site
OT ディスカバリーソース ID	ot_correlation_id
デバイスの重要度	business_criticality
Purdue レベル	purdue_level
ゾーン	ゾーン
OT デバイスタイプ	ot_asset_type
IRE 基準属性	ire_criterion_attribute

PLC [cmdb_ci_ot_plc]

PLC [cmdb_ci_ot_plc] テーブルの次の属性は、収集されたデータによって設定されます。

PLC [cmdb_ci_ot_plc] 属性

属性ラベル	属性の名前
最新のディスカバリー	last_discovered
スイッチ位置	switch_position
リモートスイッチ	switch_remote_mode

シリアル番号 [cmdb_serial_number]

シリアル番号 [cmdb_serial_number] テーブルの次の属性は、収集されたデータによって設定されます。

シリアル番号 [cmdb_serial_number] 属性

属性ラベル	属性の名前
シリアル番号	serial_number
シリアル番号タイプ	serial_number_type
有効	valid

シリアル番号用に作成された関係

親クラス	関係性タイプ	子クラス
シリアル番号 [cmdb_serial_number]	参照	ハードウェア [cmdb_ci_hardware]
ネットワークアダプタ [cmdb_ci_network_adapter]	参照	ハードウェア [cmdb_ci_hardware]

の属性マッピングと分類 **Microsoft Defender for IoT (Azure)** のサービスグラフコネクタ

次の表に、センサーとデバイスの属性マッピングと分類を示します。

センサー属性マッピング

ペイロードフィールド名	データタイプ	テーブルへのマッピング	フィールドにマッピング	説明
ID	文字列形式: /subscriptions/<subscription-id>/provider/<provider>/locations/<location>/sites/<site>/sensor/<sensor-name>	- sys_object_source - cmdb_ci_nids	sys_object_source の SNK correlation_id	センサーの一意の ID。
名前	文字列	cmdb_ci_nids	名前	センサーの名前。
properties.hostname	文字列	cmdb_ci_nids	fqdn	センサーのホスト名。
properties.ip	文字列	cmdb_ci_ip_address	ip_address	センサーの IP アドレス。
properties.learningMode	ブール値	cmdb_ci_nids	False または利用不可: ライフサイクルステージ (life_cycle_stage): 運用 ライフサイクルステータス (life_cycle_stage_status): 使用中	IoT センサーのラーニングモードステータス。

センサー属性マッピング (続く)

ペイロードフィールド名	データタイプ	テーブルへのマッピング	フィールドにマッピング	説明
			True : ライフサイクルステージ (life_cycle_stage): 運用 ライフサイクルステータス (life_cycle_stage_status): ラーニング	
properties.mac	文字列	cmdb_ci_network_adapter	名前、mac_address	センサーの MAC アドレス。
properties.sensorStatus	文字列	cmdb_ci_nids	connection_state	IoT センサーのステータス。
properties.sensorVersion	文字列	cmdb_ci_nids	firmware_version	IoT センサーのバージョン。
properties.upSince	文字列としての日時	cmdb_ci_nids	first_discovered	起動時間。
properties.zone	文字列	cmdb_ci_nids	ゾーン	IoT センサーのゾーン。

デバイス属性マッピング

ペイロードフィールド名	データタイプ	テーブルへのマッピング	フィールドにマッピング	説明
ID	文字列形式:/subscriptions/subscription-id>/providers/<providers-id>/location/<location>/deviceGroups/<device-Group>/devices/<name-field>	- sys_object_source - cmdb_ot_entity - cmdb_key_value_v2	sys_object_source の SNK cmdb_ot_entity discovery_source_id	デバイスの一意の ID。
resourceGroup	(空)	cmdb_key_value_v2	(空)	リソースグループ
tenantId	(空)	cmdb_key_value_v2	(空)	テナント ID
properties.authorizedState	文字列	cmdb_key_value_v2	(空)	デバイスの認可済みステータス
properties.criticality	文字列	cmdb_ot_entity	business_criticality	デバイスの重要度
properties.deviceName	文字列	cmdb_ci	名前	デバイスの名前。
properties.deviceSubtype	文字列	cmdb_ci	sys_class_name	デバイスサブタイプの表示名。

デバイス属性マッピング (続く)

ペイロードフィールド名	データタイプ	テーブルへのマッピング	フィールドにマッピング	説明
properties.firstSeen	文字列としての日時	- cmdb_ci - cmdb_ci_ot_control_module (コントロールモジュールが存在する場合)	first_discovered	デバイスが初めて確認されたとき。
properties.lastSeen	文字列としての日時	- cmdb_ci - cmdb_ci_ot_control_module (コントロールモジュールが存在する場合)	most_recent_discovered	デバイスが最後に確認された時間。
properties.purdueLevel	文字列	cmdb_ot_entity	purdue_level	デバイスの Purdue レベル。
properties.operatingSystem.distribution	文字列	cmdb_ci_computeros		OS ディストリビューション
properties.operatingSystem.version	文字列	cmdb_ci_computeros_version		OS バージョン
properties.operatingSystem.platform	文字列	cmdb_ci_computeros_domain		OS プラットフォーム
properties.operatingSystem.architecture	文字列	cmdb_ci_computeros_address_width		OS アーキテクチャ
properties.additionalFields.plcKeyState	(空)	cmdb_ci_ot_plc	switch_position	PLC キーステータス
properties.additionalFields.plcRunState	(空)	cmdb_ci_ot_plc	switch_remote_monitoring	PLC の実行状況
properties.hardwareObject	オブジェクト	(空)	(空)	デバイスのハードウェアデータ
properties.hardwareModel	文字列	cmdb_ci	(空)	ハードウェアモデル
properties.hardwareSerialNumber	文字列	cmdb_serial_number	serial_number	ハードウェアのシリアル番号
properties.hardwareVendor	文字列	cmdb_ci	メーカー	ハードウェアベンダー
properties.nics	オブジェクトの阵列	(空)	(空)	デバイスネットワークインターフェイスカードのリスト。
properties.nics[{}]	オブジェクト	(空)	(空)	ネットワークインターフェイスカードのプロパティ
properties.nics[{}].address	文字列	cmdb_ci_ip_address	ip_address	IPv4 アドレス

デバイス属性マッピング (続く)

ペイロードフィールド名	データタイプ	テーブルへのマッピング	フィールドにマッピング	説明
properties.nics[{}]	文字列	Address	cmdb_ci_network_name	MAC アドレス
properties.slots	オブジェクトのレイ	(空)	(空)	バックプレーンのデバイススロットのリスト。
properties.slots[{}]	オブジェクト	(空)	(空)	PLCバックプレーンのスロットデータ。
properties.slots[{}]	文字列	FirmwareVersion	cmdb_ci_ot_control_module_version	スロットのファームウェアバージョン。
properties.slots[{}]	文字列	Model	cmdb_ci_ot_control_module_model	スロットのモデル。
properties.slots[{}]	整数	BackNumber	cmdb_ci_ot_control_rack_number	バックプレーン内のラック番号
properties.slots[{}]	文字列	SerialNumber	cmdb_ci_ot_control_serial_number	スロットのシリアル番号。
properties.slots[{}]	整数	SlotNumber	cmdb_ci_ot_control_slot_number	ラック内のスロット番号。
properties.slots[{}]	文字列	FirmwareVendor	cmdb_ci_ot_control_module_vendor	スロットのハードウェアベンダー。

デバイスタイプ分類

Microsoft Azure デバイスサブタイプ名	Microsoft Azure デバイスタイプ名	オペレーティングシステム/ファームウェア
アラームサイレン	(空)	(空)
アラームシステム	(空)	(空)
ATM	(空)	(空)
バックアップサーバー	(空)	(空)

デバイスタイプ分類 (続く)

Microsoft Azure デ バイスサ ブタイプ 名	Microsoft Azure デ バイスタ イプ名	オペレーティングシステム/ファームウェア
バーコー ドスキャ ナー	(空)	(空)
DB サー バー	(空)	(空)
DCS コ ントロー ラ	産業	(空)
ドメイ ンコント ローラ	(空)	(空)
ドアコン トロール パネル	(空)	(空)
DVR	(空)	(空)
エレベーター	(空)	(空)
エンジ ニアリン グステー ション	産業	(空)
火災警報	(空)	(空)
火災検知 器	(空)	(空)
ファイア ウォール	(空)	(空)
ゲームコ ンソール	(空)	(空)
履歴担当 者	(空)	(空)
HMI	産業	(空)
湿度セン サー	(空)	(空)
HVAC	(空)	(空)

自動翻訳

デバイスタイプ分類 (続く)

Microsoft Azure デ バイスサ ブタイプ 名	Microsoft Azure デ バイスタ イプ名	オペレーティングシステム/ファームウェア
I/O アダ プター	(空)	(空)
IED	(空)	(空)
産業用包 装システ ム	(空)	(空)
産業用ロ ボット	(空)	(空)
産業規模	(空)	(空)
インター ホン	(空)	(空)
IP カメ ラ	(空)	(空)
IP 電話	(空)	(空)
範囲	(空)	(空)
メートル	(空)	(空)
モーショ ンディテ クター	(空)	(空)
マルチ キャスト/ ブ ロード キャスト	(空)	(空)
NTP サーバー	(空)	(空)
ピープル カウ	(空)	(空)

デバイスタイプ分類 (続く)

Microsoft Azure デ バイスサ ブタイプ 名	Microsoft Azure デ バイスタ イプ名	オペレーティングシステム/ファームウェア
ターシス テム		
物理的な 場所	(空)	(空)
PLC	産業	(空)
空気圧装 置	(空)	(空)
プリン ター	(空)	(空)
プロト コルコン バーター	(空)	(空)
パンチク ロック	(空)	(空)
ロボッ トコント ローラー	(空)	(空)
ルーター	(空)	(空)
RTU	(空)	(空)
サーバー	サーバー	(空)
サーボド ライブ	(空)	(空)
スロット	(空)	(空)

自動翻訳

デバイスタイプ分類 (続く)

Microsoft Azure デ バイスサ ブタイプ 名	Microsoft Azure デ バイスタ イプ名	オペレーティングシステム/ファームウェア
スマート ライト	(空)	(空)
スマート フォン	(空)	(空)
スマート スイッチ	(空)	(空)
スマート テレビ	(空)	(空)
ストレージ	(空)	(空)
スイッチ	ネット ワークデ バイス	(空)
タブレッ ト	(空)	(空)
終着駅	(空)	(空)
サーモス タット	(空)	(空)
回転式改 札口	(空)	(空)
無停電電 源装置	(空)	(空)
可変周波 数ドライ ブ	(空)	(空)
VPN ゲート ウェイ	(空)	(空)
Wifi パ イナッ プル	(空)	(空)

自動翻訳

デバイスタイプ分類 (続く)

Microsoft Azure デバイスサブタイプ名	Microsoft Azure デバイスタイプ名	オペレーティングシステム/ファームウェア
無線アクセスポイント	(空)	(空)
WLAN アクセスポイント	ネットワークデバイス	(空)
ワークステーション	ワークステーション	(空)
不明	すべて	(空)
未分類	未分類またはすべて	(空)
その他のタイプ	(空)	(空)
上記のタイプ値 (ネットワークとIoTの指定を除く)	(空)	• Windows サーバー • Windows Server、バージョン2004[8] • Windows Serverバージョン1909[9] • Windows Serverバージョン1903[9] • Windows サーバー 2019 • Windows サーバー 2016 • Windows Server 2012 R2 • Windows Server 2012

デバイスタイプ分類 (続く)

Microsoft Azure デバイスタイプ名	Microsoft Azure デバイスタイプ名	オペレーティングシステム/ファームウェア
		• Windows Server 2008 R2 • Windows Server 2008 • Windows Server 2003 R2 • Windows Server 2003 • Windows 2000 サーバー • Windows NT 4.0 サーバー • Windows NT 3.51 サーバー • Windows NT 3.5 サーバー • Windows NT 3.1 サーバー
上記のタイプ値 (ネットワークと IoT の指定を除く)	(空)	• Linux • arch • centos • デビアン • 中折れ帽子 • SUSE • Red Hat • RHEL • Ubuntu • オラクル
上記のタイプ値 (ネットワークと IoT の指定を除く)	(空)	AIX
上記のタイプ値 (ネットワークと IoT の指定を除く)	(空)	ESX

デバイスタイプ分類 (続く)

Microsoft Azure デ バイスサ ブタイプ 名	Microsoft Azure デ バイスタ イプ名	オペレーティングシステム/ファームウェア
IoT の指 定を除 く)		
上記のタ イプ値 (ネット ワークと IoT の指 定を除 く)	(空)	• HP/UX • HPUX
上記のタ イプ値 (ネット ワークと IoT の指 定を除 く)	(空)	• Hyper-V • HyperV • 超
上記のタ イプ値 (ネット ワークと IoT の指 定を除 く)	(空)	• Solaris • スノス • スノス

デバイスタイプ分類 (続く)

Microsoft Azure デ バイスサ ブタイプ 名	Microsoft Azure デ バイスタ イプ名	オペレーティングシステム/ファームウェア
上記のタ イプ値 (ネット ワークと IoT の指 定を除 く)	(空)	• macOS X サーバー • macOS サーバー • OS X • osx
上記のタ イプ値 (ネット ワークと IoT の指 定を除 く)	(空)	• UNIX • ヌー
上記のタ イプ値 (ネット ワークと IoT の指 定を除 く)	(空)	• 勝つ • windows • Microsoft • Windows 1.0、1.02、1.03、1.04、2.03、2.10、2.11、3.0、3.1、3.2、7、8、8.1、10、98、95 • Windows 2000 • ワークグループ用の Windows 3.11 • Windows Me • Windows NT 3.1、3.5、3.51、4.0 • Windows Vista の場合 • Windows XP • Windows XP Professional x64 エディション
上記のタ イプ値 (ネット ワークと	(空)	サーバー

自動翻訳

デバイスタイプ分類 (続く)

Microsoft Azure デ バイスサ ブタイプ 名	Microsoft Azure デ バイスタ イプ名	オペレーティングシステム/ファームウェア
IoT の指 定を除 く)		

サービスグラフ **Connector for Microsoft Defender for IoT** (オンプレミス管理コンソール)

Microsoft Defender for IoT (オンプレミス管理コンソール) を ServiceNow オペレーショナルテクノロジーマネージャー アプリケーションと統合して、センサーアプライアンス、OT デバイス、ネットワーク接続のインポートを自動化します。

ストアでアプリを要求する

[ServiceNow Store](#) Web サイトにアクセスして、利用可能なすべてのアプリを表示し、要求をストアに送信する方法について確認してください。リリースされたすべてのアプリのこれまでのリリースノート情報については、「[ServiceNow Store のバージョン履歴リリースノート](#)」を参照してください。

サポート対象のバージョン

Microsoft Defender for IoT (オンプレミス管理コンソール) バージョン:10.5.2 以降

ユースケース

ServiceNow オペレーショナルテクノロジーマネージャー アプリケーションで サービスグラフ Connector for Microsoft Defender for IoT (オンプレミス管理コンソール) を使用して、センサーアプライアンス、OT デバイス、ネットワーク接続をインポートできます。

ガイド付きセットアップ

サービスグラフ Connector for Microsoft Defender for IoT (オンプレミス管理コンソール) のガイド付きセットアップでは、インスタンスで統合を構成するための整理された一連のタスクが提供されます。ガイド付きセットアップにアクセスするには、「[ガイド付きセットアップの構成](#)」を参照してください。

CMDB 統合ダッシュボード

CMDB 共通統合 ストアアプリは、インストールされているすべての統合のステータス、処理結果、および処理エラーを一元的に表示するダッシュボードを提供します。すべての統合実行のメトリクスを確認することができます。特定の CMDB 統合、特定の期間、または特定の統合実行に関してビューをフィルタリングすることもできます。CMDB 統合ダッシュボードでの統合の監視の詳細については、「[CMDB 共通統合](#)」を参照してください。

データマッピング

Microsoft Defender for IoT (オンプレミス管理コンソール) データソースのデータは、強力な変換エンジン (RTE) を使用してマッピングされ、ServiceNow CMDB 構成アイテム (CI) クラス定義に変換されます。データは、識別および調整エンジン (IRE) を使用して ServiceNow CMDB に挿入されます。

セットアップが完了したら、Microsoft Defender for IoT (オンプレミス管理コンソール) アプリケーションから定期的にデータをプルするように統合を構成できます。

次の表に、Microsoft Defender for IoT (オンプレミス管理コンソール) プロジェクトに含まれるデータソースと、インポートされたデータが読み込まれる対応するステージングテーブルを示します。

Microsoft Defender for IoT のデータソースとステージングテーブル (オンプレミス管理コンソール)

データソース	ステージングテーブル
SG-OT Microsoft D4IoT 接続インポート	SG-OT Msft D4IoT 接続インポート [sn_msftd4iotsgc_sg_ot_msft_d4iot_connections_import]
SG-OT Microsoft D4IoT デバイスインポート	SG-OT Msft D4IoT デバイスインポート [sn_msftd4iotsgc_sg_ot_msft_d4iot_devices_import]
SG-OT Microsoft D4IoT センサーインポート	SG-OT Msft D4IoT センサーインポート [sn_msftd4iotsgc_sg_ot_msft_d4iot_sensors_import]

ステージングテーブルからインポートされたデータは、次のターゲットテーブルに挿入されます。

- AIX サーバー [cmdb_ci_aix_server]
- コンピューター [cmdb_ci_computer]
- 構成アイテム (CI) [cmdb_ci]
- DCS [cmdb_ci_ot_dcs]
- ESX サーバー [cmdb_ci_esx_server]
- EWS [cmdb_ci_ot_ews]
- 外部システムメタデータ [cmdb_key_value_v2]
- ゲームコンソール [cmdb_ci_game_console]
- ハンドヘルドコンピューティングデバイス [cmdb_ci_handled_computing]
- 履歴担当者 [cmdb_ci_ot_historian]
- HMI [cmdb_ci_ot_hmi]
- HP-UX サーバー [cmdb_ci_hpux_server]
- HVAC機器 [cmdb_ci_hvac]
- HyperV サーバー [cmdb_ci_hyper_v_server]
- IED [cmdb_ci_ot_ied]
- 産業用アクチュエーター [cmdb_ci_ot_industrial_actuator]
- 産業用ドライブ [cmdb_ci_ot_industrial_drive]
- 産業用ロボット [cmdb_ci_ot_industrial_robot]
- 産業用センサー [cmdb_ci_ot_industrial_sensor]

- IoT デバイス [cmdb_ci_iot]
- IP アドレス [cmdb_ci_ip_address]
- IP カメラ [cmdb_ci_ip_camera]
- IP ファイアウォール [cmdb_ci_ip_firewall]
- IP フォン [cmdb_ci_ip_phone]
- Linux サーバー [cmdb_ci_linux_server]
- ネットギア [cmdb_ci_netgear]
- ネットワークアダプタ [cmdb_ci_network_adapter]
- ネットワーク侵入検知システム [cmdb_ci_nids]
- オペレーショナルテクノロジー (OT) [cmdb_ci_ot]
- OSX サーバー [cmdb_ci_osx_server]
- OT コントロールモジュール [cmdb_ci_ot_control_module]
- OT コントロールシステム [cmdb_ci_ot_control]
- OT デバイスの詳細 [cmdb_ot_entity]
- OT フィールドデバイス [cmdb_ci_ot_field_device]
- PLC [cmdb_ci_ot_plc]
- プリンター [cmdb_ci_printer]
- RTU [cmdb_ci_ot_rtu]
- シリアル番号 [cmdb_serial_number]
- サーバー [cmdb_ci_server]
- サーバー [cmdb_ci_server]
- Solaris サーバー [cmdb_ci_solaris_server]
- ソース [sys_object_source]
- Unix Server [cmdb_ci_unix_server]
- 無停電電源装置 (UPS) [cmdb_ci_ups]
- 無線アクセスポイント [cmdb_ci_wap_network]

Microsoft Defender for IoT (オンプレミス管理コンソール) プロジェクトからデータをプルするときにデータが保存される場所の詳細については、「[対象となる CMDB クラス](#)」を参照してください。

Microsoft Defender for IoT (On-premises Management Console) のサービスグラフコネクタの構成

Microsoft Defender for IoT (On-premises Management Console) のサービスグラフコネクタのガイド付きセットアップを使用して、統合手順を案内します。

始める前に

依存関係と要件：

- 自動的にインストールされる [CMDB 共通統合](#) ストアアプリ。
- 自動的にインストールされる [CMDB CI クラスモデル](#)。

- ITOMディスカバリーライセンスプラグイン (com.snc.itom.discovery.license)。このプラグインを有効にする必要があります。
- ITOM Licensing プラグイン (com.snc.itom.license)。詳細については、「[ディスカバリーの要求](#)」を参照してください。
- 自動的にインストールされる Datastream Action プラグイン (com.glide.hub.action_type.datastream)。

必要なロール：admin

- i** 注：Microsoft Defender for IoT (On-premises Management Console) のサービスグラフコネクタ の以前のバージョンを使用している場合は、古いコネクタからデータを移行しないでください。以前のバージョンをアンインストールし、新しい統合を実行する必要があります。

手順

1. アプリケーションピッカーを使用して、アプリケーションスコープを Microsoft Defender for IoT (On-premises Management Console) のサービスグラフコネクタ アプリケーションに設定します。
詳細については、「[アプリケーションピッカー](#)」を参照してください。
2. 移動先 すべて > サービスグラフコネクタ **Microsoft D4IoT** > ガイド付きセットアップ。
3. [はじめに] ページで、[開始] を選択します。
4. MID サーバーを設定するには、次の手順を実行します。
 - a. [接続と認証情報のセットアップ] セクションで、[MID サーバーの構成] タスクを選択します。
 - b. 説明にリンクされているMID サーバー構成を完了したら、[完了としてマーク] を選択します。
5. 接続および資格情報エイリアスレコードを更新するには、次の手順を実行します。
 - a. [接続および認証情報のセットアップ] セクションで、[接続および認証情報] タスクを選択します。
 - b. **[Configure]** を選択します。
 - c. デフォルトのレコード **Microsoft D4IoT Base API** を開きます。
 - d. [接続] 関連リストから [新規] を選択して、新しい HTTP(S) 接続レコードを作成します。
 - e. [接続 URL] フィールドに、Microsoft Defender for IoT Central Manager の URL の名前を入力します。
例: https://192.168.1.100。
 - f. オプション: MID サーバーを使用している場合は、次のすべてを選択します。
 - **[MID サーバーを使用]** ボックス
 - [MID サーバー詳細構成] 関連リストからの **MID** サーバー
 - リストからの **MID** の選択
 - g. [認証情報] フィールドで、検索アイコンを選択して認証情報レコードリストを開きます。
 - h. [新規] を選択して、新しいレコードを作成します。

- i. **[API キー認証情報]** タイプを選択します。
 - j. **[API キー]** フィールドに、Microsoft Defender for IoT 管理コンソールから提供された名前と API キーを入力します。
 - k. **[送信]** を選択して認証情報レコードを作成します。
Microsoft Defender for IoT管理コンソールで API キーを作成するには、Microsoft製品ドキュメントの <https://docs.microsoft.com/en-us/azure/defender-for-iot/organizations/references-work-with-defender-for-iot-apis> を参照してください。
 - l. 接続フォームで、**[送信]** を選択して接続レコードの作成を終了します。
6. 接続をテストするには、次の手順を実行します。
- a. **[接続と資格情報のセットアップ]** セクションで、**[接続のテスト/検証]** タスクを選択します。
 - b. センサーのデータソースレコードの関連リンクセクションから **[テスト接続]** UI アクションを選択します。
接続テストが完了したら、結果を表示します。テスト結果が「成功」を返すまで、推奨されるトラブルシューティング手順を実行する必要があります。
 - c. 接続マネージャーに有効な証明書があることを確認してください。

本番環境には有効な証明書をインストールする必要があります。非本番インスタンスまたは概念実証 (POC) インスタンスの場合、接続マネージャーに有効な証明書がない場合に統合が機能するようにシステムプロパティを構成できます。次の表に、非本番環境で構成できるシステムプロパティを示します。

非本番環境のシステムプロパティ

プロパティ	値
com.glide.communications.httpClient.verify_certificate	false に設定します。
com.glide.communications.httpClient.verify_certificate	false に設定します。
	このシステムプロパティを追加する必要がある場合は、「 システムプロパティの追加 」を参照してください。
com.glide.communications.trustmanager_trustAll	true に設定します。

- d. MID セキュリティポリシーを確認します。
イントラネットレコードで、次の表の列に指定された値が表示されていることを確認します。

イントラネットレコード値

列	値
証明書チェーンチェック	誤り
ホスト名チェック	誤り
失効チェック	誤り

詳細については、「[MID サーバー証明書チェックポリシー](#)」を参照してください。

進行状況ウィンドウに完了コード「成功」が表示され、処理されたレコードの数が 接続マネージャーで同じ数のセンサーとして表示される場合、接続は正しく設定されていることが示される。

7. システムプロパティを設定するには、次の手順を実行します。

- a. [システムプロパティの構成] セクションで、[構成] を選択します。
- b. 次のシステムプロパティを構成します。

プロパティ	説明
sn_msftd4iotsgc.resourcepath.sensor	センサーリソースパスを設定します。 - センサーリソースパスは、V3 API バージョンにデフォルトで提供されます。 - 別の API バージョンを使用する場合は、パスを上書きできます。
sn_msftd4iotsgc.resourcepath.device	- デバイスリソースパスは、V3 API バージョンにデフォルトで提供されます。 - 別の API バージョンを使用する場合は、パスを上書きできます。
sn_msftd4iotsgc.resourcepath.connection	- 接続リソースパスは、V3 API バージョンにデフォルトで提供されます。 - 別の API バージョンを使用する場合は、パスを上書きできます。
sn_msftd4iotsgc.pagesize.device	各デバイスと接続 API のページごとに表示するレコードの数を入力します。デフォルト値: ページあたり 50 レコード
sn_msftd4iotsgc.pagesize.connection	- 接続および認証情報レコードの設定中に構成された Microsoft D4IoT Base API とは異なる接続エイリアスを使用する場合は、このプロパティフィールドにカスタム接続エイリアスレコードのsys_idを入力できます。 - このプロパティのデフォルト値は空です。このプロパティフィールドを空白のままにすると、Microsoft D4IoT Base API 接続エイリアスがデフォルトで使用されます。
sn_msftd4iotsgc.get_all_devices	デバイスのすべてのレコードをフェッチするか、前回成功したインポートの開始時刻以降の新しいレコードのみをフェッチするかを選択します。

プロパティ	説明
	i 注: デバイスを初めてインポートすると、このプロパティの設定に関係なく、すべてのレコードがインポートされます。
sn_msftd4iotsgc.get_all_connections	接続のすべてのレコードをフェッチするか、CMDB内で最後に成功したインポートの開始時刻以降の新しいレコードのみをフェッチするかを選択します。 i 注: 接続を初めてインポートすると、このプロパティの設定に関係なく、すべてのレコードがインポートされます。
sn_msftd4iotsgc.ot.vr.integration.id	Microsoft Defender for IoT 統合の サービスグラフ で オペレーショナルテクノロジー脆弱性対応 アプリケーションを使用している場合は、OT VR インポートレコードの sys ID を指定します。 i 注: オペレーショナルテクノロジー脆弱性対応 プラグインがインストールされていて、このプロパティフィールドが空白のままになっている場合、レコードで [アクティブ] が true に設定されていれば、Microsoft D4IoT デバイス CVE 統合 (デルタインポート) が実行されます。

c. [Save (保存)] を選択します。

8. センサーをインポートするには、次の手順を実行します。

- a. [センサーの構成 (NIDS)] セクションで、[センサーのインポート] タスクを選択します。
- b. [Configure] を選択します。
- c. [アクティブ] を選択して、スケジュール設定済みデータインポートジョブをアクティブにします。

9. NIDS を構成するには、次の手順を実行します。

- a. [センサーの構成 (NIDS)] セクションで、[センサーのインポート] タスクを選択します。
- b. 説明にリンクされている NIDS 構成を完了したら、[完了としてマーク (Mark as complete)] を選択します。

10. インポートスケジュールを設定するには、次の手順を実行します。

- a. [インポートスケジュールの構成] セクションで、[構成] を選択します。
- b. [SG-OT Microsoft D4IoT センサーのスケジュール済みインポート] を選択して、必要に応じてセンサーインポートスケジュールを確認または変更します。

- デフォルトでは、センサーのインポートスケジュールは毎日深夜に実行されるように設定されています。
- デバイスまたは接続をインポートする前にセンサーをインポートします。

c. [アクティブ] を選択して、センサーインポートスケジュールをアクティブにします。

d. **[SG-OT Microsoft D4IoT デバイスのスケジュール済みインポート]** を選択して、必要に応じてデバイスのインポートスケジュールを確認または変更します。

- デフォルトでは、デバイスのインポートスケジュールは毎日深夜に実行されるように設定されています。
- デバイスはセンサーによってクエリされます。サービスグラフコネクタは、検証済みセンサーによって検出されたデバイスを照会します。ネットワーク侵入検知システム (NIDS) アプリケーションの構成については、「[NIDS の検証](#)」を参照してください。

e. [アクティブ] を選択して、デバイスのインポートスケジュールをアクティブにします。

f. **[SG-OT Microsoft D4IoT 接続スケジュール済みインポート]** を選択して、必要に応じて接続インポートスケジュールを確認または変更します。

- デフォルトでは、接続のインポートスケジュールは、デバイスのインポートの実行後 (親の実行後) に実行されるように構成されています。
- 接続は、両方のデバイス (Microsoft API の [送信元と宛先] または CMDB の [親と子]) が既に CMDB にある場合にのみインポートされます。
- 接続をインポートする前にデバイスをインポートします。

CMDB での対象となるクラス **Microsoft Defender for IoT (On-premises Management Console)** のサービスグラフコネクタ

ガイド付きセットアップを完了したら、Microsoft Defender for IoT (オンプレミス管理コンソール) プロジェクトから定期的にデータをプルするように統合を構成できます。データは、構成アイテム [cmdb_ci] テーブルから拡張されたテーブルに保存されます。

コンピューター [cmdb_ci_computer]

コンピューター [cmdb_ci_computer] テーブルの次の属性は、収集されたデータによって設定されます。

コンピューター [cmdb_ci_computer] 属性

属性ラベル	属性の名前
最新のディスカバリー	last_discovered
オペレーティングシステム	os
OS アドレス幅 (ビット)	os_address_width
OS ドメイン	os_domain
OS バージョン	os_version

外部システムメタデータ [cmdb_key_value_v2]

外部システムメタデータ [cmdb_key_value_v2] テーブルの次の属性は、収集されたデータによって設定されます。

外部システムメタデータ [cmdb_key_value_v2] 属性

属性ラベル	属性の名前
ディスカバリーソース	discovery_source
キー	キー
ソースキー	source_key
文字列値	string_value
URL 値	url_value
値のタイプ	value_type

ハードウェア [cmdb_ci_hardware]

ハードウェア [cmdb_ci_hardware] テーブルの次の属性は、収集されたデータによって設定されます。

ハードウェア [cmdb_ci_hardware] 属性

属性ラベル	属性の名前
クラス	sys_class_name
モデル番号	model_number
最新検出日	last_discovered
場所	場所
モデル ID	model_id
メーカー	メーカー
最初の検出	first_discovered
所有者	owned_by
承認グループ	change_control
グループによる管理	managed_by_group
管理担当者	managed_by
名前	名前
会社	会社
サポートグループ	support_group
変更グループ	assignment_group
アサイン先	assigned_to
サポート担当者	supported_by

ハードウェアに対して作成された関係

親クラス	関係性タイプ	子クラス
ハードウェア [cmdb_ci_hardware]	Owns::Owned by	IP アドレス [cmdb_ci_ip_address]

ハードウェアに対して作成された関係 (続く)

親クラス	関係性タイプ	子クラス
ハードウェア [cmdb_ci_hardware]	Owens::Owned by	ネットワークアダプタ [cmdb_ci_network_adapter]
ハードウェア [cmdb_ci_hardware]	参照	外部システムメタデータ [cmdb_key_value_v2]
ハードウェア [cmdb_ci_hardware]	参照	OT デバイス [cmdb_ot_entity]

IP アドレス [cmdb_ci_ip_address]

IP アドレス [cmdb_ci_ip_address] テーブルの次の属性は、収集されたデータによって設定されます。

IP アドレス [cmdb_ci_ip_address] 属性

属性ラベル	属性の名前
IP アドレス	ip_address
IP バージョン	ip_version
構成アイテムが所有	owned_by_cmdb_ci

IP アドレス用に作成された関係

親クラス	関係性タイプ	子クラス
IP アドレス [cmdb_ci_ip_address]	参照	ネットワーク侵入検知システム [cmdb_ci_nids]
IP アドレス [cmdb_ci_ip_address]	参照	ハードウェア [cmdb_ci_hardware]

ネットワークアダプタ [cmdb_ci_network_adapter]

ネットワークアダプタ [cmdb_ci_network_adapter] テーブルの次の属性は、収集されたデータによって設定されます。

ネットワークアダプタ [cmdb_ci_network_adapter] 属性

属性ラベル	属性の名前
MAC アドレス	mac_address
名前	name
ディスカバリーソース	discovery_source

ネットワークアダプタ用に作成された関係

親クラス	関係性タイプ	子クラス
ネットワークアダプタ [cmdb_ci_network_adapter]	参照	ネットワーク侵入検知システム [cmdb_ci_nids]

ネットワークアダプタ用に作成された関係 (続く)

親クラス	関係性タイプ	子クラス
ネットワークアダプタ [cmdb_ci_network_adapter]	参照	ハードウェア [cmdb_ci_hardware]

ネットワーク侵入検知システム [cmdb_ci_nids]

ネットワーク侵入検知システム [cmdb_ci_nids] テーブルの次の属性は、収集されたデータによって設定されます。

ネットワーク侵入検知システム [cmdb_ci_nids] 属性

属性ラベル	属性の名前
最初の検出	first_discovered
NIDS ソース名	source_name
ライフサイクルステージ	life_cycle_stage
Life Cycle Stage Status (ライフサイクルステータス)	life_cycle_stage_status
名前	name
相関 ID	correlation_id
ファームウェアバージョン	firmware_version
完全修飾ドメイン名	fqdn
NIDS アサインゾーン	ゾーン
NIDS マネージャー接続ステータス	connection_state
検証済み	検証済み
メーカー	メーカー

NIDS 用に作成された関係

親クラス	関係性タイプ	子クラス
ネットワーク侵入検知システム [cmdb_ci_nids]	検出::Detected	ハードウェア [cmdb_ci_hardware]
ネットワーク侵入検知システム [cmdb_ci_nids]	Owns::Owned by	IP アドレス [cmdb_ci_ip_address]
ネットワーク侵入検知システム [cmdb_ci_nids]	Owns::Owned by	ネットワークアダプタ [cmdb_ci_network_adapter]

オペレーショナルテクノロジー (OT) [cmdb_ci_ot]

オペレーショナルテクノロジー (OT) [cmdb_ci_ot] テーブルの次の属性は、収集されたデータによって設定されます。

オペレーショナルテクノロジー (OT) [cmdb_ci_ot] 属性

属性ラベル	属性の名前
最新のディスカバリー	last_discovered

OT コントロールモジュール [cmdb_ci_ot_control_module]

OT コントロールモジュール [cmdb_ci_ot_control_module] テーブルの次の属性は、収集されたデータによって設定されます。

OT コントロールモジュール [cmdb_ci_ot_control_module] 属性

属性ラベル	属性の名前
ベンダー	ベンダー
サポートグループ	support_group
シリアル番号	serial_number
クラス	sys_class_name
最初の検出	first_discovered
承認グループ	change_control
管理担当者	managed_by
グループによる管理	managed_by_group
変更グループ	assignment_group
会社	会社
ラック番号	rack_number
スロット番号	slot_number
場所	場所
名前	名前
ファームウェアバージョン	firmware_version
最新検出日	last_discovered
アサイン先	assigned_to
所有者	owned_by
サポート担当者	supported_by
モデル ID	model_id

OT コントロールモジュール用に作成された関係

親クラス	関係性タイプ	子クラス
OT コントロールモジュール [cmdb_ci_ot_control_module]	参照	OT デバイス [cmdb_ot_entity]

OT コントロールシステム [cmdb_ci_ot_control]

OT コントロールシステム [cmdb_ci_ot_control] テーブルの次の属性は、収集されたデータによって設定されます。

OT コントロールシステム [cmdb_ci_ot_control] 属性

属性ラベル	属性の名前
モジュールあり	has_module
最新検出日	last_discovered

OT コントロールシステム用に作成された関係

親クラス	関係性タイプ	子クラス
OT コントロールシステム [cmdb_ci_ot_control]	Owens::Owned by	OT コントロールモジュール [cmdb_ci_ot_control_module]

OT デバイス [cmdb_ot_entity]

OT デバイス [cmdb_ot_entity] テーブルの次の属性は、収集されたデータによって設定されます。

OT デバイス [cmdb_ot_entity] 属性

属性ラベル	属性の名前
ISA エンティティサイト	isa_entity_site
OT ディスカバリーソース ID	ot_correlation_id
デバイスの重要度	business_criticality
Purdue レベル	purdue_level
ゾーン	ゾーン
OT デバイスタイプ	ot_asset_type

PLC [cmdb_ci_ot_plc]

PLC [cmdb_ci_ot_plc] テーブルの次の属性は、収集されたデータによって設定されます。

PLC [cmdb_ci_ot_plc] 属性

属性ラベル	属性の名前
最新のディスカバリー	last_discovered
スイッチ位置	switch_position
リモートスイッチ	switch_remote_mode

シリアル番号 [cmdb_serial_number]

シリアル番号 [cmdb_serial_number] テーブルの次の属性は、収集されたデータによって設定されます。

シリアル番号 [cmdb_serial_number] 属性

属性ラベル	属性の名前
シリアル番号	serial_number
シリアル番号タイプ	serial_number_type
有効	valid

シリアル番号用に作成された関係

親クラス	関係性タイプ	子クラス
シリアル番号 [cmdb_serial_number]	参照	ハードウェア [cmdb_ci_hardware]
ネットワークアダプタ [cmdb_ci_network_adapter]	参照	ハードウェア [cmdb_ci_hardware]

の属性マッピングと分類 **Microsoft Defender for IoT (On-premises Management Console)** のサービスグラフコネクタ

次の表に、センサーとデバイスの属性マッピングと分類を示します。

センサー属性マッピング

ペイロードフィールド名	データタイプ	テーブルへのマッピング	フィールドにマッピング	説明
ID	文字列形式: ./subscriptions/<subscription-id>/provider/<provider>/locations/<location>/sites/<site>/sensor/<sensor-name>	- sys_object_source - cmdb_ci_nids	sys_object_source の SNK correlation_id	センサーの一意的 ID。
名前	文字列	cmdb_ci_nids	名前	センサーの名前。
properties.hostname	文字列	cmdb_ci_nids	fqdn	センサーのホスト名。
properties.ip	文字列	cmdb_ci_ip_address	ip_address	センサーの IP アドレス。
properties.learningMode	ブール値	cmdb_ci_nids	False または利用不可: ライフサイクルステージ (life_cycle_stage): 運用 ライフサイクルステータス (life_cycle_stage_status): 使用中	IoT センサーのラーニングモードステータス。

センサー属性マッピング (続く)

ペイロードフィールド名	データタイプ	テーブルへのマッピング	フィールドにマッピング	説明
			True : ライフサイクルステージ (life_cycle_stage): 運用 ライフサイクルステータス (life_cycle_stage_status): ラーニング	
properties.mac	文字列	cmdb_ci_network_adapter	名前、mac_address	センサーの MAC アドレス。
properties.sensorStatus	文字列	cmdb_ci_nids	connection_state	IoT センサーのステータス。
properties.sensorVersion	文字列	cmdb_ci_nids	firmware_version	IoT センサーのバージョン。
properties.upSince	文字列としての日時	cmdb_ci_nids	first_discovered	起動時間。
properties.zone	文字列	cmdb_ci_nids	ゾーン	IoT センサーのゾーン。

デバイス属性マッピング

ペイロードフィールド名	データタイプ	テーブルへのマッピング	フィールドにマッピング	説明
ID	文字列形式: /subscriptions/ subscription-id>/providers/ <providers-id>/location/ <location>/ deviceGroups/ <device-Group>/ devices/<name-field>	- sys_object_source - cmdb_ot_entity - cmdb_key_value_v2	sys_object_source の SNK cmdb_ot_entity discovery_source_id	デバイスの一意の ID。
resourceGroup	(空)	cmdb_key_value_v2	(空)	リソースグループ
tenantId	(空)	cmdb_key_value_v2	(空)	テナント ID
properties.authorizedState	文字列	cmdb_key_value_v2	(空)	デバイスの認可済みステータス
properties.criticality	文字列	cmdb_ot_entity	business_criticality	デバイスの重要度
properties.deviceName	文字列	cmdb_ci	名前	デバイスの名前。
properties.deviceSubtype	文字列	cmdb_ci	sys_class_name	デバイスサブタイプの表示名。

デバイス属性マッピング (続く)

ペイロードフィールド名	データタイプ	テーブルへのマッピング	フィールドにマッピング	説明
properties.firstSeen	文字列としての日時	- cmdb_ci - cmdb_ci_ot_control_module (コントロールモジュールが存在する場合)	first_discovered	デバイスが初めて確認されたとき。
properties.lastSeen	文字列としての日時	- cmdb_ci - cmdb_ci_ot_control_module (コントロールモジュールが存在する場合)	most_recent_discovered	デバイスが最後に確認された時間。
properties.purdueLevel	文字列	cmdb_ot_entity	purdue_level	デバイスの Purdue レベル。
properties.operatingSystem.distribution	文字列	cmdb_ci_computeros		OS ディストリビューション
properties.operatingSystem.version	文字列	cmdb_ci_computeros_version		OS バージョン
properties.operatingSystem.platform	文字列	cmdb_ci_computeros_domain		OS プラットフォーム
properties.operatingSystem.architecture	文字列	cmdb_ci_computeros_address_width		OS アーキテクチャ
properties.additionalFields.plcKeyState	数値	cmdb_ci_ot_plc	switch_position	PLC キーステータス
properties.additionalFields.plcRunState	数値	cmdb_ci_ot_plc	switch_remote_monitoring	PLC の実行状況
properties.hardwareObject	オブジェクト	(空)	(空)	デバイスのハードウェアデータ
properties.hardwareModel	文字列	cmdb_ci	(空)	ハードウェアモデル
properties.hardwareSerialNumber	文字列	cmdb_serial_number	serial_number	ハードウェアのシリアル番号
properties.hardwareVendor	文字列	cmdb_ci	メーカー	ハードウェアベンダー
properties.nics	オブジェクトの阵列	(空)	(空)	デバイスネットワークインターフェイスカードのリスト。
properties.nics[{}]	オブジェクト	(空)	(空)	ネットワークインターフェイスカードのプロパティ
properties.nics[{}].address	文字列	cmdb_ci_ip_address	ip_address	IPv4 アドレス

デバイス属性マッピング (続く)

ペイロードフィールド名	データタイプ	テーブルへのマッピング	フィールドにマッピング	説明
properties.nics[{}]	文字列	Address	cmdb_ci_network_name	MAC アドレス
properties.slots	オブジェクトのレイ	(空)	(空)	バックプレーンのデバイススロットのリスト。
properties.slots[{}]	オブジェクト	(空)	(空)	PLCバックプレーンのスロットデータ。
properties.slots[{}]	文字列	FirmwareVersion	cmdb_ci_ot_control_module_version	スロットのファームウェアバージョン。
properties.slots[{}]	文字列	Model	cmdb_ci_ot_control_module_model	スロットのモデル。
properties.slots[{}]	整数	Number	cmdb_ci_ot_control_rack_number	バックプレーン内のラック番号
properties.slots[{}]	文字列	Number	cmdb_ci_ot_control_serial_number	スロットのシリアル番号。
properties.slots[{}]	整数	Number	cmdb_ci_ot_control_slot_number	ラック内のスロット番号。
properties.slots[{}]	文字列	FirmwareVendor	cmdb_ci_ot_control_module_vendor	スロットのハードウェアベンダー。

デバイスタイプ分類

Microsoft Azure デバイスサブタイプ名	Microsoft Azure デバイスタイプ名	オペレーティングシステム/ファームウェア
アラームサイレン	(空)	(空)
アラームシステム	(空)	(空)
ATM	(空)	(空)
バックアップサーバー	(空)	(空)

デバイスタイプ分類 (続く)

Microsoft Azure デ バイスサ ブタイプ 名	Microsoft Azure デ バイスタ イプ名	オペレーティングシステム/ファームウェア
バーコー ドスキャ ナー	(空)	(空)
DB サー バー	(空)	(空)
DCS コ ントロー ラ	産業	(空)
ドメイ ンコント ローラ	(空)	(空)
ドアコン トロール パネル	(空)	(空)
DVR	(空)	(空)
エレベー ター	(空)	(空)
エンジ ニアリン グステー ション	産業	(空)
火災警報	(空)	(空)
火災検知 器	(空)	(空)
ファイア ウォール	(空)	(空)
ゲームコ ンソール	(空)	(空)
履歴担当 者	(空)	(空)
HMI	産業	(空)
湿度セン サー	(空)	(空)
HVAC	(空)	(空)

自動翻訳

デバイスタイプ分類 (続く)

Microsoft Azure デ バイスサ ブタイプ 名	Microsoft Azure デ バイスタ イプ名	オペレーティングシステム/ファームウェア
I/O アダ プター	(空)	(空)
IED	(空)	(空)
産業用包 装システ ム	(空)	(空)
産業用ロ ボット	(空)	(空)
産業規模	(空)	(空)
インター ホン	(空)	(空)
IP カメ ラ	(空)	(空)
IP 電話	(空)	(空)
範囲	(空)	(空)
メートル	(空)	(空)
モーショ ンディテ クター	(空)	(空)
マルチ キャスト/ ブ ロード キャスト	(空)	(空)
NTP サーバー	(空)	(空)
ピープル カウン	(空)	(空)

自動翻訳

デバイスタイプ分類 (続く)

Microsoft Azure デ バイスサ ブタイプ 名	Microsoft Azure デ バイスタ イプ名	オペレーティングシステム/ファームウェア
ターシス テム		
物理的な 場所	(空)	(空)
PLC	産業	(空)
空気圧装 置	(空)	(空)
プリン ター	(空)	(空)
プロト コルコン バーター	(空)	(空)
パンチク ロック	(空)	(空)
ロボッ トコント ローラー	(空)	(空)
ルーター	(空)	(空)
RTU	(空)	(空)
サーバー	サーバー	(空)
サーボド ライブ	(空)	(空)
スロット	(空)	(空)

デバイスタイプ分類 (続く)

Microsoft Azure デ バイスサ ブタイプ 名	Microsoft Azure デ バイスタ イプ名	オペレーティングシステム/ファームウェア
スマート ライト	(空)	(空)
スマート フォン	(空)	(空)
スマート スイッチ	(空)	(空)
スマート テレビ	(空)	(空)
ストレージ	(空)	(空)
スイッチ	ネット ワークデ バイス	(空)
タブレッ ト	(空)	(空)
終着駅	(空)	(空)
サーモス タット	(空)	(空)
回転式改 札口	(空)	(空)
無停電電 源装置	(空)	(空)
可変周波 数ドライ ブ	(空)	(空)
VPN ゲート ウェイ	(空)	(空)
Wifi パ イナッ プル	(空)	(空)

自動翻訳

デバイスタイプ分類 (続く)

Microsoft Azure デバイスサブタイプ名	Microsoft Azure デバイスタイプ名	オペレーティングシステム/ファームウェア
無線アクセスポイント	(空)	(空)
WLAN アクセスポイント	ネットワークデバイス	(空)
ワークステーション	ワークステーション	(空)
不明	すべて	(空)
未分類	未分類またはすべて	(空)
その他のタイプ	(空)	(空)
上記のタイプ値 (ネットワークとIoTの指定を除く)	(空)	• Windows サーバー • Windows Server、バージョン2004[8] • Windows Serverバージョン1909[9] • Windows Serverバージョン1903[9] • Windows サーバー 2019 • Windows サーバー 2016 • Windows Server 2012 R2 • Windows Server 2012

デバイスタイプ分類 (続く)

Microsoft Azure デバイスタイプ名	Microsoft Azure デバイスタイプ名	オペレーティングシステム/ファームウェア
		• Windows Server 2008 R2 • Windows Server 2008 • Windows Server 2003 R2 • Windows Server 2003 • Windows 2000 サーバー • Windows NT 4.0 サーバー • Windows NT 3.51 サーバー • Windows NT 3.5 サーバー • Windows NT 3.1 サーバー
上記のタイプ値 (ネットワークと IoT の指定を除く)	(空)	• Linux • arch • centos • デビアン • 中折れ帽子 • SUSE • Red Hat • RHEL • Ubuntu • オラクル
上記のタイプ値 (ネットワークと IoT の指定を除く)	(空)	AIX
上記のタイプ値 (ネットワークと IoT の指定を除く)	(空)	ESX

デバイスタイプ分類 (続く)

Microsoft Azure デバイスサブタイプ名	Microsoft Azure デバイスタ イプ名	オペレーティングシステム/ファームウェア
IoT の指定を除く)		
上記のタイプ値 (ネットワークと IoT の指定を除く)	(空)	• HP/UX • HPUX
上記のタイプ値 (ネットワークと IoT の指定を除く)	(空)	• Hyper-V • HyperV • 超
上記のタイプ値 (ネットワークと IoT の指定を除く)	(空)	• Solaris • スノス • スノス

デバイスタイプ分類 (続く)

Microsoft Azure デバイスサブタイプ名	Microsoft Azure デバイスタイプ名	オペレーティングシステム/ファームウェア
上記のタイプ値 (ネットワークと IoT の指定を除く)	(空)	• macOS X サーバー • macOS サーバー • OS X • osx
上記のタイプ値 (ネットワークと IoT の指定を除く)	(空)	• UNIX • ヌー
上記のタイプ値 (ネットワークと IoT の指定を除く)	(空)	• 勝つ • windows • Microsoft • Windows 1.0、1.02、1.03、1.04、2.03、2.10、2.11、3.0、3.1、3.2、7、8、8.1、10、98、95 • Windows 2000 • ワークグループ用の Windows 3.11 • Windows Me • Windows NT 3.1、3.5、3.51、4.0 • Windows Vista の場合 • Windows XP • Windows XP Professional x64 エディション
上記のタイプ値 (ネットワークと IoT の指定を除く)	(空)	サーバー

自動翻訳

デバイスタイプ分類 (続く)

Microsoft Azure デ バイスサ ブタイプ 名	Microsoft Azure デ バイスタ イプ名	オペレーティングシステム/ファームウェア
IoT の指 定を除 く)		

オペレーショナルテクノロジーマネージャーを使用する

オペレーショナルテクノロジー (OT) 拡張クラスのインストールやユーザーロールのアサインなど、必要なすべてのセットアップタスクを完了したら、次のタスクを実行して、ServiceNow オペレーショナルテクノロジー ソリューションの基盤データと関係を作成します。

タスク	目的
1. Microsoft Excel スプレッドシートに既存のオペレーショナルテクノロジー データを入力します。	既存のデータを Microsoft Excel スプレッドシートの正しい列に配置して、データアップロードを確実に成功させます。
2. Excel スプレッドシートをインポートします。	既存の オペレーショナルテクノロジー データを構成管理データベース (CMDB) にアップロードします。
3. オペレーショナルテクノロジー機能のディスカバリーを実行します。	産業用コントロールシステム (ICS) ネットワーク内の指定された Purdue レベルの オペレーショナルテクノロジー (OT) デバイスを検出します。
4. オペレーショナルテクノロジー (OT) メニューの選択を使用します。	企業内の OT デバイスの詳細情報を編集または表示できます。

自動翻訳

Microsoft Excel のサービスグラフコネクタ

Microsoft Excel のサービスグラフコネクタ関数を使用すると、入力済みの Excel フラットファイルスプレッドシートから既存のオペレーショナルテクノロジーデータをインポートMicrosoftできます。統合ハブ抽出変換ロード (ETL) でこれを使用して、このデータを構成管理データベース (CMDB) にアップロードします。

インポートプロセスを実行する前に、Microsoft Excel スプレッドシートに既存の オペレーショナルテクノロジー データを入力する必要があります。統合ハブ ETL を使用して Microsoft Excel スプレッドシートをインポートすると、構成管理データベース (CMDB) に正しい構成アイテム (CI) レコードが作成されます。詳細については、「[運用テクノロジー \(OT\) 拡張クラス](#)」を参照してください。

関連トピック

[統合ハブ](#)

[統合ハブ ETL](#)

Microsoft Excel のサービスグラフコネクタ の構成

入力された Excel フラットファイルスプレッドシートから既存のオペレーショナルテクノロジーデータをインポートするようにMicrosoft Excel のサービスグラフコネクタを構成します。

Microsoft Excel のサービスグラフコネクタ Excel のガイド付きセットアップを使用し、タスクを順番に実行して、次を構成します。Microsoft Excel のサービスグラフコネクタ

移動先 [すべて > 産業用ワークスペースアドミン > ガイド付きセットアップ](#)で、次のガイド付きセットアップを開き、タスクを完了します。

ガイド付きセットアップの使用の詳細については、「[ガイド付きセットアップ](#)」を参照してください。

インポート前の **OT** ワークシートエントリのアサイン ロールのレビュー

ユーザーまたはユーザーグループにロールをアサインして、Microsoft Excel のサービスグラフコネクタ ステージングテーブルと ETL を管理できるようにします。

始める前に

必要なロール：admin

このタスクについて

次のテーブルにリストされているロールを持つユーザーは、オペレーショナルテクノロジーマネージャー アプリケーションを使用できます。

ロール	説明
OT ステージングユーザー [ot_staging_user]	ステージングテーブルのレコードを作成、編集、および表示できます。
CMDB インステイテュートアドミン [cmdb_inst_admin]	ETL を表示および編集できます。
OT Excel インポートユーザー [ot_excel_import_user]	インポートタスクを作成、編集、および表示できます。これは、インポートタスクを介して Excel SGC インポートを実行するための最小ロールです。このロールにはot_staging_userが含まれています。
CMDB OT エディター [cmdb_ot_editor]	Excel SGC 修復タスクを表示および再アサインできます。修復タスクを実行するには、追加のot_staging_userロールが必要です。
CMDB OT アドミン [cmdb_ot_admin]	インポートタスクと修復タスクの両方を実行できます。このロールには、ot_excel_import_userとcmdb_ot_editorの両方が含まれます。

手順

ServiceNow AI Platform ユーザー管理機能を使用して、ユーザーとグループにロールをアサインします。

タスク	ユーザー管理機能
ユーザーへのロールのアサイン	ユーザーへのロールの割り当て を参照してください。
グループへのロールのアサイン	グループへのロールのアサイン を参照してください。

クラスマッピングの確認

Microsoft Excel のサービスグラフコネクタで利用可能なクラスマッピングを確認して更新します。

始める前に

- 利用可能なクラスマッピングテーブルを表示できるように、Industrial Core プラグインがインストールされていることを確認します。
- 必要なロール:admin または cmdb_ot_admin

このタスクについて

Microsoft Excel のサービスグラフコネクタ では、Excel SGC クラスマッピング [excel_sgc_class_mapping] テーブルで利用可能な構成を使用して、各構成アイテム (CI) を配置する最適な ServiceNow 構成管理データベース (CMDB) クラスを決定します。これらの設定はいつでも変更できますが、最初のインポートを実行する前に現在の構成を確認することをお勧めします。

手順

1. 移動先 すべて > **OT マネージャーアドミン** > **Excel SGC クラスマッピング**。
2. クラスマッピングレコードの次のフィールドを確認し、必要に応じて更新します。

分類設定フィールド

フィールド	説明
ソースクラス	ソース CI のクラス。
ターゲット CMDB クラス	CI に予期される ServiceNow クラス。
OT デバイスタイプ	OT デバイスが分類されるカテゴリタイプ。デバイスタイプは、デバイスが OT ネットワーク上で果たす機能でもあります。たとえば、次のようになります。 サーバーなどのIT機器はOT機器に変換でき、ネットワーク上で果たす機能はHMIです。したがって、そのクラスは server で、デバイスタイプは HMI です。 i 注: 場合によっては、OT 機能を持たない OT デバイスや、デバイスタイプが不明な OT デバイスがあります。OT 機能のない OT デバイスの場合は、[OT 機能なし] を選択します。デバイスタイプが不明な OT デバイスの場合は、[不明] を選択します。
OS 分類を許可	True に設定すると、CI でオペレーティングシステムが見つかった場合、ターゲットはターゲットの CMDB クラスからその OS に一致する ServiceNow クラスに切り替えられます。
アクティブ	オンにすると、クラスマッピングがアクティブに設定されます。

で使用するシステムプロパティを確認する **Microsoft Excel** のサービスグラフコネクタ

OT アドミンまたは CMDB 統合アドミンとして、Microsoft Excel のサービスグラフコネクタに関連するシステムプロパティを表示します。

始める前に

サービスグラフ コネクタで使用するすべてのシステムプロパティのフィルター済みリストを表示します。

必要なロール:cmdb_ot_admin または cmdb_inst_admin

手順

1. 移動先 **すべて > 産業用ワークスペースアドミン > OT マネージャーアドミン > OT デバイスのインポート：システムプロパティ**.
リストには、名前が **sn_otsm_sgc.excel** で始まるレコードが表示されます。
2. 次のシステムプロパティを確認します。

Microsoft Excel のサービスグラフコネクタ システムプロパティ

システムプロパティ	説明
sn_otsm_sgc.excel.fields.for.transformed.name	- このプロパティにより、ユーザーは変換された名前を構築するためのフィールドを提供できます。 - フィールド値または列名はカンマで区切る必要があります。 この変換された名前は、ステージングテーブルから直接の名前フィールドの代わりに、構成アイテム (CI) の名前として使用されます。デフォルトでは、名前フィールドの値自体が変換済みの名前の値として使用されます。 - このプロパティは sn_otsm_sgc スコープに属し、このプロパティ名に自動的に追加されます。 - 読み取りおよび書き込み操作には、admin、cmdb_ot_admin、および cmdb_inst_admin ロールが必要です。
sn_otsm_sgc.excel.transformed.name.delimiter	このプロパティは、システムプロパティ fields.for.transformed.name で指定された複数のフィールドまたは列の値を使用して変換済みの名前を計算するときに使用する区切り文字を指定します。

システムプロパティ	説明
	○ fields.for.transformed.name プロパティで列名が 1 つだけ指定されている場合、区切り記号は使用されません。 ○ このプロパティは sn_otsm_sgc スコープに属し、このプロパティ名に自動的に追加されます。 ○ 読み取りおよび書き込み操作には、admin、cmdb_ot_admin、および cmdb_inst_admin ロールが必要です。
sn_otsm_sgc.excel.fields.for.validation.state.change	○ このプロパティを使用すると、属性のカンマ区切りリストを提供して、検証ステータスを [検証処理待ち] に変更できます。デフォルト値は 空 です。 i 注: [MAC アドレス]、[シリアル番号]、[変換済みの名前]、[スロット番号] (OT コントロールモジュールの場合) などの識別子フィールドを変更すると、検証ステータスが [検証処理待ち] に変更されます。 ○ このプロパティは sn_otsm_sgc スコープに属し、このプロパティ名に自動的に追加されます。 ○ 読み取りおよび書き込み操作には、admin、cmdb_ot_admin、および cmdb_inst_admin ロールが必要です。
sn_otsm_sgc.enable.cmdb.validations	○ このプロパティは、ステージングデバイスの CMDB 検証を有効にします。 True に設定すると、ステージングデバイスは既存の CMDB CI と照らして検証され、調整が行われます。 ○ このプロパティは sn_otsm_sgc スコープに属し、このプロパティ名に自動的に追加されます。 ○ 読み取りおよび書き込み操作には、admin、cmdb_ot_admin、および cmdb_inst_admin ロールが必要です。

のステージングテーブルにカスタムフィールドマッピングを追加する **Microsoft Excel** のサービスグラフコネクタ

Microsoft Excel のサービスグラフコネクタを使用して、ステージングテーブルにカスタムフィールドを追加し、そのカスタムフィールドを構成アイテム (CI) フィールドにマッピングします。

始める前に

フォームレイアウトを構成するには、「[フォームレイアウトの構成](#)」を参照してください。

ステージングテーブルにカスタムフィールドを作成するには、「[テーブルのフィールドを追加およびカスタマイズする](#)」を参照してください。

必要なロール：

- admin - スクリプトインクルードを変更できます。クラスまたはフィールドマッピングを追加し、ETL を変更できます。
- cmdb_inst_admin - 新しいクラスまたはフィールドマッピングの追加と ETL の変更のみを行うことができます。

手順

1. ステージング [sg_ot_excel_staging] テーブルにカスタム列を追加します。
2. [すべて] に移動し、[フィルター] フィールドに sg_ot_excel_staging.list を追加します。
3. キーボードの Enter キーを押します。
4. 必要に応じて、[新規] を選択してレコードを手動で作成します。
5. 移動先 **すべて > 産業用ワークスペースアドミン > OT Manager (OT マネージャー) > OT デバイスのインポート：スクリプトインクルード** をクリックし、SGOTAssetImportExcelConstants スクリプトインクルードを選択します。
6. スクリプトで、ステージングテーブルの新しい列名を更新し、SGOTAssetImportExcelConstants.importSetColumnsVsStagingColumnsMap オブジェクト内の新しい ETL 列名を「<ETL 列名>」：「<ステージングテーブルの列名>」の形式で更新します。

この例では、コロン (:) の前の「u_my_custom_field」は ETL 列名 (ETL プレビューステップでは列として表示) を示し、コロンの後の「u_my_custom_field」はステージングテーブルの列名を示します。

新しい行の上の行の最後にカンマ (,) が追加されていることを確認します。この例では、"custom_fields": "custom_fields" 行の後にカンマが追加されています。

```

SGOTAssetImportExcelConstants.importSetColumnsVsStagingColumnsMap = {
    // unique id used to uniquely identify the asset
    "id": "correlation_id",
    // Name of the asset
    "name": "transformed_name",
    // OperatingSystem of the asset
    //"operating_system": "os_version",
    // type of the asset.
    "type": "type",
    // if the asset has control module
    "has_module": "has_module",
    // id of the asset to which a control module belongs to (this is used in control module type asset).
    "control_module_parent_correlation_id": "control_module_parent_correlation_id",
    "ot_display_name": "display_name",
    "serial_number": "serial_number",
    "firmware_version": "firmware_version",
    "os_version": "os_version",
    "operating_system": "os",
    "assigned_to": "assigned_to",
    "manufacturer": "manufacturer",
    "model_number": "model_number",
    "serial_number_type": "serial_number_type",
    "purdue_level": "purdue_level",
    "asset_criticality": "asset_criticality",
    "short_description": "short_description",
    "vendor": "vendor",
    "equipment_model_entity_path": "equipment_model_entity_path",
    "first_discovered": "first_discovered",
    "hardware_version": "hardware_version",
    "status": "status",
    "backplane_name": "backplane_name",
    "backplane_id": "backplane_id",
    "slot_number": "slot_number",
    "rack_number": "rack_number",
    "module_type": "module_type",
    "device_type": "io_field_device_type",
    "support_group": "support_group",
    "site": "site",
    "ip_address": {
        "ip": "ip_address_" + SGOTAssetImportExcelConstants.STAGING.NESTED_COLUMN_DELIMITER
    },
    "mac_address": {
        "mac": "mac_address_" + SGOTAssetImportExcelConstants.STAGING.NESTED_COLUMN_DELIMITER
    },
    "memory": {
        "memory_card_serial": "memory_card_serial_" + SGOTAssetImportExcelConstants.STAGING.NESTED_COLUMN_DELIMITER,
        "memory_size": "memory_size_" + SGOTAssetImportExcelConstants.STAGING.NESTED_COLUMN_DELIMITER,
        "memory_type": "memory_type_" + SGOTAssetImportExcelConstants.STAGING.NESTED_COLUMN_DELIMITER
    },
    "software_installed": {
        "name": "software_installed_" + SGOTAssetImportExcelConstants.STAGING.NESTED_COLUMN_DELIMITER,
        "version": "software_version_" + SGOTAssetImportExcelConstants.STAGING.NESTED_COLUMN_DELIMITER,
        "install_date": "software_install_date_" + SGOTAssetImportExcelConstants.STAGING.NESTED_COLUMN_DELIMITER
    },
    // Do not change this. Key should match value of SGOTAssetImportExcelConstants.CUSTOM_FIELDS_COL_NAME_IN_IMPORT_SET
    "custom_fields": {
        "customfield": "customfield_" + SGOTAssetImportExcelConstants.STAGING.NESTED_COLUMN_DELIMITER
    }
}

```

7. [更新] を選択して、変更を保存します。
8. 移動先 すべて > 構成 > 統合ハブ **ETL**.
9. **CMDB** アプリケーション:SG-OT **Excel** インポート ETL を選択します。
10. [無効なマッピングデータが検出されました] ページが表示された場合は、[閉じる] を選択します。

11. ETL 変換マップアシスタントのガイド付きセットアップの [基本的な詳細を指定] セクションで、[ソースデータをインポートして基本的な詳細を入力] を選択します。

SG-OT Asset Excel Import

ETL Transform Map Assistant

Use this guided walkthrough to create and manage ETL Transform Map for integrating third-party data into CMDB.

1/1
Tasks

1. Specify Basic Details
Provide basic information for the ETL Transform Map.

✓ Import Source Data and Provide Basic Details

12. [サンプルインポートセット] フィールドで、[新しいインポートセットを自動プル] を選択します。

Specify Basic Details

← Provide Basic Information for the ETL Transform Map

Unsaved Changes

Save Mark as Complete

Provide the template with some basic properties, and select a data source to map to CMDB.

* CMDB Application ① SG-OT Excel Import

* Name ① SG-OT Asset Excel Import

Description ETL to import assets from Excel

* Data Source ① SG-OT Excel Import

Sample Import Set ① Auto-pull a new import set

13. [Save (保存)] を選択します。
[基本情報が正常に保存されました] バナーが表示されます。
14. [Mark as Complete (完了としてマーク)] を選択します。
15. [ETL 変換マップアシスタント] ページの [マッピング用のソースデータの準備] セクションで、[データのプレビューと準備] を選択します。

now All Favorites History Workspaces

IntegrationHub ETL

Search

Prepare Source Data for Mapping

Preview and Prepare Data

Mark as Complete

Nested Data Structure

Tree Collection

object

object(1)

The table below displays raw source data. Click a column's action menu (≡) for specific data transformation options. You can also set columns to be ignored in mapping.

object	status_value	support_group	support_group_sys_id	type	u_my_custom_field	vendor	vendor_cleansed	vendor_name_cleansed
	get initial status value	Original Value	get support group sys id	Original Value	Original Value	Original Value	cleanse vendor	split - vendor_cleansed
1				plc	My Custom value	Vendor E	48364f745328110594addecff7b127hj	Vendor E Vendor E

列が表示されない場合は、手順 11 ~ 14 を繰り返します。

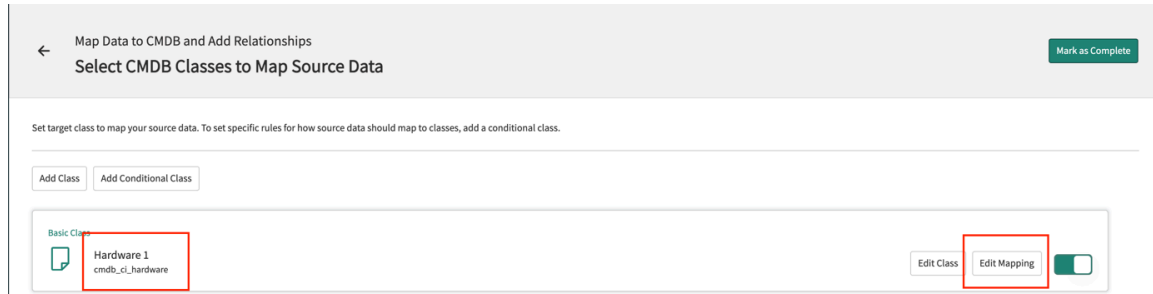
16. [Mark as Complete (完了としてマーク)] を選択します。
17. [ETL 変換マップアシスタント] ページの [データを CMDB にマップし、関係性を追加] セクションで、[ソースデータをマップする **CMDB** クラス] を選択します。
18. 列をターゲットクラスと属性にマッピングします。

たとえば、[コメント] フィールドはハードウェア [cmdb_ci_hardware] クラスにあります。フィールドがマッピングされた後、その行のステージングテーブルの [コメント] 列の値が空でない場合は、ハードウェア子クラスの [コメント] フィールドが更新されます。

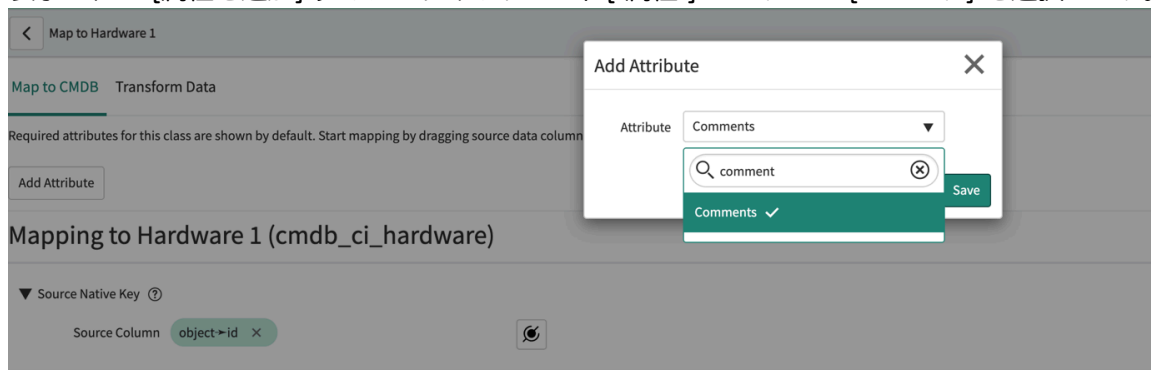
存在しない新しいフィールド、またはハードウェア *cmdb_ci_hardware* クラスに固有ではなく、オペレーショナルテクノロジー (*cmdb_ci_ot*) クラスのフィールドであるフィールドのマッ

ピングを追加する場合は、オペレーショナルテクノロジー (OT) 1 スタブにフィールドマッピングを追加できます。

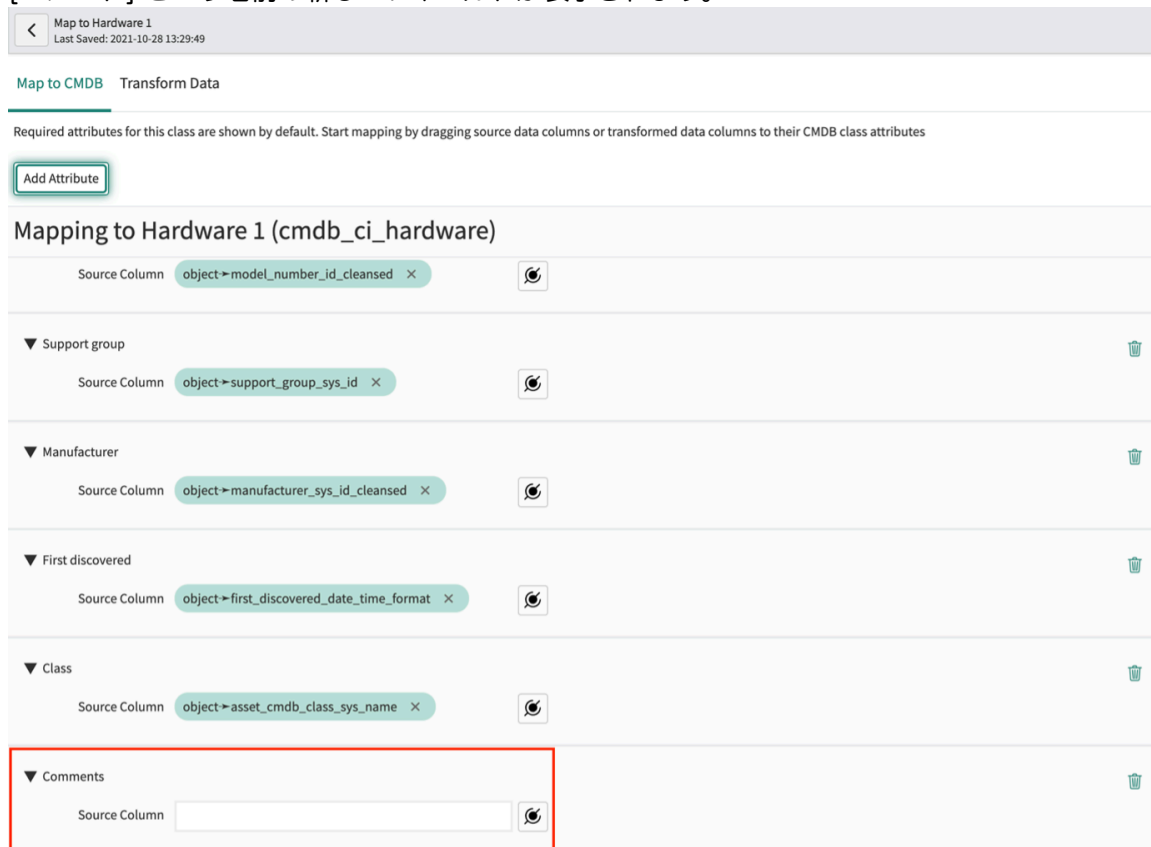
- a. ハードウェア 1 クラスにフィールドマッピングを追加します。
- b. ハードウェア 1 クラスの場合は、[マッピングの編集] を選択します。



19. 表示される [属性を追加] ダイアログボックスで、[属性] リストから [コメント] を選択します。



20. [Save (保存)] を選択します。
[コメント] という名前の新しいフィールドが表示されます。



21. [データ] ペインから、データピルを [コメント ソース列] フィールドにドラッグします。

The screenshot shows the 'Map to CMDB' interface in ServiceNow. The 'Data' pane on the right displays a list of data pills. The 'Comments' section in the 'Mapping to Hardware 1 (cmdb_ci_hardware)' pane is highlighted with a red box, showing the 'object=u.my_custom_field' source column. The 'Data' pane shows various data pills including 'serial_number_cleansed', 'serial_number_snk', 'serial_number_type', 'serial_number_type_cleansed', 'serial_number_valid', 'sgc_import_date_time_format', 'short_description', 'site', 'site_sys_id_computed', 'slot_number', 'status', 'status_value', 'support_group', 'support_group_sys_id', 'type', 'u.my_custom_field', and 'vendor'.

[ソース列] アイコン () を選択して、そのデータマッピングフィールドを選択することもできます。

[ソース列] にはデータピルが含まれます。

This screenshot is a zoomed-in view of the 'Comments' section from the previous image. It shows the 'Source Column' field with the value 'object=u.my_custom_field' and a red box highlighting the entire row. The 'Data' pane on the right is also visible, showing the 'u.my_custom_field' data pill.

22. [ETL 変換マップアシスタント] ページの [CMDB にデータをマッピングし、関係性を追加] セクションの [CMDB クラスにソースデータをマッピング する] に戻ります。

23. [Mark as Complete (完了としてマーク)] を選択します。

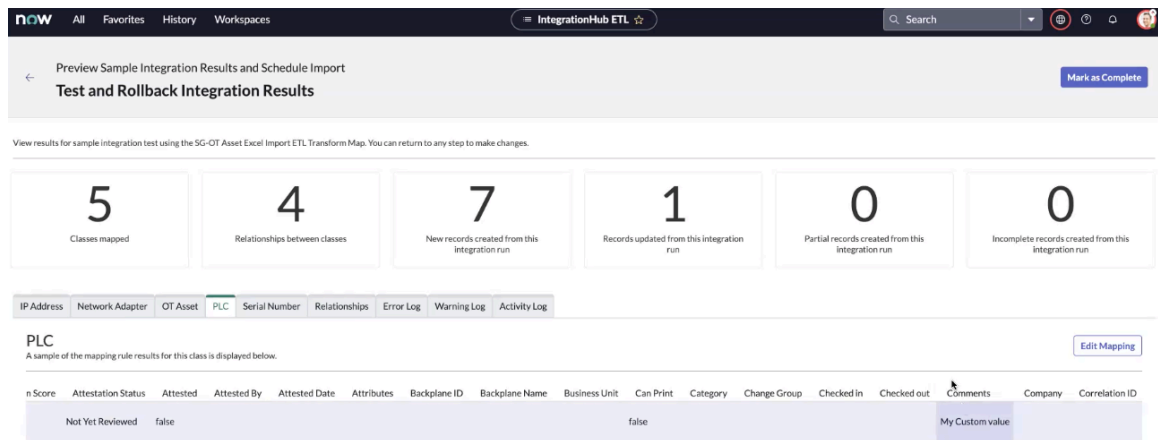
24. 次の手順に従って、新しいフィールドマッピングを確認します。

- a. ETL 変換マップアシスタントのホームページに移動します。
- b. ガイド付きセットアップの [サンプル統合結果のプレビューとインポートのスケジュール] セクションで、[テストとロールバックの統合結果] を選択します。

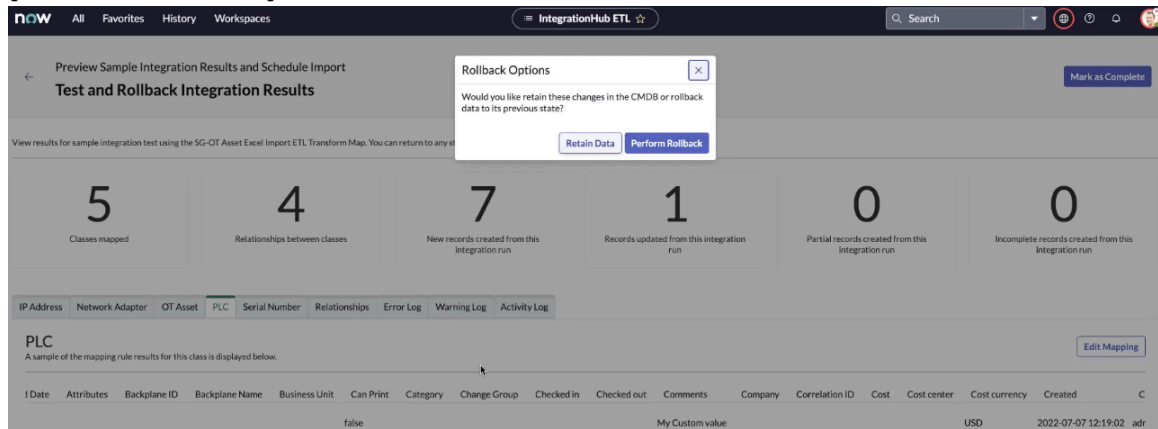
c. [統合を実行] を選択します。

d. 実行が正常に完了したら、コメント値を指定した CI の [コメント] フィールドがステージングテーブルで更新されていることを確認します。

e. [Mark as Complete (完了としてマーク)] を選択します。



f. [ロールバックの実行] を選択します。



g. ETL がアクティブ化されていない場合は、[アクティブ化] を選択します。
新しい列フィールドマッピングが正常に追加され、検証されました。

デバイス分類のカスタム実装を追加する

タイプ、os_version、およびfirmware_versionに基づいて、デバイスのベースシステム分類をカスタマイズします。

始める前に

sn_otsm_sgc.SGOTAssetImportExtensionPoint拡張ポイントのベースシステムは、sn_otsm_sgc.SGOTAssetImportUtil という名前で出荷されるデフォルトの実装スクリプトを使用します。カスタマイズされた分類を追加するには、 サービスグラフコネクタ **for Operational Technology (Excel)** スコープで拡張ポイントの実装を作成します。

i 注: ユーザーは、拡張ポイントの実装を 1 つのみ持っている必要があります。デフォルトの拡張ポイントではなくカスタム拡張ポイントを実装してアクティブ化する場合は、デフォルトの実装を非アクティブ化する必要があります。

必要なロール: admin

手順

1. 移動先 **すべて > システム拡張ポイント > スクリプト化された拡張ポイント**.
2. [sn_otsm_sgc.SGOTAssetImportExtensionPoint] を選択します。
3. [実装を作成] 関連リンクを選択します。
4. 拡張ポイント実装の名前を入力します。

5. スクリプトフィールドで、次の 2 つの関数を持つクラスオブジェクトが入力されていることを確認します。

から結果が返されたことを確認してください

getAssetCMDBSysClassNameWithOtEntityTypeSysId 拡張ポイントは、コメントに記載されている形式に従います。結果の文字列形式を変更すると、インポートの失敗や不規則性が発生します。形式は <cmdb class name>:::<ot entity type sys id> である必要があります。

オプション	説明
getAssetCMDBSysClassNameWithOtEntityTypeSysId(/ *string*/ type, /*string*/ osVersion, /*string*/ firmwareVersion)	このメソッドを実装して、デバイスが属する CMDB システムクラス名と、「:::」で連結された OT エンティティタイプsys_idを返します。 未分類のデバイスの場合、OT デバイスタ입は ot_base に設定されます。
getComputerType(//*string*/ operatingSystem)	渡されたオペレーティングシステムに基づいて CMDB システムクラス名を返します。

6. 必要な変更をすべて行ったら、[更新] を選択します。
拡張ポイントの実装が作成されます。

次のタスク

関連リストの [実装] タブで、ベースシステムの拡張ポイントの実装を開いて非アクティブ化します。

デバイスのカスタム検証を追加する

OT デバイスの検証をカスタマイズします。

始める前に

sn_otsm_sgcのベースシステム。SGOTAssetCustomValidationExtensionPoint 拡張ポイントは、デフォルトのsn_otsm_sgcを使用します。SGOTExcelStagingAssetValidationProcessor 実装スクリプト。サービスグラフコネクタ for Operational Technology (Excel) スコープで拡張ポイントの実装を作成することで、カスタマイズされた検証を追加できます。

必要なロール：admin

手順

1. 移動先 **すべて > システム拡張ポイント > スクリプト化拡張ポイント**。
2. **[sn_otsm_sgc]** を選択します。SGOTAssetCustomValidationExtensionPoint。
3. **[実装を作成]** 関連リンクを選択します。
カスタム検証を追加できるスクリプトインクルードが作成されます。

4. カスタム検証を追加するには、次の検証シナリオを参照してください

	A	B	C	D	E	F	G	H	I	J
	Custom Validation									
1	Default Validation Partially Valid	Invalid (Override - False)	Valid (Override - False)	Partially Valid (Override - False)	Invalid (Override - True)	Valid (Override - True)	Partially Valid (Override - True)	No Implementation created (Override - True)	Implementation has different Name (Override - True)	Invalid state (Type) (Override - True)
2	(en_otam_sgc.enable.cmdb.validations - True) Valid	Partially valid	Partially valid	Partially Valid	Invalid	Valid	Partially Valid	Partially Valid	Same as Custom validation state	Same as Default state
3	(en_otam_sgc.enable.cmdb.validations - True) Invalid	Valid	Valid	Valid	Invalid	Valid	Partially valid	Valid	Same as Custom validation state	Same as Default state
4	(en_otam_sgc.enable.cmdb.validations - True) Partially Valid	invalid	invalid	invalid	Invalid	Invalid	invalid	Invalid	Invalid	Same as Default state
5	(en_otam_sgc.enable.cmdb.validations - False) Valid	Partially valid	Partially valid	Partially Valid	Invalid	Valid	Partially Valid	Partially Valid	Same as Custom validation state	Same as Default state
6	(en_otam_sgc.enable.cmdb.validations - False) Invalid	Valid	Valid	Valid	Invalid	Valid	Partially valid	Valid	Same as Custom validation state	Same as Default state
7	(en_otam_sgc.enable.cmdb.validations - False) Partially Valid	invalid	invalid	invalid	invalid	Invalid	invalid	Invalid	Invalid	Same as Default state

い。

5. [Update (更新)] を選択します。

テスト Microsoft Excel のサービスグラフコネクタ

トラブルシューティングのアクションは、オペレーショナルテクノロジー デバイスまたはデータをインポートする際の一般的な問題の解決に役立ちます。システムログにアクセスして、これらのエラーのトラブルシューティングを行います。

これらのログを使用して、問題をデバッグしたり、サービスグラフコネクタ ステップが適切に実行されているかを確認したりできます。

問題	ソリューション
ETL からの サービスグラフコネクタ のテスト実行後に [部分的ペイロード] タブにエントリがある場合 ガイド付きセットアップ	次の条件が原因です。 - デバイスの必須フィールドの値がありません。 - 親デバイスが関連付けられていないコントロールモジュール - デバイスとコントロールモジュールの親 ID フィールドのタイプがステージングテーブルに正しく入力されていることを確認します。
ETL からの サービスグラフコネクタ のテスト実行後に [不完全なペイロード] タブにエントリがある場合 ガイド付きセットアップ	デバイスを識別するために一意に使用されるフィールドの値が欠落しているためです。
ステージングテーブルのタイムスタンプ列が空で表示される場合	ユーザーは UTC 形式 (YYYY-MM-DD hh:mm:ss) を使用して日付と時刻を入力する必要があります。
検証プロセス後にレコードの検証ステータスの更新が表示されない場合	ユーザーは手動でページを更新する必要があります。
ユーザーがステージングテーブルのレコードの既存のデータを変更した場合、検証ステータスは [検証処理待ち] に設定されません。	次の属性が変更されると、検証ステータスは [検証処理待ち] に設定されます。 - 識別子フィールド (MAC アドレス (1-9)) - シリアル番号 - 名前 - 相関 ID - タイプ - コントロールモジュールの親相関 ID - 変換済みの名前の計算で使用されるフィールド

問題	ソリューション
	• ラック番号 • スロット番号 システムプロパティの詳細については、「で使用されるシステムプロパティを確認する Microsoft Excel のサービスグラフコネクタ」を参照してください。
レコードがステージングテーブルにインポートされた後、変換された名前の計算に関連するシステムプロパティで行われた更新は、ステージングテーブルレコードに反映されません。	ステージングテーブルにデータをインポートする前に、システムプロパティを変更します。
重複レコードが CMDB に存在する場合、ステージングテーブルはそれを重複として検出しません。	検証は、ステージングテーブルで利用可能なデータに対してのみ実行されます。 CMDBで使用可能なデータの検証は実行されません。
サイト名はスプレッドシートまたはステージングテーブルで提供されますが、スプレッドシートのインポート後に OT デバイスには表示されません。	CMDB内の既存のサイトレコードのみが考慮されます。 サイト (ISA 設備階層モデルエンティティ) の entity_nameは、Excel またはステージングテーブルのサイト列に指定された値と一致する必要があります。 サイトのentity_nameが一致しない場合、値は空に設定されます。

が使用するスクリプトインクルードを表示 **Microsoft Excel** のサービスグラフコネクタ

アドミニストレーターとして、関連するスクリプトインクルードを表示します。 Microsoft Excel のサービスグラフコネクタ

始める前に

Microsoft Excel のサービスグラフコネクタで使用されるすべてのスクリプトのフィルター済みリストを表示します。

必要なロール：admin

手順

1. 移動先 **すべて > 産業用ワークスペースアドミン > OT Manager (OT マネージャー) > OT デバイスのインポート：スクリプトインクルード**.
このリストには、名前が SGOTAsset または SGOTExcelStaging で始まるレコードが表示されます。
2. スクリプトのリストを表示します。

インポートタスクによる **Microsoft Excel** のサービスグラフコネクタ の使用

Microsoft Excel のサービスグラフコネクタを使用すると、OT デバイスデータのステージングレコードの 構成管理データベース (CMDB) へのアップロード、検証、およびインポートを処理するインポートタスクを作成できます。

インポートタスクの概要

OT Excel インポートユーザー [ot_excel_import_user] ロールを割り当てられたユーザーは、産業用ワークスペースでインポートタスクを作成できます。インポートタスクは、次のタスクを処理します。

- 入力した Microsoft Excel スプレッドシートをステージングテーブルにアップロードします。
- Microsoft Excelスプレッドシートから作成されたステージングレコードを検証します。
- 有効なステージングレコードを CMDBにインポートします。
- 必要に応じて、無効なステージングレコードの修復タスクを作成します。

インポートタスクの作成

Microsoft Excel のサービスグラフコネクタのインポートタスクを作成して、Microsoft Excelスプレッドシートからのオペレーショナルテクノロジー (OT) デバイスデータのインポートを処理します。

始める前に

必要なロール:ot_excel_import_user

手順

1. 移動先 **すべて > 産業用ワークスペース**.
2. リスト (☰) アイコンを選択します。
3. [OT Excel SGC:インポートタスク] モジュールで、使用可能なリストのいずれかを選択します。
4. **[New (新規)]** を選択します。
5. フォームのフィールドに入力します。
6. **[Save (保存)]** を選択します。
7. [添付ファイル] パネルから Microsoft Excel テンプレートをダウンロードし、コンピューターにローカルに保存します。
8. 必要に応じて、テンプレートに OT デバイスデータを入力します。
スプレッドシートの入力方法の詳細については、「[サービスグラフコネクタインポート用のインポート前 OT ワークシートエントリレビューツールの準備](#)」を参照してください。
9. 完了した Microsoft Excel スプレッドシートをアップロードします。
 - a. [添付ファイル] パネルで、[+] ボタンをクリックします。
 - b. ローカルドライブから、完了した Microsoft Excel スプレッドシートをアップロードします。
 - c. [添付ファイルをインポート] UI アクションが表示されるように、インポートタスクにアサインされていることを確認してください。
インポートタスクの [アサイン先] フィールドを表示していない場合は、次の手順に進む前に、[自分にアサイン] UI アクションをクリックします。
 - d. [添付ファイルをインポート] UI アクションをクリックします。
 - e. システムがインポートプロセスを完了するまで待ちます。
完了すると、[ステータス] フィールドが [保留中のステージングインポート] から [ステージングインポートに成功しました] に変わります。

結果

インポートプロセスが完了し、Microsoft Excelスプレッドシートが正常にインポートされたら、[ステージングレコード] タブを選択して、オペレーショナルテクノロジー (OT) デバイスデータのステージングレコードを表示できます。

次のタスク

インポートプロセスが完了したら、インポートされたステージングレコードを検証できます。詳細については、「[インポートされたステージングレコードの検証](#)」を参照してください。

サービスグラフコネクタインポート用のインポート前 **OT** ワークシートエントリレビューツールの準備

アップロードを成功させるには、既存のデータを正しい列に配置してスプレッドシートを準備することが重要です。

始める前に

必要なロール:ot_excel_import_user

このタスクについて

手順

1. Microsoft Excel スプレッドシートの次の列に入力します。

- i** 注: 列名は変更できません。追加の列をステージングテーブルに追加できます。ステージングテーブルに新しいカスタムフィールドマッピングを追加する方法の詳細については、「[のステージングテーブルにカスタムフィールドマッピングを追加する Microsoft Excel のサービスグラフコネクタ](#)」を参照してください。

スプレッドシートに入力する際のガイダンスについては、次の表を参照してください。スプレッドシートには多くの列が含まれています。例とフィールドの説明は複数のセクションに分かれています。

- 列 A から K への入力
- 列 L から Y への入力
- AI による列 Z の入力
- 列 AJ から AT への入力
- 列 AU から BD への入力
- 列 BE から BR への入力
- BS から BW の列への入力
- 1 列目から 8 列目の入力

列 A から K

列	必須の列名	タイプ	説明と例
A	デバイスの重要度	文字列	OT デバイスの重要度をそのロールに基づいて測定します。例： ○ 高または最重要 ○ 中程度またはやや重大 ○ 「低」または「やや重要」 ○ なしまたは重大ではない

列	必須の列名	タイプ	説明と例
B	アサイン先	文字列	この OT デバイスがアサインされているユーザーのメールアドレス。 例:bob@example.com
C	バックプレーン ID	文字列	バックプレーンの識別と制御モジュールへのマッピングに使用される一意の ID。例:BPSN123
D	バックプレーン名	文字列	OT デバイスのバックプレーンの名前 (ある場合)。例:バックプレーン #51、PLC1バックプレーン
E	コントロールモジュールの親 ID	文字列	親コントロールシステムのバックプレーンに対するコントロールモジュールの識別に使用される一意の ID。例:482bb239-05e8-4bad-ba59-925eb87ff06e
F	関連 ID	文字列	OT デバイスの識別に使用される一意の ID。文字列correlation_idを入力します。例:482bb239-05e8-4bad-ba59-925eb87ff06e または 5123456。 この列エントリは必須です。 - インポートされた各 OT デバイスには、一意のcorrelation_idが必要です。 - インポートする OT デバイスデータは通常、外部ソースシステムで発生し、通常は各レコードに一意の識別子が割り当てられます。
G	カスタムフィールド 1	文字列	(オプション)OT デバイスのカスタムデータは、CI の [属性] フィールドに保存されます。この列を使用して、分類やその他の目的でフリーフォームデータを OT デバイスに関連付けることができます。例:再生品、中古品
H	カスタムフィールド 2	文字列	(オプション)OT デバイスのカスタムデータは、CI の [属性] フィールドに保存されます。この列を使用して、分類やその他の目的でフリーフォームデータを OT デバイスに関連付けることができます。例:塗装、スタンプング
I	カスタムフィールド 3	文字列	(オプション)OT デバイスのカスタムデータは、CI の [属性] フィールドに保存されます。この列を使用して、分類やその他の目的でフリーフォームデータを OT デバイスに関連付けることができます。
J	カスタムフィールド 4	文字列	(オプション)OT デバイスのカスタムデータは、CI の [属性] フィールドに保存されます。この列を使用して、分類やその他の目的でフリーフォームデータを OT デバイスに関連付けることができます。
K	カスタムフィールド 5	文字列	(オプション)OT デバイスのカスタムデータは、CI の [属性] フィールドに保存されます。この列を使用して、分類やその他の目的でフリーフォームデータを OT デバイスに関連付けることができます。

列 L から Y

列	必須の列名	タイプ	説明と例
L	表示名	文字列	OT デバイスの表示名を入力するために使用されます。
M	機器モデルエンティティパス	文字列	OT デバイスがマッピングされている

列	必須の列名	タイプ	説明と例
			機器モデルエンティティのパス。
N	ファームウェアバージョン	文字列	OT デバイスのファームウェアバージョン (ある場合)。例:12.0
O	最初の検出	日時	OT デバイスがネットワーク上で最初に検出されたときの ISO 形式のタイムスタンプ。例:YYYY-MM-DD HH:MM:SS。
P	ハードウェアバージョン	文字列	OT デバイスのハードウェアバージョン (ある場合)。例:13.2
Q	モジュールあり	ブール	モジュール付き制御システムの場合、このシステムにモジュールがあることを示します。例:True、False
R	IO フィールドデバイスタイプ	文字列	このデバイスがフィールドデバイスの場合、入力、出力、またはその両方に使用されるかどうかを示します。例： - 入力 - 出力 - input_output このデバイスは、入力と出力の両方として機能します。
土	IP アドレス 1	文字列	OT デバイスに関連付けられている最初の IP アドレス (存在する場合)。複数の IP アドレスがある場合は、次の IP アドレス列 (IP アドレス 2) を使用します。例:10.0.0.22、10.0.0.12
木	IP アドレス 2	文字列	OT デバイスに関連付けられている 2 つ目の IP アドレス (存在する場合)。例:192.168.100.1、192.168.100.5

列	必須の列名	タイプ	説明と例
U	IP アドレス 3	文字列	OT デバイスに関連付けられている 3 番目の IP アドレス (存在する場合)。
V	IP アドレス 4	文字列	OT デバイスに関連付けられている 4 番目の IP アドレス (存在する場合)。
W	IP アドレス 5	文字列	OT デバイスに関連付けられている 5 番目の IP アドレス (存在する場合)。
X	IP アドレス 6	文字列	OT デバイスに関連付けられている 6 番目の IP アドレス (存在する場合)。
Y	IP アドレス 7	文字列	OT デバイスに関連付けられている 7 番目の IP アドレス (存在する場合)。

列 Z から AI

列	必須の列名	タイプ	説明と例
Z	IP アドレス 8	文字列	OT デバイスに関連付けられている 8 番目の IP アドレス (存在する場合)。
AA	IP アドレス 9	文字列	OT デバイスに関連付けられている 9 番目の IP アドレス (存在する場合)。
血液型	MAC アドレス 1	文字列	OT デバイスに関連付けられている最初の MAC アドレス (存在する場合)。複数の MAC アドレスがある場合は、次の MAC アドレス列(MAC アドレス 2)を使用します。 例:94:94:1d:01:6d:5f、cc:7c:4a:fb:2

列	必須の列名	タイプ	説明と例
			i 注: OT デバイスの場合、次の 3 つのスプレッドシート列のうち少なくとも 1 つにエントリを作成する必要があります。これらの列の値はすべてスプレッドシートに対して一意である必要があります。 - MAC アドレス 1 - 名前 - シリアル番号
AC	MAC アドレス 2	文字列	OT デバイスに関連付けられている 2 番目の MAC アドレス (存在する場合)。例:e5:4d:c8:36:b1:2d
AD	MAC アドレス 3	文字列	OT デバイスに関連付けられている 3 番目の MAC アドレス (存在する場合)。
AE	MAC アドレス 4	文字列	OT デバイスに関連付けられている 4 番目の MAC アドレス (存在する場合)。
AF	MAC アドレス 5	文字列	OT デバイスに関連付けられている 5 番目の MAC アドレス (存在する場合)。
AG	MAC アドレス 6	文字列	OT デバイスに関連付けられている 6 番目の MAC アドレス (存在する場合)。
AH	MAC アドレス 7	文字列	OT デバイスに関連付けられている 7 番目の MAC アドレス (存在する場合)。
AI	MAC アドレス 8	文字列	OT デバイスに関連付けられている 8 番目の MAC アドレス (存在する場合)。

列 AJ から AT

列	必須の列名	タイプ	説明と例
AJ	MAC アドレス 9	文字列	OT デバイスに関連付けられている 9 番目の MAC アドレス (存在する場合)。
AK	メーカー	文字列	OT デバイスのメーカーの名前。例:ロックウェル・オートメーション、デル
アル	メモリーカードのシリアル 1	文字列	OT デバイスにインストールされている最初のメモリーカード (存在する場合) のアサインされたシリアル番号。メモリーカードが複数ある場合は、次のメモリーカードのシリアル列(メモリーカードのシリアル2)を使用します。例:MMC DA362131、MemSN123
AM	メモリーカードのシリアル 2	文字列	OT デバイスにインストールされている 2 枚目のメモリーカード (存在する場合) のアサイン済みシリアル番号。例:MemSN123
ひとつの	メモリーカードのシリアル 3	文字列	OT デバイスにインストールされている 3 枚目のメモリーカード (存在する場合) のアサイン済みシリアル番号。
AO	メモリーサイズ 1	文字列	OT デバイスに取り付けられる最初のメモリーカードのサイズ (ある場合)。例:256 GB または 1 GB
AP	メモリーサイズ 2	文字列	OT デバイスにインストールされている 2 枚目のメモリーカードのサイズ (ある場合)。例:256 GB または 1 GB
AQ	メモリーサイズ 3	文字列	OT デバイスにインストールされている 3 枚目のメモリーカードのサイズ (ある場合)。例:256 GB または 1 GB
アール	メモリータイプ 1	文字列	OT デバイスにインストールされているメモリーカードのタイプ。メモリーカードが複数ある場合は、複数の列を使用します。例:RAM
として	メモリータイプ 2	文字列	OT デバイスにインストールされているメモリーカードのタイプ。例:RAM
で	メモリータイプ 3	文字列	OT デバイスにインストールされているメモリーカードのタイプ。

列 AU から BD

列	必須の列名	タイプ	説明と例
AU	モデル番号	文字列	OT デバイスのメーカーのモデル番号。例:ThinkServer TD230、XPS 15z
AV	モジュールタイプ	文字列	このデバイスが 1 つの場合、コントロールモジュールの機能の説明。例:入力、出力
AW	名前	文字列	OT デバイスのホスト名 (通常は FQDN の一部)。例:PLC1、ドアアセンブリ HMI、ロボット制御モジュール。 i 注: OT デバイスの場合、これら 3 つのスプレッドシート列のうち少なくとも 1 つにエントリを作成する必要があります。これらの列の値はすべて、スプレッドシートで一意である必要があります。 - MAC アドレス 1 - 名前 - シリアル番号
斧	オペレーティングシステム	文字列	OT デバイスにインストールされているオペレーティングシステム (存在する場合)。例:Linux Fedora、Windows 10、Windows 2000、Mac OS 8。 i 注: OT デバイスの場合は、必須ではありませんが、次のスプレッドシート列にエントリを作成する必要があります。 - タイプ - 利用可能な場合、オペレーティングシステム - 利用可能な場合、ファームウェアバージョン
はい	OS バージョン	文字列	OT デバイスにインストールされているオペレーティングシステムの報告されたバージョン (存在する場合)。例:10.0、13.5.2 i 注: OT デバイスの場合は、必須ではありませんが、次のスプレッドシート列にエントリを作成する必要があります。 - タイプ - 利用可能な場合は、os_version - 利用可能な場合、ファームウェアバージョン
アリゾナ州	OT ステージングタスク	文字列	ステージングテーブルの無効なレコードを修正するために作成されたタスク。
文学士	Purdue レベル	文字列	OT デバイスにアサインされた Purdue レベル。Purdue レベルを割り当てると、オペレーショナルテクノロジー機能のディスカバリーで各アイテムが正

列	必須の列名	タイプ	説明と例
			しい ICS レベルで適切に検索され、正確なディスカバリー結果が生成されます。例:1、2、3
BB	ラック番号	文字列	コントロールモジュールが取り付けられているラック。例:1、2、3
紀元前	シリアル番号	文字列	OT デバイスにアサインされたシリアル番号 (存在する場合)。 例:SN545、SN998  注: OT デバイスの場合、これら 3 つのスプレッドシート列のうち少なくとも 1 つにエントリを作成する必要があります。これらの列の値はすべて、スプレッドシートで一意である必要があります。 - MAC アドレス 1 - 名前 - シリアル番号
BD	シリアル番号タイプ	文字列	通常は「system」の値に設定されますが、別のタイプのシリアル番号の場合もあります。例:uuid

列 **BE** から **BR**

列	必須の列名	タイプ	説明と例
BE	簡単な説明	文字列	OT デバイスの簡単な説明。例:ドア塗装セルのHMI、ドア組立ロボットを制御します。
BF	サイト	文字列	設備モデルはサイトレベルから始まり、各工業用地を記述する詳細な階層構造が含まれています。 詳細については、「 ISA-95 機器モデル 」を参照してください。
BG	スロット番号	文字列	コントロールモジュールの場合、このデバイスが制御システムのシャーシ内で占有するスロットを示します。例:1、2
BH	ソフトウェアのインストール日 1	日時	アプリケーションソフトウェアが OT デバイスにインストールされた日付。複数の日付がある場合は、複数の列を使用します。 日付には UTC 形式のみを使用してください。 例:YYYY-MM-DD HH:MM:SS
BI	ソフトウェアのインストール日 2	日時	アプリケーションソフトウェアが OT デバイスにインストールされた日付。複数の日付がある場合は、複数の列を使用します。 日付には UTC 形式のみを使用してください。例:YYYY-MM-DD HH:MM:SS

列	必須の列名	タイプ	説明と例
BJ の	ソフトウェア のインストール 日 3	日時	アプリケーションソフトウェアが OT デバイスにインストールされた 日付。複数の日付がある場合は、複数の列を使用します。 日付には UTC 形式のみを使用してください。例:YYYY-MM-DD HH:MM:SS。
BK	インストール されているソ フトウェア 1	文 字 列	OT デバイスにインストールされているアプリケーションソフトウェ アの名前 (存在する場合)。複数の名前がある場合は、複数の列を使用 します。例:ロックウェルHMIビジョン
BL	インストール されているソ フトウェア 2	文 字 列	OT デバイスにインストールされているアプリケーションソフトウェ アの名前 (存在する場合)。
BM	インストール されているソ フトウェア 3	文 字 列	OT デバイスにインストールされているアプリケーションソフトウェ アの名前 (存在する場合)。
BN	ソフトウェア バージョン 1	文 字 列	OT デバイスにインストールされているアプリケーションソフトウェ アの報告されたバージョン (存在する場合)。複数のバージョンがある 場合は、複数の列を使用します。 例:v1.2 または v2011 SP3 HF2 または 4.54.32145
ボー	ソフトウェア バージョン 2	文 字 列	OT デバイスにインストールされているアプリケーションソフトウェ アの報告されたバージョン (存在する場合)。 例:v1.2 または v2011 SP3 HF2 または 4.54.32145
BP	ソフトウェア バージョン 3	文 字 列	OT デバイスにインストールされているアプリケーションソフトウェ アの報告されたバージョン (存在する場合)。 例:v1.2 または v2011 SP3 HF2 または 4.54.32145
BQ	ステータス	文 字 列	OT デバイスのステータス: -- なし -- アサインされたステータスはありません。 不在 施設に OT デバイスが存在しません。 メンテナンス中 OT デバイスはメンテナンス中であり、現在オフライン です。 在庫あり OT デバイスは施設に在庫があります。 インストール済み OT デバイスが施設に設置されている。 インストール待ち OT デバイスは施設へのインストールを保留中です。 修理待ち

列	必須の列名	タイプ	説明と例
			OT デバイスは修理を保留中ですが、まだオンラインではありません。 廃止 OT デバイスが廃止されました。 盗難 OT デバイスが盗まれました。 i 注: このフィールドの値は、CI フォームの [ライフサイクルステージ] フィールドと [ライフサイクルステータス] フィールドにマッピングされます。
BR	サポートグループ	文字列	この OT デバイスのプライマリサポートグループの名前。例:ドアサポート、企業 IT サポート。

列 **BS** から **BW**

列	必須の列名	タイプ	説明と例
理学士	変換済みの名前	文字列	ユーザーはこの列に入力しないでください。 デフォルトでは、変換済みの名前の値は、変換済み列のシステムプロパティを使用して入力されます。 ユーザーは変換済みの名前を編集できません。 システムのプロパティについては、「で使 用されるシステムプロ パティを確認する Microsoft Excel の サービスグラフコネク タ」を参照してください。
BT	タイプ	文字列	OT デバイス/構成アイテム (CI) のタイプ。 例:PLC、DCS

列	必須の列名	タイプ	説明と例
			i 注: - 有効な CI タイプのリストと説明については、「運用テクノロジー (OT) 拡張クラス」を参照してください。 - OT デバイスの場合は、必須ではありませんが、次のスプレッドシート列にエントリを作成する必要があります。 - タイプ - os_version
BU	検証コメント	文字列	ユーザーはこの列に入力しないでください。 デフォルトでは、検証コメントは、Excel からインポートされたステージングテーブルレコードで検証が実行された後に入力されます。 レコードのインポート時に検証コメントは更新されません。 ユーザーは検証コメントを編集できません。
BV	検証ステータス	文字列	ユーザーはこの列に入力しないでください。 デフォルトでは、データがステージングテーブルにインポートされると、検証ステータスが設定されます。 OT デバイスのステータス:

列	必須の列名	タイプ	説明と例
			検証の保留中 レコード がステー ジング テーブ ルにイン ポートさ れるとき のデフォ ルトス テータ ス。 無効 CMDB に CI レ コードを 一意に作 成するこ とはでき ません。 部分的に有効 変換済 みの名 前、MAC アドレス 1、シリ アル番号 のいずれ かに値が ありませ ん。他の すべての フィール ド (相関 ID、コン トロール モジュー ルの親 ID) には 値があり ます。 有効 すべての 識別子が 存在し、 インポー トの準備 ができて います。 インポート済み

列	必須の列名	タイプ	説明と例
			ステージングテーブルからインポートセットテーブルへのデータのインポートを完了しました。 ユーザーは検証ステータスを編集できません。
BW	ベンダー	文字列	OT デバイスのベンダーの名前。

列 1 から 8

列	必須の列名	タイプ	選択肢列 (該当する場合)	説明と例
1	バックアップ構成ステータス	選択肢リスト	バックアップが有効、バックアップが無効、不明、適用外、計画済み、計画外	CI が関連するポリシーと一緒にバックアップサービスまたはアプライアンスに構成されているかどうかを示します。 例:バックアップが有効
2	バックアップ実行モード	選択肢リスト	手動、自動、手動または自動、不明	バックアップが定期的に自動で実行されるように構成されているか、必要に応じて手動で実行されるように構成されているかを示します。 例:手動、自動
3	バックアップソース ID	文字列		外部または内部のバックアップサービスでデバイスを識別する、デバイスのバックアップサービスソース識別子。バックアップソース ID には、host_id、vcenter_id、instanc

列	必須の列名	タイプ	選択肢列 (該当する場合)	説明と例
				を含めることができます。 例:AdvWrks2008R2Backup
4	最後のバックアップ試行	glide_date_time		デバイスに対して最後にバックアップを試みた日時。 例:2024-06-18 09:53:37
5	最後に成功したバックアップ	glide_date_time		デバイスに対して最後に成功したバックアップの日時。 例:2024-06-18 09:53:37
6	バックアップ目標復旧時点	glide_duration		バックアップ間の経過時間と失われたデータの量を表します。 例:90 12:00:00
7	バックアップ管理担当者	文字列		バックアップの管理を担当するユーザーのメール ID 例:firstname.lastname@example.
8	バックアップ管理グループ	文字列		バックアップの管理を担当するプライマリサポートグループの名前。 例:App Engine アドミン

2. Microsoft Excel スプレッドシートに入力したら、簡単にアクセスしてアップロードできるように既知の場所に保存します。

インポートされたステージングレコードの検証

インポートタスクからインポートされたステージングレコードを検証して、欠落しているデータ、重複するデータ、無効なデータを検出します。

始める前に

必要なロール:ot_excel_import_user

手順

1. 移動先 **すべて > 産業用ワークスペース**.
2. リスト (☰) アイコンを選択します。
3. [OT Excel SGC:インポートタスク] モジュールで、使用可能なリストのいずれかを選択します。
4. 検証するインポートタスクレコードを選択します。
5. [検証] UI アクションが表示されるように、インポートタスクにアサインされていることを確認してください。

i 注: インポートタスクの [アサイン先] フィールドを表示していない場合は、次の手順に進む前に、[自分にアサイン] UI アクションをクリックします。

6. [検証] UI アクションをクリックします。
検証プロセスが完了すると、インポートタスクレコードの [ステータス] フィールドが [検証完了 (**Validation complete**)] に変わります。作成されたステージングレコードの検証ステータスは、次のいずれかの値に更新できます。

- 有効
- 無効
- 一部無効

無効な場合、[検証コメント] フィールドに無効な状態の原因が含まれます。

インポートされたステージングレコードが CMDB内の既存の構成アイテム (CI) と一致する場合は、既存の OT レコードをプレビューできます。詳細については、「[で既存の OT レコードをプレビュー CMDB](#)」を参照してください。

次のタスク

有効なレコードの場合は、構成管理データベース (CMDB) インポートを直接トリガーできます。詳細については、「[有効なステージングレコードの CMDB インポートをトリガーします](#)」を参照してください。

無効または部分的に無効なレコードを解決するために、オプションで修復タスクを作成できます。詳細については、「[無効なステージングレコードの修復タスクの作成](#)」を参照してください。

検証の管理

検証では、ステージングテーブルにインポートされたデータを確認および管理できます。

実行する検証:

- 相関 ID がありません (相関 ID)
- タイプがコントロールモジュール (コントロールモジュールの親 ID) の場合、親相関 ID がありません
- シリアル番号 (シリアル番号) がありません
- 変換済みの名前 (変換済みの名前) がありません
- MAC アドレスがありません (検証は列 MAC アドレス 1 で実行されます)
- 欠損タイプ (タイプ)
- ラック番号がありません (ラック番号)
- スロット番号がありません (スロット番号)
- 機器モデルエンティティパスが存在しません (機器モデルエンティティパス)

- 指定されたサイト名が無効です (サイト名)
- 変換済みの名前 (変換済みの名前) の重複を検証

i 注: コントロールモジュールでは、この検証はスキップされます。

- MAC アドレスの重複を検証 (MAC アドレス 1 のすべての列を確認)
- シリアル番号列 (シリアル番号) の重複を検証
- 相関 ID 列 (相関 ID) の重複を検証
- ラック番号とスロット番号の重複を検証

i 注: この検証はコントロールモジュール専用です。

- モジュールとコントロールモジュールの親 ID を検証

i 注: この検証は、PLCと制御モジュールのみを対象としています。

- 無効なタイプの検証: `sn_otsm_sgc.SGOTAssetImportExtensionPoint` 拡張ポイント実装を使用して、デフォルトの Excel タイプから OT デバイスタイプへのマッピングと比較します。

追加のマッピングがある場合は、拡張ポイント

`sn_otsm_sgc.SGOTAssetImportExtensionPoint` ベースシステムの拡張ポイント実装を作成します。

デバイス分類のカスタム実装の追加の詳細については、「[デバイス分類のカスタム実装を追加する](#)」を参照してください。

で既存の **OT** レコードをプレビュー **CMDB**

ステージングテーブルから新しいレコードをインポートする前に、構成管理データベース (CMDB) 内の既存のオペレーショナルテクノロジー (OT) デバイスレコードをプレビューします。既存のレコードをプレビューすることで、関連のないレコードの調整や結合を回避できます。

始める前に

必要なロール: `ot_excel_import_user`

このタスクについて

ステージングテーブルから OT デバイスをインポートするときに一致する構成アイテム (CI) が CMDB 内にある場合、既存のレコードが新しいレコードと調整または結合される場合があります。一致する CI には、ホスト名、MAC アドレス、またはシリアル番号が含まれます。誤ってレコードを調整または結合しないように、ステージングテーブル内のレコードと一致する CI を共有する既存のレコードをプレビューできます。

手順

1. 移動先 **すべて > 産業用ワークスペース**.
2. リスト () アイコンを選択します。
3. [OT Excel SGC:インポートタスク] モジュールで、使用可能なリストのいずれかを選択します。
4. 一致する CI があることを確認するインポートタスクレコードを選択します。
5. [検証コメント] 列で、一致する CI が見つかったかどうかを確認します。
[検証コメント] 列には、見つかった一致する CI の説明と、一致する CI へのリンクが含まれています。一致する CI が CMDBで見つかり、[検証] ステータスは [部分的に有効] に設定されます。次の表に、一致する CI 検証コメントを示します。

一致する CI 検証コメント

一致する CI	検証コメント
ホスト名	別の CI に対して同じ変換済みの名前が見つかりました:<Link to CI>
MAC アドレス	別の CI に対して同じ MAC アドレス [MAC アドレス] が見つかりました:<Link to CI>
シリアル番号	別の CI で同じシリアル番号 [シリアル番号] が見つかりました: <Link to CI>

6. オプション: [Matching CI in the CMDB (CMDB 内の一致する CI)] 列から選択して、一致する CI を確認します。

有効なステージングレコードの **CMDB** インポートをトリガーします

有効なステージングレコードの 構成管理データベース (CMDB) インポートをトリガーして、直接インポートします CMDB

始める前に

必要なロール:ot_excel_import_user

手順

1. 移動先 すべて > 産業用ワークスペース.
2. リスト (☰) アイコンを選択します。
3. [OT Excel SGC:インポートタスク] モジュールで、使用可能なリストのいずれかを選択します。
4. CMDBインポートをトリガーするインポートタスクレコードを開きます。
5. [**CMDB** インポートをトリガー] UI アクションが表示されるように、インポートタスクにアサインされていることを確認してください。
インポートタスクの [アサイン先] フィールドを表示していない場合は、次の手順に進む前に、[自分にアサイン] UI アクションをクリックします。
6. [**CMDB** インポートをトリガー] UI アクションをクリックします。
7. 産業用ワークスペースの OT リストモジュールで新しくインポートされた OT デバイスを確認します。

無効なステージングレコードの修復タスクの作成

Microsoft Excel のサービスグラフコネクタとともにインポートされたオペレーショナルテクノロジー (OT) デバイスデータの検証を実行した後、オプションで修復タスクを作成して無効なステージングレコードを解決します。

始める前に

必要なロール:ot_excel_import_user

このタスクについて

オプションで、無効なステージングレコードを解決するための修復タスクを作成できます。ステージングレコードで発生する可能性のある検証エラーの詳細については、「[検証の管理](#)」を参照してください。

手順

1. 移動先 **すべて > 産業用ワークスペース**.
2. リスト (☰) アイコンを選択します。
3. [OT Excel SGC:インポートタスク] モジュールで、使用可能なリストのいずれかを選択します。
4. 修復タスクを作成するインポートタスクレコードを選択します。
5. [修復タスクの作成 (**Create Remediation Tasks**)] UI アクションが表示されるように、インポートタスクにアサインされていることを確認してください。
インポートタスクの [アサイン先] フィールドを表示していない場合は、次の手順に進む前に、[自分にアサイン] UI アクションをクリックします。
6. [修復タスクの作成] UI アクションをクリックします。

結果

無効なステージングレコードに対して修復タスクが作成されます。インポートタスクレコードの修復タスクにアクセスするには、[修復タスク] リストを選択します。

i 注: 同じサイトに属する無効なステージングレコードすべてに対して、1 つの修復タスクが作成されます。

修復タスクレコードを表示するときに、[ステージングレコード] タブを選択して、それに関連付けられたステージングレコードを表示することもできます。

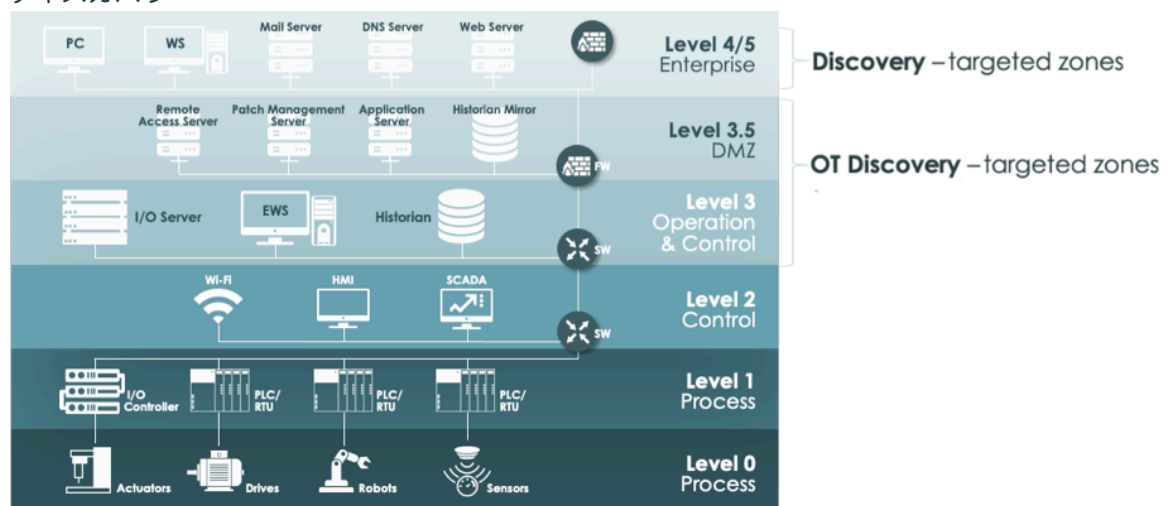
OT ネットワークの IT ディスカバリー

OT ネットワークの IT ディスカバリー機能を実行して、産業用コン オペレーショナルテクノロジー システム (ICS) ネットワーク内の指定された Purdue レベルの IT クラス (OT) デバイスを検出できます。IT クラスアイテムには、データセンターと工場の両方に存在するスイッチ、ルーター、およびコンピューターが含まれます。

標準的な ディスカバリー 処理が行われる場所

OT ネットワークの IT ディスカバリープロセスは、標準のディスカバリープロセスと同様に動作します。

OT ネットワークの標準および IT ディスカバリーのターゲットとなる Purdue レベル
ディスカバリー



ServiceNow AI Platform の標準ディスカバリー処理は、通常、エンタープライズ内の次の Purdue レベルで行われます。

処理済みの **Purdue** レベル

Purdue レベル	説明
4	すべての情報技術 (IT) 機能などのサイトビジネスとロジスティクス。
5	エンタープライズネットワーク。エンタープライズリソースプランニング (ERP) 機能が使用されます。

- i** 注: 産業用制御システムの Purdue レベルの詳細については、「https://subscription.packtpub.com/book/networking_and_servers/9781788395151/1/ch01lvl1sec10/the-purdue-model-for-industrial-control-systems」を参照してください。

OT ネットワークの **IT** ディスカバリー処理が行われる場所と方法

対照的に、OT ネットワークの IT ディスカバリー処理は、OT ディスカバリースケジュールの作成時に選択したレベルに応じて、次の Purdue レベルで実行できます。

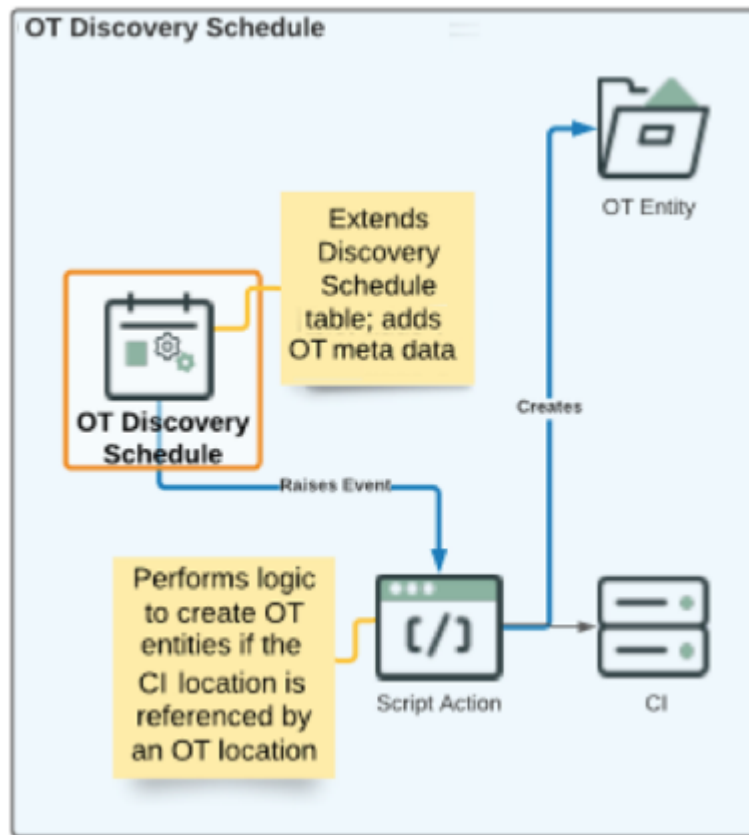
処理済みの **Purdue** レベル

Purdue レベル	説明
3.5	非武装地帯(DMZ)または産業非武装地帯(IDMZ)。従来の (IT) DMZ と同様に、OT 指向の IDMZ を使用すると、さまざまなセキュリティ要件を持つネットワークを安全に接続できます。
3	プラントまたはサイト全体の制御および監視機能が存在するサイトオペレーション。

通常、OT ネットワークの IT ディスカバリーは、ICS ネットワークの DMZ (または IDMZ、Purdue レベル 3.5) で実行します。この Purdue レベルには、通常、検出および管理する IT クラスと OT クラスのコンピューターとサーバーがあります。

- i** 注: 産業活動を中断する可能性を回避するために、ICS ネットワークで Purdue レベル 0 から 2 に対して ディスカバリー プロセスを実行しないでください。

OT ネットワークの IT ディスカバリー処理



OT ディスカバリースケジュールを実行すると、次の処理が実行されます。

1. 割り当てられた IP アドレスを処理し、そこに存在するすべてのハードウェアアイテムを検出します。
2. 構成アイテム (CI) のディスカバリーが完了すると、内部的に (discovery.device.complete) イベントがトリガーされます。このロジックは、構成管理データベース (CMDB) に OT エンティティ (cmdb_ot_entity) レコードが存在するかどうかを確認します。
 - 存在する場合、検出されたアイテムの関連属性が変更されると、その CI に関連する OT エンティティが更新されます。
 - 存在しない場合は、作成します。
3. 場所属性に加えて、定義された属性も OT ディスカバリースケジュールから CI および関連する OT エンティティレコードにプッシュされます。
4. また、検出された OT デバイスにインストールされているアプリケーションの OT エンティティレコードも作成されます。OT ネットワークの IT ディスカバリーで作成された OT エンティティレコードを持つアプリケーションを表示するには、産業用ワークスペースリストビューに移動し、[オペレーショナルテクノロジー (OT)] の下にある [アプリケーション] リストを開きます。

関連トピック

[運用テクノロジー \(OT\) 拡張クラス](#)

[MID サーバー](#)

[ディスカバリー](#)

[プローブとセンサーを使用した水平ディスカバリープロセスフロー](#)

[水平検出のスケジュール](#)

OT ネットワークの IT ディスカバリー関連リンクとリスト

OT ネットワークの IT ディスカバリーには、いくつかの関連リンクとリストが含まれています。

関連リンク

関連リンク	説明
クイック範囲	OT ディスカバリースケジュールの実行時にスキャンする IP アドレスとアドレス範囲。複数の形式 (ネットワーク、範囲、またはリスト) の IP アドレスをカンマで区切った単一の文字列に入力します。使用中の MID サーバーは、指定された IP 範囲に接続する必要があります。 詳細については、「 ディスカバリースケジュールのクイック IP 範囲の作成 」を参照してください。
ディスカバリー今	OT ネットワークの IT ディスカバリープロセスを直ちに実行します。
ポイントスキャンを実行	[ポイントスキャンを実行] ダイアログにアクセスします。詳細については、「 ポイントスキャンの実行 」を参照してください。

関連リスト

関連リスト	説明
ディスカバリー IP 範囲	ディスカバリー スキャンして検出する IP アドレスとアドレス範囲。シンプルな CI スキャン (動作なし) を使用している場合は、この関連リストを使用してこれらの IP アドレスを定義します。使用中の MID サーバーは、指定された IP 範囲に接続する必要があります。 i 注: セキュリティを強化するために、ディスカバリーターゲットの範囲を制限して不要なネットワークとデバイスを除外します。
ディスカバリー 範囲セット	1 つ以上の Shazzam プローブを使用して、OT ディスカバリースケジュールがスキャンする各範囲セットの定義。
ディスカバリー ステータス	現在および過去の OT ディスカバリースケジュール実行の結果の履歴。

関連トピック

[MID サーバー](#)

[Shazzam プローブ、ポートプローブ、およびプロトコル](#)

[Shazzam プローブの作成](#)

オペレーショナルテクノロジーディスカバリースケジュールを作成し、ディスカバリープロセスを実行します

OT 機能の ディスカバリー を実行する方法とタイミングを調整するオペレーショナルテクノロジー (OT) ディスカバリースケジュールを定義します。また、すぐにクイック ディスカバリー を実行するか、実際の OT ディスカバリー を実行することもできます。

始める前に

OT ネットワークの IT ディスカバリーを実行する前に、次のアクションを実行します。

- 標準 ディスカバリー アプリケーションをインストールして構成します。詳細については、「[ディスカバリーのセットアップ](#)」を参照してください。
- CMDB CI クラスモデルプラグインをインストールします。詳細については、「[オペレーショナルテクノロジー \(OT\) 拡張クラスのインストール](#)」を参照してください。
- MID サーバーをインストールします。詳細については、「[MID サーバーのインストール](#)」を参照してください。

必要なロール:ot_discovery_admin

手順

1. 移動先 すべて > **OT** ディスカバリー > **OT** ディスカバリースケジュール。
2. クイック ディスカバリーを実行するか、OT ディスカバリースケジュールを選択または作成します。

タスク	説明
即時実行 クイック ディスカバリー	[クイックディスカバリー] をクリックし、次のアクションを実行します。 a. [ターゲット IP] フィールドに、OT プロセスの ディスカバリー を実行する IP アドレスを入力します。 b. [MID サーバー] フィールドで、 ディスカバリー プロセスを実行する MID サーバーを選択します。 c. [OK] をクリックします。
OT 検出スケジュールを選択または作成します	a. 既存の OT ディスカバリースケジュールを選択するか、[新規] をクリックして新しいスケジュールを作成します。 b. 次の手順を実行して、[OT ディスカバリー スケジュール] フォームで OT ディスカバリースケジュールレコードを作成します。

3. フォームの [OT ディスカバリースケジュール] フィールドに入力します。

フィールド	説明
名前	OT ディスカバリースケジュールのわかりやすい一意の名前。
検出	OT ディスカバリースケジュールのスク্যানタイプ。 構成アイテム

フィールド	説明
	ディスカバリー識別子を使用して、デバイスをCMDB内の構成アイテム (CI) と照合し、CMDBを更新します。すべてのプロトコル (SSH、WMI、SNMP) をスキャンする特定の MID サーバーを選択して簡単なディスカバリーを実行するか、ディスカバリー動作を使用して高度なディスカバリーを実行します。動作を選択した場合、[MID サーバー] フィールドは利用できません。 IP アドレス 認証情報を使用せずにデバイスをスキャンします。このスキャンでは、指定された範囲内のすべてのアクティブな IP アドレスが検出され、デバイス履歴レコードが作成されますが、CMDB は更新されません。IP アドレススキャンでは、単一のデバイスで実行されている複数の IP アドレスも表示されます。Windows コンピューターや Cisco ネットワーク機器など、デバイスをクラス別およびタイプ別に識別します。
デフォルトの Purdue レベル	OT ディスカバリースケジュールを実行する Purdue レベル、またはすべての Purdue レベルに対して [--なし--] を選択する Purdue レベル。 i 注: Purdue レベルの詳細については、https://subscription.packtpub.com/book/networking_and_servers/9781788395151/1/ch01lvl1sec10/the-purdue-model-for-industrial-control-systems を参照してください。

このフォームのほとんどのフィールドは、標準のディスカバリーフォームと同じか同じように動作します。標準的なディスカバリースケジュールと異なるフィールドのみがこのトピックに表示されます。残りのフィールドの詳細については、「[水平ディスカバリーのスケジュール](#)」を参照してください。

4. ディスカバリープロセスをすぐに実行するか、OT ディスカバリースケジュールを保存してレコードで指定した時間に実行します。

タスク	説明
すぐに ディスカバリー を実行	[今すぐ検出] 関連リンクをクリックします。
OT ディスカバリースケジュールで指定された時間に ディスカバリー を実行	[Update (更新)] をクリックします。

結果

OT ネットワークの IT ディスカバリープロセスが実行されると、[ディスカバリー ステータス] 関連リストに履歴レコードが作成されます。

でオペレーショナルテクノロジー デバイスを作成する 産業用ワークスペース

産業用ワークスペースにオペレーショナルテクノロジー (OT) デバイスを作成します。

始める前に

必要なロール:cmdb_ot_editor

このタスクについて

産業用ワークスペース で OT デバイスを手動で作成して、OT エンティティ [cmdb_ot_entity] レコードを作成し、それを CI に関連付けることができます。

手順

1. 移動先 **すべて** > 産業用ワークスペース.
2. リスト () アイコンを選択します。
3. オペレーショナルテクノロジー (OT) モジュールで、次のいずれかのリストを選択します。
 - すべての OT デバイス
 - OT 監督システム
 - OT コントロールシステム
 - OT フィールドデバイス
 - OT コンピューターおよびサーバー
 - OT ネットワーク機器
 - 産業用 IoT (IIoT)
 - OT システム
 - 未分類の OT デバイス
4. [新しい CI の作成] を選択します。
5. [OT CI を作成] タブで、必要に応じて以下のセクションに入力します。
 - クラスを選択
 - 必要な属性
 - 追加の属性
 - 関係定義
 - レビュー
6. [Create (作成)] を選択します。
7. [新しい CI の作成済み (New CI created)] ウィンドウで、[新しい CI のレビュー (Review new CI)] を選択して、作成された OT CI のフォームにリダイレクトします。
既存の CI がある場合は、[既存の CI のレビュー] を選択します。
8. フォームで次のフィールドに入力します。

新規 CI フォーム

フィールド	説明
表示名	レコードに表示される OT デバイスの名前。 <i>i</i> 注: このフィールドには任意の文字列値を追加できます。複数のデバイスに同じ OT 表示名を設定できます。これは OT デバイスを理解しやすくするためのもので、ステージングテーブルから OT デバイスをインポートするときに生成される一意の CI 名とは異なります。
Purdue レベル	割り当てられた Purdue レベル。レベル範囲は 0 ～ 5 です。 <i>i</i> 注: 産業用制御システムの Purdue レベルの詳細については、「https://subscription.packtpub.com/book/networking_and_servers/9781788395151/1/ch01lvl1sec10/the-purdue-model-for-industrial-control-systems」を参照してください。
デバイスの重要度	デバイスに障害が発生した場合のサイトプロセスに対する相対的なリスクの測定: ○ 1: 最重要 ○ 4: 重要ではない
サイト	デバイスが配置またはアサインされている最上位の親エンティティ、または工業用サイト。

9. [Save (保存)] を選択します。

インポートまたは検出後に OT デバイスを編集または表示する

オペレーショナルテクノロジー (OT) メニューのオプションを使用して、企業内の OT デバイスの詳細情報を編集または表示します。

始める前に

次のいずれかの方法で オペレーショナルテクノロジー デバイスデータをインポートします。

- OT ネットワークの IT ディスカバリーを実行します。詳細については、「[OT ネットワークの IT ディスカバリー](#)」を参照してください。
- ServiceNow Store の オペレーショナルテクノロジー Certified サービスグラフ Connector を使用します。

必要なロール: cmdb_ot_viewer、cmdb_ot_editor、cmdb_ot_admin、または admin

このタスクについて

cmdb_ot_viewer ロールが割り当てられている場合は、OT デバイスのみを表示できます。cmdb_ot_editor ロールまたは cmdb_ot_admin ロールが割り当てられている場合は、次の方法で OT デバイスレコードを編集できます。

- ServiceNow AI Platform で OT デバイスレコードを個別に編集します。
- 産業用 ワークスペースリストビューから複数の OT デバイスレコードを一括編集します。

手順

1. 1 つの OT デバイスレコード ServiceNow AI Platformを編集するには、次の手順を実行します。

- a. 移動先 **すべて > オペレーショナルテクノロジー (OT)** をクリックし、次のいずれかのメニュー項目を選択します。

すべての OT デバイス

デフォルトでは、このリストにコントロールモジュールは含まれません。

IP アドレス別のすべての OT デバイス

[IP アドレス別のすべての OT デバイス] リストを表示する場合は、次の点に注意してください。

- 複数の IP アドレスを持つ OT デバイスは、割り当てられた IP アドレスごとに 1 回表示されます。
- OT デバイスの名前を選択して、OT デバイスレコードを開きます。レコードに表示される IP アドレスを選択すると、その IP アドレスのレコードのみが開きます。
- このリストから新しい OT デバイスレコードを作成することはできません。

OT コントロールシステム

デフォルトでは、このリストにコントロールモジュールは含まれません。

モジュール付き OT コントロールモジュール

[モジュール付き OT コントロールシステム (OT Control Systems with Modules)] リストを表示するときは、次の点に注意してください。

- リストビューには、親コントロールシステム別にグループ化されたすべてのコントロールモジュールが表示されます。
- このリストから新しい OT デバイスレコードを作成することはできません。

b. [**OT デバイス**] 列で、編集する OT デバイスを選択します。

c. フォームで、フィールドに入力します。

d. [**Update (更新)**] をクリックします。

2. 複数の OT デバイスレコードを 産業用 ワークスペース一括編集するには、次の手順を実行します。

a. 移動先 **すべて > 産業用ワークスペース**。

b. リスト ( ビューを開き、[**オペレーショナルテクノロジー (OT)**] で利用可能な次のいずれかのリストを選択します。

- OT 監督システム
- OT コントロールシステム
- OT フィールドデバイス
- OT コンピューターおよびサーバー
- OT ネットワーク機器
- 産業用 IoT (IIoT)
- 未分類の OT デバイス

c. 編集する各 OT デバイスの横にあるチェックボックスをオンにします。

- 注:** 一括編集できるのは、クラス フィールドが同じ OT デバイスのみです。クラスが異なる OT デバイスに一括編集機能を使用することはできません。

d. 構成アイテム (CI) フィールドを編集するには、[編集] ボタンを選択し、必要に応じてフォームフィールドを編集します。



す。

- 注:** CI フィールドを一括編集できるレコードの最大数は、1 ページに表示されるレコード数です。

e. [Update (更新)] をクリックします。

f. OT デバイスの詳細を編集するには、[OT の詳細を編集] ボタンを選択し、必要に応じてフォームフィールドを編集します。



す。

- 注:** OT の詳細の一括編集はバックグラウンドジョブであり、完了するまでに時間がかかる場合があります。バックグラウンドジョブがビジー状態の場合、他の OT デバイスレコードを一括編集することはできません。

OT デバイスの関連アイテムと関連リスト

[すべての OT デバイス]、[IP アドレス別のすべての OT デバイス]、および [CI 別のすべての OT デバイス] メニューオプションには、いくつかの関連アイテムとリストが含まれています。

関連アイテム

このセクションには、この OT デバイスに関連付けられている関連アイテムまたは従属アイテムが一覧表示されます。

- 注:** すべての OT デバイスに次の関連リストが表示されるわけではありません。オペレーショナルテクノロジークラスまたは拡張クラスの OT デバイスの場合、次の関連リストが表示されます。Windows サーバーなど、別のハードウェアクラスに分類される OT デバイスの場合、インスタンスアドミンは関連リストをフォームに追加する必要があります。

1. 関連レコードを表示するには、関連アイテムの名前 (メモリモジュールなど) をクリックします。
2. この OT デバイスの構成アイテム (CI) 関係を追加するには、[CI 関係を追加] アイコン (CI  アイコン) をクリックします。検索フィールドを使用して、関係を作成する CI アイテムを検索します。
3. 依存関係ビューフォームにアクセスして OT デバイスの関係を図で表示するには、依存関係ビューを表示アイコン () をクリックします。
4. 関連アイテムの表示方法とフィルタリング方法を管理する設定を変更するには、設定アイコン () をクリックします。

OT デバイス関連リスト

関連リスト	説明
IP アドレス	OT デバイスに関連付けられている IP アドレス、IP バージョン、ネットマスク、NIC 番号、および構成アイテム。
ネットワークアダプタ	名前、MAC アドレス、IP アドレス、ネットマスク、MAC メーカー、および Dynamic Host Configuration Protocol(DHCP)対応インジケータ。これには、OT デバイスに関連付けられているネットワークアダプタのステータスが含まれます。
シリアル番号	OT デバイスに関連付けられているシリアル番号、有効性インジケータ、およびシリアル番号タイプ。
機器モデルエンティティ	OT デバイスによって自動化される機器モデルエンティティ。
OT サブネットマッピング	OT デバイスを機器モデルエンティティに関連付けるサブネットマッピング。
OT コントロールモジュール	OT コントロールシステムタイプまたは拡張クラス (PLC など) の OT デバイスに関連付けられているコントロールモジュール。 表示される OT コントロールシステムレコードとの「所有者:所有」関係を持つ各 OT コントロールモジュール。 プラットフォームでは、ユーザーは OT コントロールモジュールを作成できます。 [モジュールタイプ] フィールドに応じて、次の入力/出力値から選択できます。 • なし • ローカル • リモート • Distributed
CMDB 360	マルチソース CMDB [cmdb_multisource_data] テーブル内の関連する CMDB 360 データ。
メモリモジュール	OT デバイスに関連付けられているメモリモジュールのシリアル番号、有効性インジケータ、およびシリアル番号タイプ。
インストールされているソフトウェア	OT デバイスにインストールされているアプリケーションソフトウェア (存在する場合)。
OT 脆弱性一致アイテム	OT デバイスに関連付けられている脆弱性一致アイテム。
OT インシデント	OT デバイスに関連付けられている OT インシデント。
OT 変更要求	OT デバイスに関連付けられている OT 変更要求。

OT デバイス関連リスト (続く)

関連リスト	説明
外部システムメタデータ	CI に関連付けられているソースシステム、ディスカバリーソース、および更新済みデバイス内のデバイスの URL。 URL は、サービスグラフコネクタを介してソースシステムによって自動的に入力されます。
OT プロトコル	これは、プロトコルコンバータークラスに適用されます。 プロトコルコンバータークラスに関連付けられているプロトコル、説明、ベンダー、およびバージョン。
バックアップ情報	現在の CI に関連付けられているバックアップ情報オブジェクト。
デバイスからデバイスへの接続	OT デバイスと他のデバイスとのネットワーク接続を表示します。
キー値	利用可能な OT 統合が入力され、キーと値のペアとしてキャプチャされた OT デバイスに関連する追加情報。
ソフトウェアインストール	OT デバイスにインストールされているソフトウェアが利用できない場合 ソフトウェア資産管理 キャプチャします。 i 注: ソフトウェア資産管理がインストールされ、エンタイトルメントされている場合、インストール済みソフトウェアのデータが [ソフトウェア インストール] 関連リストに表示されます。
ファームウェアのインストール	OT デバイスに関連付けられたファームウェア。

オペレーショナルテクノロジーデバイスフォーム

オペレーショナルテクノロジー (OT) デバイスフォームを使用して、企業内の OT デバイスの詳細情報を編集します。

オペレーショナルテクノロジーデバイスフォーム

フィールド	説明
OT 表示名	レコードに表示される OT デバイスの名前。 i 注: このフィールドには任意の文字列値を追加できます。複数のデバイスに同じ OT 表示名を設定できます。これは OT デバイスを理解しやすくするためのもので、ステージングテーブルから OT デバイスをインポートするときに生成される一意の CI 名とは異なります。

オペレーショナルテクノロジーデバイスフォーム (続く)

フィールド	説明
OT デバイスタイプ	OT デバイスが分類されるカテゴリタイプ。デバイスタイプは、デバイスが OT ネットワーク上で果たす機能でもあります。たとえば、次のようになります。 サーバーなどのIT機器はOT機器に変換でき、ネットワーク上で果たす機能はHMIです。したがって、そのクラスは server で、デバイスタイプは HMI です。 i 注: 場合によっては、OT 機能を持たない OT デバイスや、デバイスタイプが不明な OT デバイスがあります。OT 機能のない OT デバイスの場合は、[OT 機能なし] を選択します。デバイスタイプが不明な OT デバイスの場合は、[不明] を選択します。
デバイスの重要度	デバイスの障害のサイトプロセスに対する相対的なリスクの尺度。たとえば、次のようになります。 • 1 : 最重要 • 4 : 重要ではない
サイト	デバイスが配置またはアサインされている最上位の親エンティティ、または工業用サイト。
Purdue レベル	アサインされた Purdue レベル。範囲は 0 ~ 5 です。 i 注: 産業用制御システムの Purdue レベルの詳細については、「https://subscription.packtpub.com/book/networking_and_servers/9781788395151/1/ch01lvl1sec10/the-purdue-model-for-industrial-control-systems」を参照してください。
ゾーン	デバイスが割り当てられているサイトの場所内のエリア。
クラス	OT デバイスにアサインされたクラスの名前。 i 注: CI クラスのリストと説明については、運用テクノロジー (OT) 拡張クラス を参照してください。
ステータス	OT デバイスのステータス:

オペレーショナルテクノロジーデバイスフォーム (続く)

フィールド	説明
	-- なし -- アサインされたステータスはありません。 不在 施設に OT デバイスが存在しません。 メンテナンス中 OT デバイスはメンテナンス中であり、現在オフラインです。 在庫あり OT デバイスは施設に在庫があります。 インストール済み OT デバイスが施設に設置されている。 インストール待ち OT デバイスは施設へのインストールを保留中です。 修理待ち OT デバイスは修理を保留中ですが、まだオンラインではありません。 廃止 OT デバイスが廃止されました。 盗難 OT デバイスが盗まれました。
ディスカバリー 源	OT デバイスデータの ディスカバリー ソース。たとえば、統合ハブ ETL を使用して Microsoft Excel スプレッドシートから OT デバイスをインポートした場合は、SG-OT Excel インポートです。詳細については、「 Microsoft Excel のサービスグラフコネクタ 」を参照してください。
インフラストラクチャ関係	OT デバイスと他の OT デバイスおよび機器モデルエンティティとの関係を示します。
サービス関係	OT デバイスと機器モデルエンティティの関係を示します。
CI タイムライン	OT デバイスに関連付けられた OT インシデント、OT 変更、および監査履歴のタイムラインを表示します。
次のフィールドは、プログラマブルロジックコントローラー (PLC) クラスレコードにのみ適用されます。	
キースイッチ	キースイッチモード:

オペレーショナルテクノロジーデバイスフォーム (続く)

フィールド	説明
	リモートモード PLCの構成を変更できます。 ローカルモード デフォルトモードでは、PLCの構成を変更できません。
スイッチ位置	PLCのスイッチ位置には、次の位置があります。 • ラン • プログラム • リモート • 停止 • テスト デフォルトでは、スイッチの位置は [なし] に設定されています。 スイッチの位置が リモートに設定されている場合、スイッチリモートモードが有効になります。
スイッチリモートモード	PLCのスイッチリモコンには次のモードがあります。 • ラン • プログラム • テスト • なし
資産	構成管理データベース (CMDB)で構成アイテム (CI) が作成されると、資産レコードが作成されます。資産レコードには、CI のモデルカテゴリが含まれています。オペレーショナルテクノロジー (OT) のモデルカテゴリの詳細については、「のモデルカテゴリ オペレーショナルテクノロジー」を参照してください。OT デバイスのモデルカテゴリを表示するには、次の手順を実行します。 1. 移動先 すべて > オペレーショナルテクノロジー (OT) > すべての OT デバイス。 2. 資産レコードを表示する OT デバイスを選択します。

オペレーショナルテクノロジーデバイスフォーム (続く)

フィールド	説明
	3. [資産] フィールドの横にある [このレコードをプレビュー] アイコン () を選択します。 4. [レコードを開く (Open Record)] を選択します。
次のフィールドは、次のクラスレコードにのみ適用されます。 • OT 監督システム • OT コントロールシステム • OT フィールドデバイス • 未分類の OT デバイス	
仮想	選択した場合、OT デバイスが仮想であることを示します。

IT ハードウェアデバイスを **OT** デバイスに変換する

OT ネットワークに属する IT ハードウェアデバイスを特定した場合は、これらの IT 構成アイテム (CI) を OT デバイスに変換できます。

始める前に

必要なロール:cmdb_ot_admin または admin

このタスクについて

このタスクは、すべての IT ハードウェアデバイスに適用できます。

手順

1. IT CI を選択します。
たとえば、すべて > 構成 > ベースアイテム > コンピュータ。
2. OT デバイスに変換する IT ハードウェアデバイスを選択します。
3. [関連リンク] モジュールで、[**OT** デバイスの詳細を追加] を選択します。

[OT デバイス] フォームが表示されます。
4. [OT デバイスの詳細] フォームのフィールドに入力します。
5. [Update (更新)] を選択します。
6. 変換された OT デバイスを表示するには、次に移動します: すべて > オペレーショナルテクノロジー (**OT**) > すべての **OT** デバイス。

結果

選択した IT ハードウェアデバイスが OT デバイスに変換されました。

または、複数の IT ハードウェアデバイスを選択し、一括編集で OT デバイスに変換することもできます。詳細については、「[一括編集で IT ハードウェアを OT デバイスに変換する](#)」を参照してください。

一括編集で IT ハードウェアを OT デバイスに変換する

複数の IT ハードウェアデバイスを選択し、一括編集で OT デバイスに変換することで、レコードをより迅速かつ効率的に編集できます。

始める前に

必要なロール:cmdb_ot_admin または admin

手順

1. 移動先 すべて > 産業用ワークスペースアドミン > 産業用ワークスペース。
2. 産業用 ワークスペースで、[すべての IT ハードウェア] リストに移動します。
3. オプション: [すべての IT ハードウェア] リストをフィルタリングするには、次のアクションを実行します。
 - リストの右上隅にあるフィルター 
 - 適用するフィルターをリストに追加します。
 - **[Update (更新)]** を選択します。
4. 変換する各 IT ハードウェアデバイスの横にあるチェックボックスをオンにします。
リスト内のすべての IT ハードウェアデバイスを選択する場合は、[名前] 列の横にあるチェックボックスをオンにします。
5. **[OT デバイスに変換]** ボタンを選択します。
6. フォームで、フィールドに入力します。

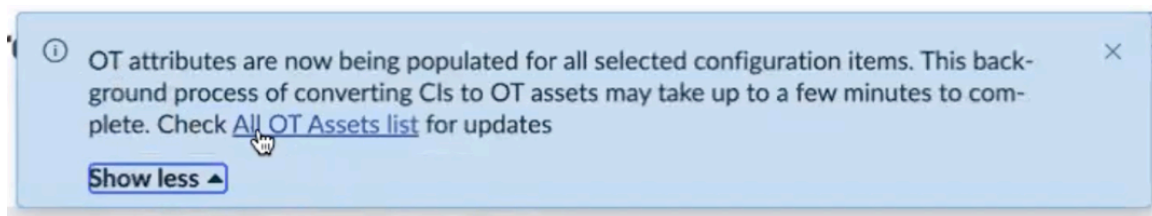
[OT デバイスに変換] フォーム

フィールド	説明
OT デバイスタイプ	OT デバイスが分類されるカテゴリタイプ。デバイスタイプは、デバイスが OT ネットワーク上で果たす機能でもあります。たとえば、次のようになります。 サーバーなどのIT機器はOT機器に変換でき、ネットワーク上で果たす機能はHMIです。したがって、そのクラスは server で、デバイスタイプは HMI です。  注: 場合によっては、OT 機能を持たない OT デバイスや、デバイスタイプが不明な OT デバイスがあります。OT 機能のない OT デバイスの場合は、[OT 機能なし] を選択します。デバイスタイプが不明な OT デバイスの場合は、[不明] を選択します。
デバイスの重要度	デバイスに障害が発生した場合のサイトプロセスに対する相対的なリスクの測定: ○ 1 : 最重要 ○ 4 : 重要ではない

フィールド	説明
Purdue レベル	割り当てられた Purdue レベル。レベル範囲は 0 ～ 5 です。 <i>注:</i> 産業用制御システムの Purdue レベルの詳細については、「https://subscription.packtpub.com/book/networking_and_servers/9781788395151/1/ch01lvl1sec10/the-purdue-model-for-industrial-control-systems」を参照してください。
ゾーン	デバイスが割り当てられているサイトの場所内のエリア。
サイト	デバイスが配置またはアサインされているトップレベルの親エンティティ、または工業用サイト。

7. [変換] を選択します。

プロセスが開始されたことを知らせる次のバナーが表示されます。[すべての OT デバイス] リストで更新を確認するには、バナーのリンクを選択します。



自動翻訳

結果

選択した IT ハードウェアデバイスが OT デバイスに変換されました。

IT を OT に再アサインするための一括更新ルールセット機能を使用して、IT ハードウェアを OT デバイスに自動的に変換するスケジュール済みジョブを作成することもできます。詳細については、「[IT レコードを OT デバイスに自動的に変換します](#)」を参照してください。

一括編集で **OT** デバイスを **IT** ハードウェアデバイスに変換する

オペレーショナルテクノロジー (OT) デバイスを一括編集して、OT デバイスの詳細を削除します。次に、OT デバイスを IT ハードウェアデバイスに変換します。

始める前に

必要なロール: cmdb_ot_admin または admin

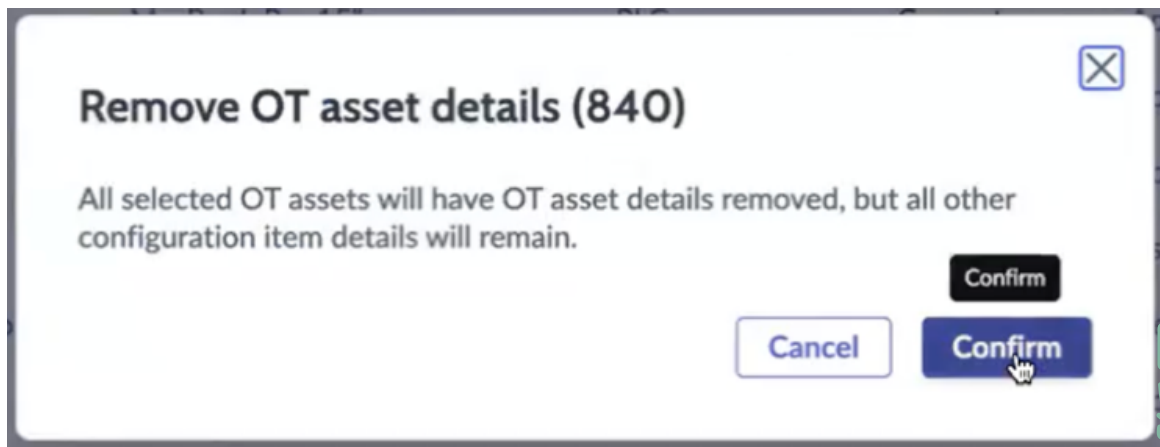
このタスクについて

OT 機能を持たず、IT ハードウェアデバイスとして分類する必要がある OT デバイスに遭遇した場合は、一括編集で複数の OT デバイスを選択して編集し、それらを IT ハードウェアデバイスに変換できます。

手順

1. 移動先 **すべて > 産業用ワークスペースアドミン > 産業用ワークスペース**。
2. リストビューで、次のいずれかのリストを選択します。

- OT コンピューターおよびサーバー
 - OT ネットワーク機器
 - 産業用 IoT (IIoT)
3. IT ハードウェアデバイスに変換する OT デバイスを選択します。
リスト内のすべての OT デバイスを選択する場合は、[OT デバイス] 列の横にあるチェックボックスをオンにします。
4. [**OT** デバイスの詳細を削除] ボタンを選択します。
OT デバイスの詳細を削除し、他のすべての構成アイテムの詳細を保持することを確認するダイアログボックスが表示されます。
- i** 注: CI の詳細、ネットワークアダプタ、または IP アドレスは削除されません。OT 固有のデータのみが削除されます。



5. [**Confirm** (確認)] を選択します。

結果

選択した OT デバイスから OT デバイスの詳細が削除され、OT デバイスが IT ハードウェアデバイスに変換されます。これらの IT ハードウェアデバイスは、産業用ワークスペースの [IT ハードウェア] リストビューで表示できます。

IP アドレスを OT デバイ스에 マッピング

SyncIPAddressToOT スケジュール済みジョブを使用して、利用可能なすべての OT デバイスの IP アドレス情報を更新および同期できます。SyncIPAddressToOT スケジュール済みジョブは、IP アドレス (cmdb_ci_ip_address) テーブルから IP アドレス情報を取得し、CI の IP アドレスフィールドに追加します。

始める前に

必要なロール: admin

手順

1. 移動先 **すべて** > システム定義 > スケジュール済みジョブ.
2. [スケジュール済みジョブ] ページで、[検索] フィルターに「SyncIPAddressToOT」と入力し、Enter キーを押してスケジュール済みジョブを検索します。
3. SyncIPAddressToOT を選択します。
4. [スケジュール済みスクリプト実行SyncIPAddressToOT] ページで、[今すぐ実行] を選択します。

デバイス間接続の表示と編集

産業用ワークスペースの [デバイス間接続] リストを使用して、オペレーショナルテクノロジー (OT) デバイスのデバイス間接続を表示および編集します。

始める前に

- Industrial Core [sn_ot_core] プラグインがインストールされていることを確認します。
- 必要なロール：admin

このタスクについて

デバイスからデバイスへの接続では、OT デバイスルックアップロジックに OTNetworkUtils スクリプトインクルードを使用します。ルックアップロジックは、IP アドレス、サイト、および管理対象ネットワークに基づいて、対応する送信元と宛先の CI を識別します。

[デバイスからデバイス間接続] リストには、OT デバイスネットワーク接続 [sn_ot_device_network_connection] テーブルと CI 関係 [cmdb_rel_ci] テーブルの両方のフィールドが表示されます。

手順

1. 移動先 **すべて > 産業用ワークスペース**。
2. リスト (☰) アイコンを選択します。
3. **[OT ネットワーク]** モジュールの下で、[デバイスからデバイス間の接続] リストを選択します。
4. 必要に応じて、次のフィールドを編集します。

[デバイス間接続] フォーム

フィールド	説明
親	ソースデバイスの構成アイテム (CI) レコード。
子	宛先デバイスの CI レコード。
ソース IP アドレス	ソースデバイスにアサインされた IP アドレス。
ソースデバイス CI	ソースデバイスの CI レコード。
ソース MAC アドレス	ソースデバイスの MAC アドレス。
宛先 IP アドレス	宛先デバイスに割り当てられた IP アドレス。
宛先デバイス CI	宛先デバイスの CI レコード。
宛先 MAC アドレス	宛先デバイスの MAC アドレス。
宛先ポート	宛先デバイスが通信に使用するネットワークポート。
前回の通信タイムスタンプ	デバイスが最後に通信した日時。 i 注：前回の通信タイムスタンプが 90 日以上のデバイス間接続レコードは削除されます。 前回の通信タイムスタンプを編集するには、次のアクションを実行します。

フィールド	説明
	a. 移動先 すべて > インスタンススキャン > テーブルのクリーンアップ. b. <code>sn_ot_device_network_connection</code> レコードで、必要に応じて [経過時間 (秒)] フィールドを編集します。デフォルトは 7,776,000 です。
転送プロトコル	データ転送に使用されるプロトコル。たとえば、TCP、UDP などです。
アプリケーションプロトコル	使用されるアプリケーションレベルのプロトコル。例: HTTP、Modbus、FTP
ソース管理対象ネットワーク	ソースデバイスが存在する管理対象ネットワークセグメント。
宛先管理対象ネットワーク	宛先デバイスが存在する管理対象ネットワークセグメント。
ディスカバリーソース	接続情報を提供しているソース。

5. [Save (保存)] を選択します。

結果

OT デバイスのデバイス間接続を表示するには、OT デバイスレコードの [デバイスからデバイス間の接続] 関連リストにアクセスします。OT デバイスの関連アイテムと関連リストの詳細については、「[インポートまたは検出後に OT デバイスを編集または表示する](#)」を参照してください。

ネットワーク侵入検知システムアプライアンスの管理

`cmdb_nids_admin` ロールまたは `admin` ロールを持っている場合は、ServiceNow AI Platform の NIDS メニューからネットワーク侵入検知システム (NIDS) クラスレコードにメタデータ属性を割り当てることができます。

ネットワーク侵入検知システムは、サポートされている統合からの IT および OT デバイスのインポートを管理するのに役立ちます。場所や NIDS ネットワークタイプなどのメタデータを NIDS レコードに割り当てると、検出された OT デバイスと IT デバイスを区別しやすくなり、関連するメタデータが作成されたレコードに自動的に追加されます。`cmdb_nids_admin` ロールまたは `admin` ロールを持つユーザーは、「**NIDS** アサインメタデータ」タブを編集し、アクティビティストリームでユーザーが行った変更を表示できます。

- i** 注: テーブル内の NIDS レコードの手動作成は、レコードのリストビューまたはフォームビューから制限されます。

NIDS クラスレコードについて詳しくは、[ネットワーク侵入検知システム \(NIDS\) CI 拡張クラス](#) を参照してください。

NIDS レコードの [検証済み] フィールドが `true` に設定されている場合、NIDS フォームで NIDS の次の属性のいずれかが変更されると、警告メッセージが表示されます。

- NIDS ネットワークタイプ
- NIDS ソース名
- NIDS ソース ID

関係によって検出された NIDS レコードが削除されると、警告メッセージが表示されます。

ネットワーク侵入検知システム (NIDS) ガイド付きセットアップを使用して、次の手順を実行できます。

- インスタンスでまだアカウントを持っていないユーザーのためにユーザーとロールを構成する
- オペレーショナルテクノロジー (OT) 認定サービスグラフコネクタから NIDS レコードをインポートして、NIDS アプライアンスが OT ネットワークと IT ネットワークのどちらで実行されているかを指定する
- 検出されたデバイスをインポートできるように NIDS を検証する。NIDS の検証について詳しくは、[NIDS の検証](#)を参照してください。

NIDS ガイド付きセットアップにアクセスするには、 **ネットワーク侵入検知システム (NIDS) > NIDS ガイド付きセットアップ**。

デバイスを検出する NIDS センサーのマネージャーとしてアプライアンスを割り当てるには、 **ネットワーク侵入検知システム (NIDS) > マネージャー** 該当する「管理コンソール」または「中央マネージャー」レコードを編集します。

- センサーリストをレビューし、現在マネージャーとしてアサインされているデバイスがないことを確認します。
- センサーとして機能しないデバイスの場合、変更はマネージャーを **True** にします。

NIDS で割り当てられたメタデータを検出されたデバイスにコピーする NIDSUtils スクリプトインクルードについては、 [インストールされたスクリプトインクルード オペレーショナルテクノロジーマネージャー](#)を参照してください。

関連トピック

[ネットワーク侵入検知システム \(NIDS\) CI 拡張クラス](#)

[インストールされたスクリプトインクルード オペレーショナルテクノロジーマネージャー](#)

NIDS の検証

NIDS を検証して、センサーによって検出されたデバイスを ETL からインポートします。センサーはデバイスインポートの対象ではないため、センサーはラーニングモードでない場合にのみ検証に合格できます。

始める前に

共通サービスデータモデル (CSDM) プラグインをインストールすることをお勧めします。サービスグラフコネクタは、構成管理データベース (CMDB) 標準に従ってライフサイクルデータモデルに合わせて調整されます。詳細については、「[CSDM フレームワークを段階的に実装する](#)」を参照してください。

必要なロール: cmdb_nids_admin

このタスクについて

[ライフサイクルステージ] フィールドと [ライフサイクルステージステータス] フィールドは、センサーの学習モードをキャプチャするために使用されます。[ライフサイクルステージ] フィールドが [運用] に設定され、かつ [ライフサイクルステージステータス] が [学習モード] に設定されている場合、検証は失敗します。[ライフサイクルステージステータス] フィールドが [使用中] に設定されている場合、検証は成功しています。

手順

1. 移動先 **すべて > ネットワーク IDS アプライアンス (NIDS) > センサー**。
2. リストに管理コンソールまたは中央マネージャーがある場合は、次のアクションを実行します。

- a. [レコードを編集] をクリックします。
- b. 「NIDS アドミン構成」 タブで、「**NIDS** マネージャーである」を選択して、「検証済み」列を true に設定します。
3. 「NIDS アドミン構成」セクションで、「ライフサイクルステージステータス」の値が「学習モード」になっていないことを確認します。
それ以外の場合、検証は失敗します。
4. **NIDS** ネットワークタイプを選択します。

ネットワークタイプは、センサーの場所に基づいて選択する必要があります。

- i** 注: ネットワークタイプ OT によって OT デバイスレコードが作成されます。ネットワークタイプ IT では、OT デバイスレコードは作成されません。

5. [**NIDS** アサインメタデータ (**NIDS Assigned Meta Data**)] タブで、NIDS によって検出されたすべてのデバイスが入力されていることを確認します。
6. [検証] をクリックします。

i 注:

ゾーン値は ETL によって入力されます。ゾーン値が NIDS レコードに手動で入力された場合、ETL によって入力された内容が上書きされます。

NIDS レコードが検証されない場合、センサーによって検出されたデバイスは ETL からインポートされません。

次のタスク

または、一括検証で複数の NIDS センサーを検証することもできます。詳細については、「[複数の NIDS センサーを一度に検証する](#)」を参照してください。

複数の **NIDS** センサーを一度に検証する

一括検証を通じて複数の NIDS センサーを一度に検証し、レコードをより迅速かつ効率的に編集できるようにします。

始める前に

必要なロール:cmdb_nids_admin

このタスクについて

各 NIDS センサーを個別に検証する代わりに、一括検証を使用して複数の NIDS センサーを一度に検証できます。

- i** 注: ディスカバリーソースごとに NIDS センサーを慎重に確認し、一括検証中は注意して続行してください。

手順

1. 移動先 **すべて > ネットワーク IDS アプライアンス (NIDS) > センサー**。
2. 検証するセンサーレコードのチェックボックスをオンにします。
3. [**Validate Sensors**] ボタンを選択します。

結果

検証したセンサーの ライフサイクルステージステータス が [使用中] の場合、検証成功のメッセージが表示されます。

選択したセンサーの [ライフサイクルステータス] が [ラーニングモード] であるか、[検証済み] 列が true に設定されている場合は、ラーニングモードの 1 つ以上のセンサーが検証されていないか、まだ検証されていないことを警告するエラーメッセージが表示されます。一括検証を続行するには、[ライフサイクルステータス] 列を [使用中] に変更することを検討する必要があります。

オペレーショナルテクノロジーシステムサービスのモデル化

オペレーショナルテクノロジー (OT) システムサービスをモデル化して、分散制御システム (DCS) などの他の制御システムを作成できます。

OT システムサービスとは、物理プロセス、機械、および生産工程を管理、制御、および監視するために使用されるテクノロジーとシステムのカテゴリを指します。OT システムサービスは通常、製造、エネルギー、公益事業、輸送などのセクターで採用されています。

OT システムサービスには次のものが含まれます。

- 分散制御システム (DCS)
- Supervisory Control and Data Acquisition (SCADA)
- 産業用制御システム (ICS)
- 安全計装システム (SIS)
- 製造実行システム (MES)
- プロセス制御システム
- 輸送管理システム
- エネルギー管理システム
- ビル管理システムサービス (BMS)

これらのシステムサービスは、産業プロセスを効率的かつ安全に実行することを集合的に保証します。

DCS の例

OT システムサービスをモデル化して、他のコントロールシステムを作成できます。たとえば、分散制御システム (DCS) とすべての関連コンポーネント (PLC、制御モジュール、EWS、RTU、HMI、SCADA など) をモデル化できます。DCS は、プラントや生産工程の自動制御と運用のためのプラットフォームです。DCS によって、多数の異なるプロセスを行うプラント全体を調整および監督します。

DCS は、閉ループ制御を使用するプロセス指向のシステムです。次の表で、DCS のコンポーネントについて説明します。

DCS のコンポーネント

コンポーネント	説明
オペレーターステーション	DCS の心臓部であるオペレーターは、プロセスを目で確認し、アラームとアラートを監視します。
サーバー、EWS、ヒストリアン	ハードウェア構成のデータ収集とデータ交換。
コントローラー、I/O モジュール	サーバーへのデータ交換。
フィールドデバイス	トランスミッター、スイッチ、アクチュエーター、バルブなどのデバイス。

DCS は、中央にある単一のコントローラーが制御機能処理する集中制御システムとは異なりますが、この中では各プロセス要素、マシン、またはマシンのグループが専用のコントローラーによって制御されます。

オペレーショナルテクノロジーシステムサービスの作成

オペレーショナルテクノロジー (OT) システムサービスを作成して、分散制御システム (DCS) とそのすべての関連コンポーネント (制御モジュール、プログラミングロジック制御 (PLC) など) をモデル化します。

このタスクについて

次の場所で OT システムサービスを作成できます。

- ServiceNow AI Platform **OT** システムリストの
- 産業用 ワークスペース リストビュー

始める前に

必要なロール：admin

手順

1. ServiceNow AI Platform で OT システムサービスを作成する場合は、次のアクションを実行します。
 - a. 移動先 **すべて > オペレーショナルテクノロジー (OT) > OT システム**.
 - b. **[New (新規)]** を選択します。
 - c. フォームで次のフィールドに入力します。

OT システムサービスフォーム

フィールド	説明
表示名	OT システムサービスの表示名を入力するために使用されます。
名前	OT システムサービスのホスト名。
ISA エンティティサイト	OT システムサービスが属する ISA エンティティサイト。
メーカー	OT システムサービスのメーカーの名前。
モデル番号	OT システムサービスのメーカーのモデル番号。
簡単な説明	OT システムサービスの簡単な説明。
詳細	
所有者	OT システムサービスのプライマリ所有者の名前。
管理担当者	OT システムサービスのプライマリマネージャーの名前。
事業上の重要度	システムサービスの重要度または重要度の測定値。例： ▪ 高または最重要 ▪ 中程度またはやや重大

フィールド	説明
	「低」または「やや重要」 - なしまたは重大ではない
サポートグループ	OT システムサービスのプライマリサポートグループの名前。
グループによる管理	OT システムサービスを管理するグループの名前。
運用ステータス	システムサービスのステータス。

d. **[Submit (送信)]** を選択します。

2. 産業用 ワークスペースリストビューで OT システムサービスを作成する場合は、次のアクションを実行します。

a. 移動先 **すべて > 産業用ワークスペース**。

b. **[リスト]**  アイコンを選択します。

c. オペレーショナルテクノロジー **(OT)** モジュールで、**[OT システム]** リストを選択します。

d. **[New (新規)]** を選択します。

e. フォームで次のフィールドに入力します。

OT システムサービスフォーム

フィールド	説明
表示名	OT システムサービスの表示名を入力するために使用されます。
名前	OT システムサービスのホスト名。
ISA エンティティサイト	OT システムサービスが属する ISA エンティティサイト。
メーカー	OT システムサービスのメーカーの名前。
モデル番号	OT システムサービスのメーカーのモデル番号。
簡単な説明	OT システムサービスの簡単な説明。
詳細	
所有者	OT システムサービスのプライマリ所有者の名前。
管理担当者	OT システムサービスのプライマリマネージャーの名前。
事業上の重要度	システムサービスの重要度または重要度の測定値。例： - 高または最重要 - 中程度またはやや重大 「低」または「やや重要」 - なしまたは重大ではない

フィールド	説明
サポートグループ	OT システムサービスのプライマリサポートグループの名前。
グループによる管理	OT システムサービスを管理するグループの名前。
運用ステータス	システムサービスのステータス。

f. **[Save (保存)]** を選択します。

次のタスク

これで、OT デバイスをシステムサービスに追加できるようになりました。詳細については、「[オペレーショナルテクノロジーシステムサービスへのデバイスの追加](#)」を参照してください。

オペレーショナルテクノロジーシステムサービスへのデバイスの追加

オペレーショナルテクノロジー (OT) デバイスを OT システムサービスに追加して、デバイスが属する機器モデルエンティティと OT システムサービスの間の関係を作成します。

始める前に

必要なロール：admin

手順

1. 移動先 **すべて > 産業用ワークスペース**.
2. **[リスト]**  アイコンを選択します。
3. オペレーショナルテクノロジー (**OT**) モジュールで、**[OT システム]** リストを選択します。
4. デバイスを追加する OT システムサービスを選択します。
5. **[関連レコード]** タブで、**[関連付けられた OT デバイス]** 関連レコードを選択します。
6. **[Add (追加)]** を選択します。
7. 1 つ以上の OT デバイスの横にあるチェックボックスをオンにします。
8. すべての OT デバイスを選択したら、**[追加]** を選択します。

結果

OT デバイスを追加すると、次の関係が作成されます。

- 選択した構成アイテム (CI) と OT システムサービス間の Depends on::Used by 関係
- OT システムサービスと CI の機器モデルエンティティ間の Managed by::Manages 関係。

機器モデルエンティティへの オペレーショナルテクノロジー システムサービスのマッピング

スケジュール済みジョブを有効にして、オペレーショナルテクノロジー (OT) システムサービスを ISA 機器モデルエンティティにマッピングします。OT デバイスと機器モデルエンティティの関係が変更されると、スケジュール済みジョブは OT システムサービスと機器モデルエンティティの関係を再計算します。

始める前に

必要なロール：admin

手順

1. 移動先 **すべて** > システム定義 > スケジュール済みジョブ.
2. [フィルターを表示/非表示] アイコン ()
3. 次のフィルターを追加します。
[名前][次の値に等しい][OT システムを ISA エンティティにマッピング]
4. [**OT システムを ISA エンティティにマッピング**] スケジュール済みジョブレコードを選択します。
5. [アクティブ] フィールドの横にあるチェックボックスをオンにします。
6. [実行] フィールドで、ニーズに最適なオプションを選択します。
7. [Update (更新)] を選択します。

オペレーショナルテクノロジーシステムサービスの依存関係マップの表示

オペレーショナルテクノロジー (OT) システムサービスの依存関係マップを表示して、選択した OT システムサービスの階層構造と、本番プロセス内の他のエンティティとの関係をグラフィカルに表示します。

このタスクについて

OT システムサービスの依存関係マップは、次の場所に表示できます。

- ServiceNow AI Platform OT システムのサービスレコードで
- 産業用ワークスペース OT システムのサービスレコードで

始める前に

必要なロール:cmdb_ot_editor

手順

1. ServiceNow AI Platform で OT システムサービスの依存関係マップを表示する場合は、次のアクションを実行します。
 - a. 移動先 **すべて** > オペレーショナルテクノロジー (**OT**) > **OT システム**.
 - b. OT 依存関係マップを表示する OT システムサービスレコードを選択します。
 - c. [**OT 依存関係マップを表示**] を選択します。
2. 産業用ワークスペースで OT システムサービスの依存関係マップを表示する場合は、次のアクションを実行します。
 - a. 移動先 **すべて** > 産業用ワークスペース.
 - b. [リスト]  アイコンを選択します。
 - c. オペレーショナルテクノロジー (**OT**) モジュールで、[**OT システム**] リストを選択します。
 - d. OT 依存関係マップを表示する OT システムサービスレコードを選択します。
 - e. [**OT 依存関係マップを表示**] を選択します。

IT レコードを **OT** デバイスに自動的に変換します

[IT を OT に再アサインするための一括更新ルールセット] 機能を使用して、IT ハードウェアをオペレーショナルテクノロジー (OT) デバイスに自動的に変換するスケジュール済みジョブを作成します。このスケジュール済みジョブは、変換するすべての IT ハードウェアに OT エンティティの詳細を一度に追加します。

始める前に
必要なロール：admin

このタスクについて

OT エンティティレコードを作成する対象の IT ハードウェアとして分類されている構成アイテム (CI) がある場合があります。次の一般的なガイドラインに従ってください。

- 使用するフィールドが、ステップ 3 ～ 4 のフィルター基準条件に適用されていることを確認してください。パフォーマンス関連の問題を回避するために、データセットが 100 万レコードを超えていないことを確認します。
- ステップ 3 ～ 6 で、個別の CI クラスに対して個別のスケジュール済みジョブ定義を作成します。これにより、各 CI レベルをフィルタリングし、OT エンティティのデフォルト値を定義できます。
- ステップ 3 でフィルターの [クラス] フィールドを使用して、特定の CI クラスのみをクエリします。

i 注： ソーステーブルでは、ハードウェアクラスとその拡張クラスのみが使用されます。

- [プレビュー] ボタンを使用して、ステップ 4 でさらにレビューするために選択したレコードを検証します。
- ステップ 5 の **[OT エンティティのデフォルト構成]** タブでデータを確認します。OT エンティティレコードは、これらのデフォルト値を使用して作成されます。

IT ハードウェアを OT デバイスに手動で変換することもできます。詳細については、「[一括編集で IT ハードウェアを OT デバイスに変換する](#)」を参照してください。

手順

1. 移動先 **すべて > 産業用ワークスペースアドミン > OT マネージャーアドミン > 自動化された IT OT** への一括変換。
2. **[New (新規)]** を選択します。
3. **[フィルター基準 - OT デバイス]** タブで、変換する必要がある CI を識別するためのソーステーブルとフィルター基準を設定します。

たとえば、プリフィックスが COMP の、システムにインポートされるすべてのコンピューターについて OT エンティティの詳細を追加する場合は、ソーステーブルで **cmdb_ci_computer** を選択し、フィルター基準として [名前] [で始まる] [COMP]、[クラス] [次の値に等しい] [コンピューター]、および **[OT デバイスの詳細]** [空] を追加しま

す。

CMDBグループを使用して、インストールされているソフトウェアなどの追加情報に基づいて IT CI をグループ化し、OT デバイスに変換できるようにすることもできます。詳細については、「[CMDBグループを使用して OT コンテキストを IT CI に追加する](#)」を参照してください。

4. [プレビュー] ボタンを選択して、設定したフィルター条件から選択されたレコードの数を確認します。

OT エンティティの詳細 (OT デバイスタイプやデバイスの重要度など) がこれらのレコードに追加されます。

5. [OT エンティティのデフォルト構成] タブで、フィールドに入力します。

次の表のフィールドは、OT エンティティレコードまたは OT 関連のメタデータに追加されるデフォルト値を示しています。

[OT エンティティのデフォルト構成] フォーム

フィールド	説明
OT デバイスタイプ	OT デバイスが分類されるカテゴリタイプ。デバイスタイプは、デバイスが OT ネットワーク上で果たす機能でもあります。たとえば、サーバーなどの IT デバイスを OT デバイスに変換でき、ネットワーク上で果たす機能は HMI です。そのクラスは server で、デバイスタイプは HMI です。 ❗ 注: 場合によっては、OT デバイスに OT 機能がないか、デバイスタイプが不明です。OT デバイスに OT 機能がない場合は、[OT 機能なし] を選択します。OT デバイスのデバイスタイプが不明な場合は、[不明] を選択します。
デバイスの重要度	デバイスに障害が発生した場合のサイトプロセスに対する相対的なリスクの測定: ○ 1 : 最重要 ○ 4 : 重要ではない
Purdue レベル	割り当てられた Purdue レベル。レベル範囲は 0 ~ 5 です。 ❗ 注: 産業用制御システムの Purdue レベルの詳細については、「 https://subscription.packtpub.com/book/networking_and_servers/9781788395151/1/ch01lvl1sec10/the-purdue-model-for-industrial-control-systems 」を参照してください。
ゾーン	デバイスが割り当てられているサイトの場所内のエリア。
サイト	デバイスが配置またはアサインされているトップレベルの親エンティティ、または工業用サイト。

6. [実行] フィールドで、このジョブを実行するスケジュール時刻を選択します。

7. [アクティブ] フィールドの横にあるチェックボックスをオンにします。

8. [Submit (送信)] を選択します。

CMDBグループを使用して OT コンテキストを IT CI に追加する

構成管理データベース (CMDB) グループを使用して、インストールされているソフトウェアなどの追加情報に基づいて IT 構成アイテム (CI) をグループ化します。次に、オペレーショナルテクノロジー (OT) コンテキストを IT CI に追加できます。

始める前に

必要なロール：admin

このタスクについて

CMDBグループを使用しても、IT CI のクラスは変更されません。代わりに、OT コンテキストをキャプチャする IT CI に OT エンティティレコードを追加します。

注:

次の一般的なガイドラインに従ってください。

1. CMDB グループのフィルター条件が毎回一意の CI レコードのセットを返すようにします。たとえば、「**OT** デバイスの詳細が空である」などのフィルター条件を追加すると、OT デバイスの詳細がないレコードのみが考慮されるようになります。
2. インデックス付きフィールドがフィルター基準条件の一部として使用されていることを確認してください。パフォーマンス関連の問題を回避するために、データセットが 10,000 レコードを超えないようにしてください。

 注: CMDB グループ API は、10,000 件、または次のプロパティで定義された制限を超えるレコードの取得をサポートしていません。

- glide.cmdb.query.max_results_limit

- glide.cmdb.group.max_ci_limit

これに対処するには、CMDB クエリに現在の制限よりも多くのレコードが含まれている場合に、より大きなクエリ結果が得られるようにこれらのプロパティを調整する必要があります。

3. CMDB ごとに自動化された IT から OT への一括変換 (sn_automated_it_ot_bulk_conversion) レコードを作成して、グループレベルでフィルタリングを行い、それぞれの OT エンティティのデフォルト値を定義してください。
4. **[OT エンティティのデフォルト構成]** タブでデータを検証します。OT エンティティレコードは、これらのデフォルト値を使用して作成されます。

手順

1. 適切な IT CI を識別するために必要なフィルター基準を持つ CMDB グループを定義します。詳細については、「[CMDB グループ](#)」を参照してください。
2. CMDBグループに関連付けられた自動化された IT から OT への一括変換 (sn_automated_it_ot_bulk_conversion) レコードを作成します。このレコードを作成すると、OT エンティティの詳細を介して IT CI に OT コンテキストが追加されます。

自動化された IT から OT への一括変換レコードを作成する方法の詳細については、「[IT レコードを OT デバイスに自動的に変換します](#)」を参照してください。

3. **sn_automated_it_ot_bulk_conversion_m2m_cmdb_group** でレコードを作成するには、次のアクションを完了します。

- a. 移動先 **すべて > 産業用ワークスペースアドミン > OT マネージャーアドミン > 自動化された IT OT** への一括変換：**CMDB グループ**の使用。
- b. **[New (新規)]** を選択します。
- c. **[自動化された IT から OT への一括変換]** フィールドで、ステップ 2 で作成したレコードを選択します。
- d. **[CMDB グループ]** フィールドで、ステップ 1 で作成した CMDB を選択します。
- e. **[Submit (送信)]** を選択します。
レコードは、CMDB グループを自動化された IT から OT への一括変換レコードに関連付けます。

たとえば、特定の HISTORIAN ソフトウェアがインストールされているすべてのコンピューターの OT エンティティの詳細を追加する場合は、このフィルター基準に一致する CMDB グループを作成する必要があります。次に、スケジュール済みジョブを作成し、それを HISTORIAN ソフトウェアがインストールされているコンピューターの CMDB グループにリンクします。

オペレーショナルテクノロジーマネージャーの参照

参照トピックには、オペレーショナルテクノロジーマネージャー アプリケーションに関する追加情報が記載されています。

オペレーショナルテクノロジーマネージャーとともにインストールされるコンポーネント

ユーザーロールなど、オペレーショナルテクノロジーマネージャー アプリケーションをアクティブ化すると、いくつかのタイプのコンポーネントをインストールできます。

- i** 注：アプリケーションファイルテーブルには、このアプリケーションとともにインストールされたコンポーネントがリストされています。このテーブルへのアクセス手順については、「[アプリケーションとともにインストールされているコンポーネントの検索](#)」を参照してください。

インストール済みプラグイン

プラグイン	説明
産業用コア	OT サービスグラフコネクタに必要なクラスマッピングが含まれています。 Industrial Core プラグインの詳細については、「 Industrial Core プラグイン 」を参照してください。

インストールされているロール

ロール	説明
オペレーショナルテクノロジー ディスカバリー アドミニストレーター [ot_discovery_admin]	オペレーショナルテクノロジープロセスのディスカバリーを実行できますが、構成管理データベース (CMDB) にアクセスして、検出されたアイテムから作成された構成アイテム (CI) および関連 オペレーショナルテクノロジー (OT) エンティティを表示することはできません。詳細

ロール	説明
	については、「 オペレーショナルテクノロジー ディスカバリー スケジュールを作成し、ディスカバリー プロセスを実行します 」を参照してください。
オペレーショナルテクノロジー マネージャー ビューアー [cmdb_ot_viewer]	オペレーショナルテクノロジー (OT) デバイス レコードへの読み取り専用アクセス。
オペレーショナルテクノロジー マネージャー エディター [cmdb_ot_editor]	運用テクノロジー (OT) 拡張クラス の作成、読み取り、更新、および削除アクセス権。 i 注: cmdb_ot_editor ロールを割り当てられたユーザーは、OT 構成アイテム (CI) のみを編集および削除でき、IT CI を編集することはできません。
オペレーショナルテクノロジー マネージャー アドミン [cmdb_ot_admin]	オペレーショナルテクノロジー (OT) デバイス レコードの作成、読み取り、更新、および削除アクセス権。OT エンティティタイプ内の特定の構成を編集および管理することもできます。詳細については、「運用テクノロジー (OT) 拡張クラス」を参照してください。 i 注: cmdb_ot_editor ロールを割り当てられたユーザーは、OT 構成アイテム (CI) のみを編集および削除でき、IT CI を編集することはできません。

のインストール済みソフトウェア オペレーショナルテクノロジー管理

オペレーショナルテクノロジー管理 ソリューションのインストール済みソフトウェアは、オペレーショナルテクノロジー (OT) ネットワークの IT ディスカバリー、またはインストール済みソフトウェアをサポートする OT 認定 サービスグラフコネクタ から提供されます。

インストール済みソフトウェアの概要

CI にインストールされるソフトウェアは、ソフトウェア資産管理 (SAM) アプリケーションがインストールされているかどうかによって異なります。SAM が有効になると、次のテーブルが作成されます。

- Software Discovery モデル [cmdb_sam_sw_discovery_model]
- ソフトウェア モデル [cmdb_software_product_model]
- ソフトウェアインストール [cmdb_sam_sw_install]

SAM が有効になったときにソフトウェアインストールを管理するためのテーブル構造がどのように異なるかの詳細については、「[ソフトウェア資産管理による検出](#)」を参照してください。

ソフトウェア資産管理データを表示するようにコンピューターの CI を設定することもできます。詳細については、「[ソフトウェア資産管理データを表示するための CI の構成](#)」を参照してください。

OT デバイスのインストール済みソフトウェアの表示

OT デバイスのインストール済みソフトウェアは、産業用 ワークスペース 次の場所で確認できます。

- **[OT デバイスにインストールされているソフトウェア]** リストに移動します **すべて > オペレーショナルテクノロジー (OT) > OT デバイスにインストールされているソフトウェア**。
- **オペレーショナルテクノロジー (OT) モジュールの下の 産業用 ワークスペース リストビューの [OT デバイスにインストールされているソフトウェア]** リスト。
- OT デバイスレコードの **[関連レコード]** タブにある **[インストールされているソフトウェア]** リスト。

Industrial Core プラグイン

Industrial Core プラグインには、オペレーショナルテクノロジー (OT) 認定 サービスグラフコネクタに必要なクラスマッピングが含まれています。

Industrial Core プラグインの概要

Industrial Core プラグイン [sn_ot_core] は、OT 固有のデータモデルと OT のサイトベースのライセンス要件をサポートするための基本機能を導入します。プラグインは、オペレーショナルテクノロジー管理 ソリューション内のすべての製品が依存関係として必要です。依存関係は、直接の依存関係にすることも、基本製品を介した依存関係にすることもできます。たとえば、オペレーショナルテクノロジーマネージャー アプリケーションは依存関係です。オペレーショナルテクノロジー脆弱性対応 アプリケーションの場合、Industrial Core プラグインは Industrial Core の直接の依存関係であるためオペレーショナルテクノロジーマネージャー依存関係として追加オペレーショナルテクノロジー脆弱性対応。

- i 注:** OT 機能と統合するすべてのパートナーアプリケーションは、Industrial Core プラグインへの依存関係を宣言する必要があります。これにより、ライセンスと将来のモデル拡張の一貫した処理が保証されます。

Industrial Core プラグインの機能

次の表は、Industrial Core プラグインの機能をまとめたものです。

プラグイン機能

機能	説明
OT クラスマッピングテンプレート [ot_class_mapping_template]	Industrial Core プラグインでは、OT サービスグラフコネクタのユーザーがアクセスできるテーブル部分を使用してクラスマッピングを管理するための構成テンプレートが導入されています。この構成テンプレートは、以前のスクリプトベースのアプローチに代わるものです。 OT クラスマッピングテンプレートは現在オプションですが、UI で直接クラスマッピングを表示、管理、および上書きでき、透明性と柔軟性が向上するため、この方法を採用することをお勧めします。 i 注: パートナーは、アプリケーションのスコープ内で OT クラスマッピングテンプレートテーブルを拡張して、統合に固有のクラスマッピングをキャプチャできます。 OT クラスマッピングテンプレートの詳細については、「オペレーショナルテクノロジー (OT) 拡張クラス」を参照してください。

プラグイン機能 (続く)

機能	説明
	Microsoft Excel のサービスグラフコネクタのクラスマッピングを確認する方法の詳細については、「 クラスマッピングの確認 」を参照してください。
OT デバイスのネットワーク接続 [sn_ot_device_network_connection]	OT デバイスネットワーク接続 [sn_ot_device_network_connection] テーブルは CI 関係 [cmdb_rel_ci] テーブルを参照し、OT デバイスの CI 関係におけるデバイス間接続を識別します。 i 注: このデータには利用可能な OT 統合が入力され、手動で作成することはできません。 OT デバイスネットワーク接続データモデルの詳細については、「オペレーショナルテクノロジー (OT) 拡張クラス」を参照してください。
OT アクティビティ [sn_ot_activity]	OT デバイスで発生する次のアクティビティをキャプチャします。 - 構成アイテムの追加、更新、または廃止 - IP アドレスの追加
OT バックアップジョブの実行履歴 [ot_backup_history_and_comparison_log]	バックアップジョブ実行履歴クラスは、すべてのバックアップ実行のレコード履歴を作成します。
OT 自動化リポジトリ [ot_automation_repo]	OT バックアップジョブ実行履歴クラスは、すべてのバックアップ実行のレコード履歴を比較します。
OT 自動化リポジトリデバイス M2M [ot_automation_repo_device_m2m]	OT 自動化リポジトリクラスは、OT エンティティで実行するすべての構成変更を保存するリポジトリとして機能します。
OT 自動化コミット [ot_automation_commit]	OT 自動化リポジトリデバイス M2M クラスは、OT 自動化リポジトリと OT エンティティテーブルへの参照として機能します。

カスタマイズされたデバイスの命名戦略

カスタムデバイス命名機能を使用すると、特定のクラスのデバイスに対してパーソナライズされた命名戦略を定義できます。デバイス名は、実装する戦略に基づいてインポート中に割り当てられます。

のモデルカテゴリ オペレーショナルテクノロジー

CMDBで構成アイテム (CI) が作成されると、資産レコードが作成されます。資産レコードには、CI のモデル カテゴリが含まれています。

次の表に、オペレーショナルテクノロジー (OT) で利用可能なモデルカテゴリとその CI クラスを示します。

OT モデルカテゴリ

名前	CI クラス
産業	該当なし
産業全般	オペレーショナルテクノロジー (OT) [cmdb_ci_ot]
運用機器	運用機器 [cmdb_ci_oe]
OT コントロール	OT コントロールシステム [cmdb_ci_ot_control]
OT コントロール 3D プリンター	産業用 3D プリンター [cmdb_ci_ot_insustrial_3d_printer]
OT コントロール CNC	CNC [cmdb_ci_ot_cnc]
OT コントロール DCS	DCS [cmdb_ci_ot_dcs]
OT コントロール DPU	DPU [cmdb_ci_ot_dpu]
OT コントロール IED	IED [cmdb_ci_ot_ied]
OT コントロールモジュール	OT コントロールモジュール [cmdb_ci_ot_control_module]
OT コントロール PLC	PLC [cmdb_ci_ot_plc]
OT コントロール RTU	RTU [cmdb_ci_ot_rtu]
OT コントロール SCADA	SCADA サーバー [cmdb_ci_ot_scada_server]
OT コントロールサーバー	OPC サーバー [cmdb_ci_ot_opc_server]
OT フィールドアクチュエーター	産業用アクチュエーター [cmdb_ci_ot_industrial_actuator]
OT フィールドデバイス	OT フィールドデバイス [cmdb_ci_ot_field_device]
OT フィールドドライブ	産業用ドライブ [cmdb_ci_ot_industrial_drive]
OT フィールドロボット	産業用ロボット [cmdb_ci_ot_industrial_robot]
OT フィールドセンサー	産業用センサー [cmdb_ci_ot_industrial_sensor]
OT 監督	OT 監督システム [cmdb_ci_ot_overusery]
OT 監督 EWS	EWS [cmdb_ci_ot_ews]
OT 監督履歴担当者	履歴担当者 [cmdb_ci_ot_historian]
OT 監督 HMI	HMI [cmdb_ci_ot_hmi]
OT 監督 OPC	OPC クライアント [cmdb_ci_ot_opc_client]
OT 監督 SCADA	cmdb_ci_ot_scada_client

IT から OT へ、および OT から IT への変換のための API

OT 資産管理 アプリケーションで IT を IT から オペレーショナルテクノロジー (OT) に変換するためのリフレッシュワークフローシナリオを処理するために使用される API は 2 つあります。

で使用される **API OT 資産管理**

OT 資産管理 では、資産と OT 資産の構成アイテム (CI) 間の同期を維持する必要があります。次の API は、OT 資産管理 アプリケーションでの IT から OT への変換と OT から IT への変換に使用されます。

i 注: IT CI クラスは変更されません。代わりに、OT デバイスコンテキストを提供する OT エンティティレコードが追加されます。

- IT を OT 資産 API に変換
- OT を IT 資産 API に変換

IT を **OT 資産 API** に変換

OT 資産への変換 API は、OT 構成アイテム (CI) が新しい CI に置き換えられるリフレッシュワークフローで使用されます。この API は、以前の OT エンティティレコードのレプリカを作成し、それらを新しい CI にマッピングします。以前の CI とその関連 OT エンティティレコードに変更は加えられていません。この API では、新しい CI と以前の CI 参照の両方が使用されます。

OT を **IT 資産 API** に変換

OT を IT 資産に変換 API は、資産を交換する必要がある場合に使用されます。API は、渡された CI の OT エンティティレコードを削除します。

オペレーショナルテクノロジー (OT) 資産の資産と構成アイテム (CI) の同期の詳細については、「[オペレーショナルテクノロジー \(OT\) 資産の資産と構成アイテム \(CI\) の同期](#)」を参照してください。

OT 資産管理 の詳細については、「[OT 資産管理](#)」を参照してください。

オペレーショナルテクノロジー バックアップ管理データモデル

オペレーショナルテクノロジー (OT) バックアップ管理は、OT デバイスのバックアップに関する可視化と実用的なインサイトを提供します。以下で説明するクラス・テーブルは相互に関連しており、まとめてバックアップ管理データ・モデルを形成します。

バックアップ ストレージ情報 [cmdb_backup_storage_information] クラスを使用して、内部または外部のバックアップサービスでデバイスを識別するバックアップレコードを作成します。バックアップストレージ情報テーブルには、以下の属性が含まれています。

属性	説明
バックアップ構成ステータス	CI が関連するポリシーと一緒にバックアップサービスまたはアプライアンスに構成されているかどうかを示します。
ディスカバリソース	バックアップレコードのディスカバリソース。
バックアップサービス	外部および内部バックアップシステム、サービス、またはアプライアンスをホストしている共通サービスデータモデル (CSDM)テクニカルサービスへの参照
管理担当者	バックアップの管理を担当するユーザーの名前または ID。

属性	説明
最新の正常実行	デバイスに対して正常に実行された最新のデータバックアップの日時。
最新の実行試行	デバイスに対して試行された最新のデータバックアップの日時。
次の実行試行	デバイスに対して次のデータバックアップが試行される日時。
最新の実行ログ	実行されたすべてのデバイスデータバックアップの詳細なログエントリ。
バックアップソース ID	外部または内部のバックアップサービスでデバイスを識別する、デバイスのバックアップサービスレコード。バックアップソース ID には、host_id、vcenter_id、instance_id、db_id を含めることができます。
ジョブ定義 ID	データバックアップジョブに割り当てられた識別番号。
目標復旧ポイント	バックアップ間で経過可能な時間と、失われる可能性のあるデータの量
実行モード	バックアップが定期的に自動的に実行されるように構成されているか、必要に応じて手動で実行されるように構成されているかを示します。
バックアップソース	バックアップされた CI の詳細。このテーブルには、参照される CI のバックアップステータスの詳細が保持されます。
ジョブ定義名	データバックアップジョブに割り当てられた名前。
グループによる管理	バックアップの管理を担当するユーザーグループの名前。
ドメイン	インスタンスが属するドメインの ID

バックアップジョブ実行履歴 [cmdb_backup_job_execution_history] クラスを使用して、すべてのバックアップ実行のレコード履歴を作成します。バックアップジョブの実行履歴テーブルには、次の属性が含まれています。

属性	説明
バックアップジョブ情報	作成したバックアップジョブの詳細。
バックアップ終了時間	バックアップジョブが終了した時刻。
完了ステータス	バックアップジョブの現在の完了ステータス。
アーカイブ用にマーク	バックアップジョブの実行履歴を 90 日後にアーカイブする場合に選択します。

OT バックアップジョブ実行履歴 [ot_backup_history_and_comparison_log] クラスを使用して、すべてのバックアップ実行のレコード履歴を比較します。バックアップログテーブルには、次の属性が含まれています。

属性	説明
現行バージョン	OT デバイスの現在のバージョン。

属性	説明
現在のバージョンとバックアップ	OT デバイスの現在のバージョンとバックアップレコードで利用可能なバージョン情報の比較。
現在のバージョンとバックアップエラー	OT デバイスの現在のバージョンと、バックアップジョブの実行中にエラーが発生したバックアップレコードで利用可能なバージョン情報との比較。
現在のバージョンとバックアップの警告	OT デバイスの現在のバージョンと、バックアップジョブの実行中に警告が発生したバックアップレコードで利用可能なバージョン情報との比較。
以前のバージョンとバックアップ	以前に記録されたバージョンの OT デバイスと、バックアップレコードで利用可能なバージョン情報の比較。
以前のバージョンとバックアップエラー	以前に記録されたバージョンの OT デバイスと、バックアップジョブの実行中にエラーが発生したバックアップレコードで利用可能なバージョン情報との比較。
以前のバージョンとバックアップの警告	以前に記録されたバージョンの OT デバイスと、バックアップジョブの実行中に警告が発生したバックアップレコードで利用可能なバージョン情報との比較。

関連トピック

[オペレーショナルテクノロジー \(OT\) 拡張クラス](#)

オペレーショナルテクノロジー バックアップ管理のバージョン管理データモデル

オペレーショナルテクノロジー (OT) バックアップ管理では、複数のスクリプトまたはプログラムを開発して、OT デバイスのデータバックアッププロセスを自動化できます。バージョン管理データモデルを使用すると、OT エンティティ用に開発したすべてのバックアップスクリプトまたはプログラムのレコードを保持できます。

次のクラステーブルは相互接続されており、まとめて オペレーショナルテクノロジー (OT) バックアップ管理データモデルのバージョン管理データモデルを形成します。

OT 自動化リポジトリ (ot_automation_repo) クラスをリポジトリとして使用して、OT エンティティで実行するすべての構成変更を保存します。このクラスでは、次の属性を使用できます。

属性	説明
プロジェクトの最終更新日	プロジェクトに対する最新の変更の日時。
コメント	OT エンジニアから提供された追加情報。
複数の編集が有効か	プロジェクトに対して複数の編集を有効にするには、[はい] または [いいえ] を選択します。
現在のステータスからの日数	プロジェクトが現在のステータスになってから経過した日数。
最新バージョン	プロジェクトがアサインされている OT デバイスの現在のバージョン。
プロジェクトの進捗状況	プロジェクトのステータス。

OT 自動化リポジトリおよび OT エンティティテーブルへの参照として、OT 自動化リポジトリデバイス M2M (ot_automation_repo_device_m2m) クラスを使用します。このクラスでは、次の属性を使用できます。

属性	説明
自動化リポジトリ	すべてのプロジェクトの変更と構成が保存されるリポジトリ。
OT エンティティ	プロジェクトがアサインされている OT エンティティ。

プロジェクトにコミットした変更への参照として、OT AutomationCommit (ot_automation_commit) クラスを使用します。このクラスでは、次の属性を使用できます。

属性	説明
自動化バージョン	OT エンティティに対してコミットされたスクリプトまたはプログラムのバージョン。

関連トピック

[オペレーショナルテクノロジー バックアップ管理データモデル](#)

関連情報

ネットワーク侵入検知システム (NIDS) 拡張クラス、OT 拡張クラス、および関連アプリケーションの詳細を確認してください。

拡張クラスの概要

拡張クラスは、オペレーショナルテクノロジー管理 が 構成管理データベース (CMDB)でどのように機能するかを理解するのに役立ちます。

ネットワーク侵入検知システム (NIDS) CI 拡張クラス

ネットワーク侵入検知システム (NIDS) [cmdb_ci_nids] クラスは、パッシブネットワークモニタリングアプライアンスと、それが検出するネットワーク上のデバイスとの間の関係をビルドします。

オペレーショナルテクノロジー (OT) 拡張クラス

構成管理データベース (CMDB) は OT のクラスを更新します。

関連アプリケーション

CMDB CI クラスモデル

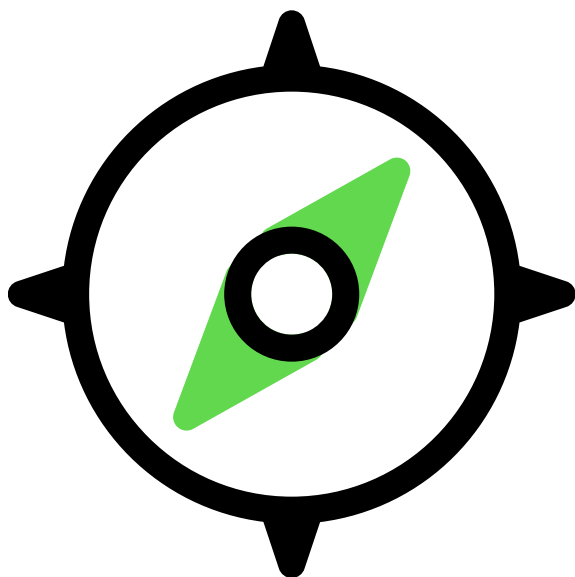
CMDB CI Class Models ストアアプリは、クラスの説明、識別ルール、識別子エントリ、および依存関係を含む、CMDB クラス階層を拡張するクラスモデルを追加します。

製造業プロセスマネージャー

製造業プロセスマネージャー アプリケーションを使用して、ServiceNow オペレーショナルテクノロジー ソリューションに必要な ISA-95 機器モデルのデータ基盤を作成します。製造業プロセスマネージャーを使用すると、各サイトで独自のバージョンの機器モデルを作成できます。

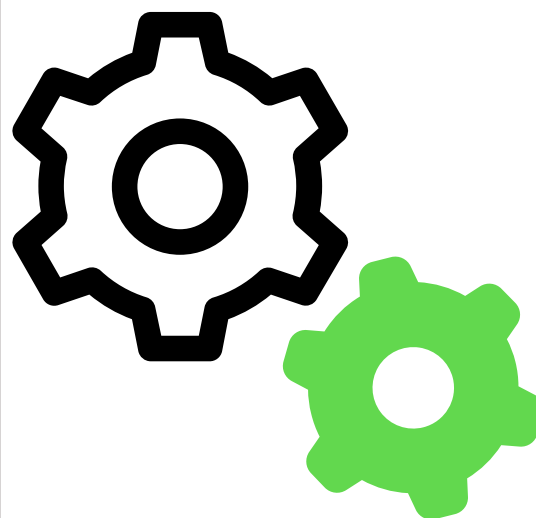
i 注: 製造プロセスマネージャーは、Vancouver の産業用プロセスマネージャーに名前が変更されました。バージョン 1.0.9 以前を使用している場合でも、アプリケーションは Manufacturing Process Manager と呼ばれます。バージョン 2.0 を使用している場合、このアプリケーションは産業用プロセスマネージャーと呼ばれます。

探索



メーカーがどのように使用するかを学ぶ 製造業プロセスマネージャー

構成



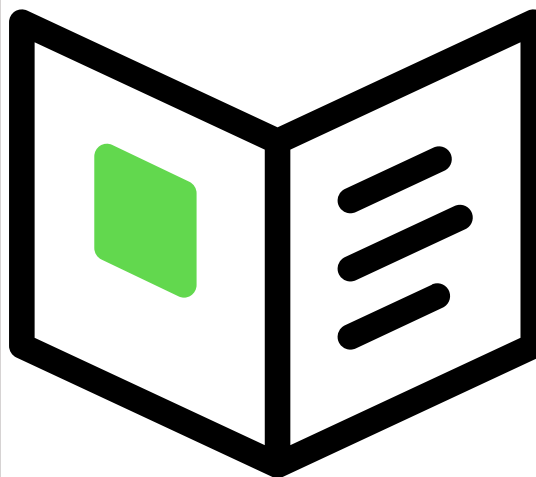
実装の計画と構成

使用方法



オペレーショナルテクノロジーデバイス
および機器モデルエンティティのレビュー

参照



関連情報とアプリケーションの詳細を取得

製造業プロセスマネージャーの探索

製造業プロセスマネージャーで使用する一般的な用語、略語、および ISA-95 機器モデルの業界標準の詳細について説明します。

製造業プロセスマネージャーの概要

製造業プロセスマネージャー アプリケーションの概要をご覧ください。

https://player.vimeo.com/video/1044353688?h=eba3593d47&badge=0&autopause=0&player_id=0&app_id=58479

製造業プロセスマネージャー 一般的な用語

製造業プロセスマネージャーを開始する前に、このコンテンツで使用される一般的な用語と頭字語を見てみましょう。

一般的な用語と頭字語

期間	頭字語	定義
オペレーショナルテクノロジー	OT	物理プロセスを制御するために産業オートメーションに使用されるテクノロジー。 ❗ 注: オペレーショナルテクノロジーはモノのインターネット(IoT)ではありません。
International Society of Automation (国際自動制御学会)	ISA	ISA-95 機器モデルを含む、工業企業の標準を発行する組織。
抽出、変換、ロード	ETL	ソースシステムからデータを取得して変換し、ターゲットシステムにアップロードするために使用される一般的な用語。

ISA-95 機器モデル

ISA-95 設備モデルは、産業施設と其中的の生産設備を表す業界標準です。さまざまなレベルとレベルタイプを持つ機器モデルテンプレートを定義することで、施設内の機器モデルエンティティを記述できます。

このテンプレートを使用すると、次のアクションを実行できます。

- 機器モデルエンティティをマッピングします。このマップを使用して、階層構造を作成します。
- 産業用のさまざまなサイトに合わせて複数の機器モデルを作成します。
- 各サイトにユーザーを割り当て、特定のサイトの機器モデル情報へのアクセス権を管理できるようにします。たとえば、アトランタのユーザーがアトランタのサイト情報にのみアクセスでき、ミシガン州のサイトのデータにはアクセスできないように指定できます。詳細については、「[アドミニストレーター以外の機器モデルサイトアクセスの割り当てまたは削除](#)」を参照してください。

設備モデルはサイトレベルから始まり、各工業用地を記述する詳細な階層構造が含まれています。機器モデルテンプレートを適用して、このデータを階層的に構造化します。

次の図は、製造業プロセスマネージャーのインストール時に提供される標準の ISA-95 デフォルトテンプレートの例です。この図は、アトランタにある自動車製造施設を表しています。

- サイトの下の下位レベルは、ドアアセンブリエリア、独自の従属作業センター、および作業単位を表します。

作業セルは、製造施設内の指定された領域であり、リソースのグループが戦略的に配置され、連携して特定のタスクまたはプロセスを効率的に完了します。ワークセンターには、人、機械、および設備が含まれます。

- 作業区レベルと作業単位レベルには、それぞれレベルタイプがあります。このモデルでは、ワークセンターレベルに 4 つの異なるレベルタイプがあります。
 - プロセスセル: プロセスセルは、生産の特定の段階に特化した製造施設内の特定の領域です。これには、プログラマブル論理コントローラー (PLC)、センサー、アクチュエーターなど、プロセスを自動化および監視するために必要なすべての機器が含まれています。プロセスセルデータは、制御、品質監視、および診断のために収集されます。

たとえば、自動車工場のロボット溶接セルなどです。

- 生産単位: 生産単位は、関連する製造操作を実行するために連携するプロセスセルのグループです。生産単位では、プロセスセルの活動を調整し、材料とデータフローを管理し、プロセスを最適化し、品質を維持することができます。

たとえば、自動車製造工場では、生産ユニットに溶接、塗装、組み立て、およびパッケージング用のセルが含まれる場合があります。

- 生産ライン: 生産ラインは、製品を最初から最後まで製造する一連のプロセスセルまたは生産ユニットです。生産ラインは、全体的な制御と監視を提供し、すべてのセルとユニットの活動を調整し、原材料から完成品までのプロセス全体を管理します。

たとえば、部品が完全な車両に組み立てられる自動車組立ラインなどです。

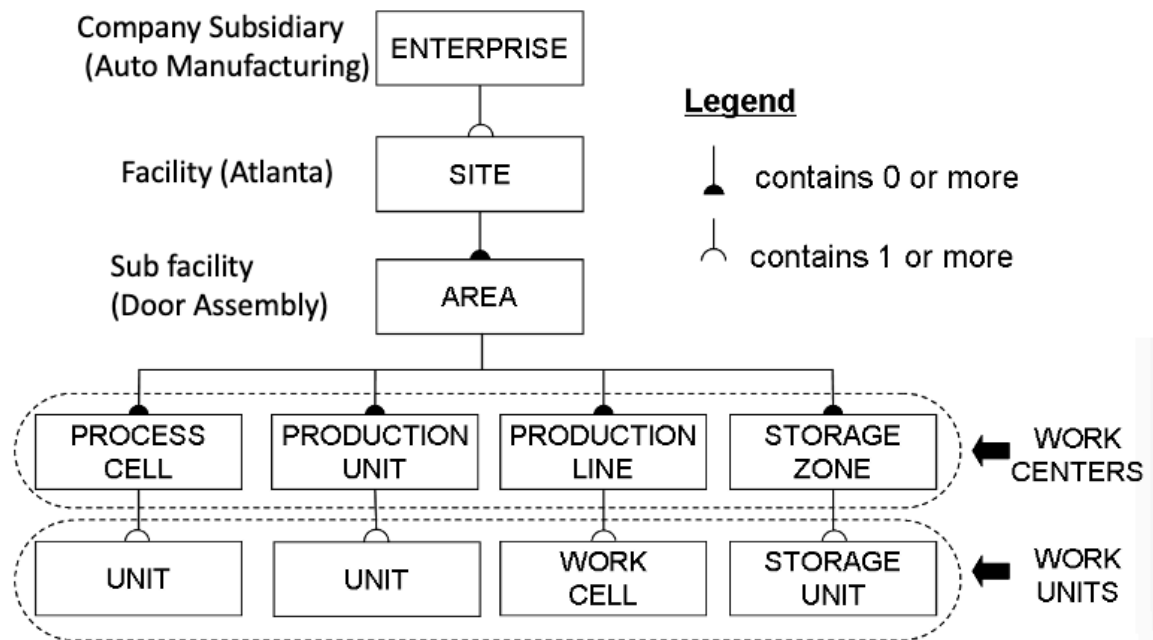
- ストレージゾーン: ストレージゾーンは、原材料、仕掛品、または完成品を保管するための指定されたエリアです。保管ゾーンには、効率的な材料の流れと可用性を維持するための在庫管理システムが必要です。

たとえば、生産前の原材料や出荷を待っている完成品を保管するための倉庫などです。

- ストレージユニット: 工業用地のストレージユニットとは、特定の機器、材料、または製品を保管するために使用される指定されたスペースまたは構造を指します。

たとえば、自動車製造工場では、自動車の塗装、電気付属品、および生の鋼を保管するための指定された保管ユニットがあります。

機器モデルテンプレートの例



機器モデルテンプレート

機器モデルテンプレートを作成して、機器モデルを特徴付けたり、類似のタイプの機器モデルエンティティをグループ化して物理的な産業施設を記述するデータを構造化したりできます。

機器モデルテンプレートは、次のコンポーネントで構成されています。

機器モデルテンプレート

機器モデルテンプレートの名前と説明。

機器モデルテンプレートの階層レベル

機器モデルデータのソートと構造化に使用される、割り当てられた階層レベル。

機器モデルテンプレートの階層レベルのタイプ

階層レベル内のさまざまなタイプのエリア、機能、または生産プロセスを表すタイプ。

機器テンプレートの詳細とその構造のグラフィック例については、「[ISA-95 機器モデル](#)」と「[機器モデルテンプレートの定義](#)」を参照してください。

製造業プロセスマネージャーの構成

ServiceNow オペレーショナルテクノロジー ソリューションに必要な機器モデルデータ基盤を作成できるように、製造業プロセスマネージャー アプリケーションを構成します。

注:

admin ロールを持っている場合は、産業用 ガイド付きセットアップを使用して、製造業プロセスマネージャー アプリケーションのセットアップ手順を実行できます。

ガイド付きセットアップにアクセスするには、次に移動します: 産業用ワークスペースアドミン > ガイド付きセットアップ。

タスク	目的
1. ServiceNow Storeから製造業プロセスマネージャーをインストールします。	製造業プロセスマネージャー アプリケーションとサポートプラグインをインストールします。
2. 製造業プロセスマネージャー ロールを割り当てます。	ロールを割り当てて、各ユーザーが使用できるアクションをコントロールします。
3. サービスグラフ コネクタインポート用の Microsoft Excel スプレッドシートに入力します。	ServiceNow AI Platform にアップロードするために、Microsoft Excel スプレッドシートを作成し、既存の ISA-95 設備階層モデルデータを入力します。
4. Excel スプレッドシートをインポートします。	既存の ISA-95 設備階層モデルデータを 構成管理データベース (CMDB)にアップロードします。
5. ServiceNow パートナーが提供するサービスグラフ [service-graph] コネクタをインストールし、統合を使用して機器モデルデータをインポートします。	パートナーが提供する ServiceNow コネクタが ServiceNow Storeで利用可能になったときにインストールし、機器モデルデータをインポートします。
6. 管理者以外のロールを持つユーザーに機器モデルサイトのアクセス権を付与します。	cmdb_ot_isa_viewer または cmdb_ot_isa_editor ロールが割り当てられたユーザーのサイトアクセス権をアサインまたは削除します。
オプション: OT デバイスのマッピングの自動化	OT デバイスから本番プロセスへのマッピングを自動化します。 i 注: マッピング機能を有効にするには、次のプラグインが必要です。 - オペレーショナルテクノロジーマネージャー - 製造業プロセスマネージャー

製造業プロセスマネージャー をインストールする

必要なエンタイトルメントとアドミニストレーター [admin] ロールがある場合は、製造業プロセスマネージャー アプリケーションと関連するプラグインをインストールできます。

始める前に

- アプリケーションとその関連するすべての ServiceNow Store アプリケーションに有効な ServiceNow エンタイトルメントがあることを確認してください。詳細については、次を参照してください。 [のエンタイトルメントを取得する ServiceNow 製品またはアプリケーション](#)。

必要なロール: admin

このタスクについて

次のアイテムが 製造業プロセスマネージャー とともにインストールされます。

- プラグイン
- ガイド付きセットアップを含むアプリケーションメニュー
- ロール
- テーブル

製造業プロセスマネージャー アプリケーションとともにインストールされているコンポーネントの表示の詳細については、「[製造業プロセスマネージャーとともにインストールされるコンポーネント](#)」を参照してください。

- i 注:** オペレーショナルテクノロジー ヴィジビリティのライセンスを持たないOperational Technology Service Managementユーザーの場合は、次の点に注意してください。
- 最新バージョンの オペレーショナルテクノロジーインシデント管理 をインストールすると、製造業プロセスマネージャー もインストールされます。
 - 最新バージョンの オペレーショナルテクノロジー変更管理 をインストールすると、製造業プロセスマネージャー もインストールされます。

Operational Technology Service Managementエクスペリエンスにアクセスできるように、最新バージョンにアップグレードする必要があります。

手順

1. 移動先 **すべて > システムアプリケーション > 利用可能なすべてのアプリケーション > すべて**。
2. フィルター基準と検索バーを使用して 製造業プロセスマネージャー アプリケーションを検索します。

名前または ID でアプリケーションを検索できます。アプリケーションが見つからない場合は、ServiceNow Store への要求が必要になることがあります。

ServiceNow Store Web サイトにアクセスして利用可能なすべてのアプリを表示し、ストアにリクエストを送信する方法について確認してください。リリースされたすべてのアプリのリリースノート情報については、「[ServiceNow Storeバージョン履歴のリリースノート](#)」を参照してください。

3. アプリケーションのインストールダイアログボックスで、アプリケーションの依存関係を確認します。

依存するプラグインとアプリケーションがインストールされる場合、現在インストールされている場合、またはインストールする必要がある場合は、表示されます。インストールする必要があるプラグインまたはアプリケーションがある場合は、製造業プロセスマネージャーをインストールする前にインストールする必要があります。

4. オプション: 利用できるデモデータをインストールするには、[デモデータのロード] チェックボックスをオンにします。
デモデータは、一般的なユースケース向けのアプリケーション機能を説明するサンプルレコードです。開発またはテストインスタンスで初めてアプリケーションをインストールする場合は、デモデータを読み込みます。
5. **[Install (インストール)]** を選択します。

産業用ワークスペースアドミン アプリケーションメニューとガイド付きセットアップ

アプリケーションと関連するプラグインをインストールすると、産業用ワークスペースアドミン アプリケーションメニューを使用して、関連する オペレーショナルテクノロジーマネージャー、製造業プロセスマネージャー、オペレーショナルテクノロジーインシデント管理、オペレーショナルテクノロジー脆弱性対応、オペレーショナルテクノロジー変更管理、オペレーショナルテクノロジーのナレッジ管理、および オペレーショナルテクノロジー要求管理 機能にアクセスできます。

産業用ワークスペースアドミン アプリケーションメニューのコンテンツ

産業用ワークスペースアドミンアプリケーションメニューにアクセスするには、アプリケーションナビゲーターに「Industrial Workspace Admin」と入力します。オペレーショナルテクノロジー管理ソリューションは、現在、次のアプリケーションと機能で構成されています。

- オペレーショナルテクノロジーマネージャー
- 製造業プロセスマネージャー
- オペレーショナルテクノロジー脆弱性対応
- オペレーショナルテクノロジーインシデント管理
- オペレーショナルテクノロジー変更管理
- オペレーショナルテクノロジーのナレッジ管理
- オペレーショナルテクノロジー要求管理

i 注: オペレーショナルテクノロジーインシデント管理 と オペレーショナルテクノロジー変更管理 を使用する前に、まず オペレーショナルテクノロジーマネージャー アプリケーションまたは 製造業プロセスマネージャー アプリケーションをインストールする必要があります。

産業用ワークスペースアドミンアプリケーションメニューに表示されるオプションは、インストールされている OT アプリケーションと、ユーザーにアサインされているロールによって異なります。製造業プロセスマネージャーをインストールすると、産業用ワークスペースアドミンアプリケーションメニューで次の機能を使用できます。

- ガイド付きセットアップ
- すべての OT プロパティ
- ワークスペースのシステムプロパティ
- OT 進捗状況スコアカード構成
- OT 進捗状況スコアカード属性
- OT マネージャー。次の選択肢が含まれます。
 - OT マネージャーアドミン
 - 産業用プロセスマネージャー
 - OT インシデントアドミン
 - オペレーショナルテクノロジー変更管理

アプリケーションのインストールと割り当てられたロールの詳細については、「[製造業プロセスマネージャー をインストールする と 製造業プロセスマネージャーユーザーロールのアサイン](#)」を参照してください。

産業用ワークスペースアドミン ガイド付きセットアップ

admin ロールを持っている場合は、ガイド付きセットアップを使用して、製造業プロセスマネージャー アプリケーションのセットアップ手順をガイドできます。

ガイド付きセットアップにアクセスするには、次に移動します: 産業用ワークスペースアドミン > ガイド付きセットアップ。

ガイド付きセットアップでロック解除済みとして表示される具体的な手順は、インスタンスにインストールしたアプリケーションによって異なります。

製造業プロセスマネージャーのみがインストールされている場合、次のセットアップ機能がロックされます。

- 産業用ワークスペースのセットアップ手順。
- オペレーショナルテクノロジーマネージャーのセットアップ手順。
- オペレーショナルテクノロジーマネージャーに依存する製造業プロセスマネージャーステップ。
- オペレーショナルテクノロジー脆弱性対応のセットアップ手順。
- オペレーショナルテクノロジーインシデント管理のセットアップ手順。
- オペレーショナルテクノロジー変更管理のセットアップ手順。
- オペレーショナルテクノロジーのナレッジ管理のセットアップ手順。
- オペレーショナルテクノロジー要求管理のセットアップ手順。

ガイド付きセットアップとその使用方法の詳細については、「[ガイド付きセットアップの使用](#)」を参照してください。

製造業プロセスマネージャーユーザーロールのアサイン

ユーザーにロールをアサインすると、製造業プロセスマネージャー アプリケーションの各機能やデータへのアクセスを制御できます。

始める前に

必要なロール：admin

このタスクについて

次のテーブルにリストされているロールを持つユーザーは、製造業プロセスマネージャー アプリケーションを使用できます。

ロール	説明
機器モデルビューア [cmdb_ot_isa_viewer]	アサインされた ISA 設備階層モデル [cmdb_ci_ot_isa_entity] テーブルレコードを表示することのみ可能です。詳細については、「 での 製造業プロセスマネージャー の使用 オペレーショナルテクノロジーマネージャー 」と「 設備モデルの管理 」を参照してください。
機器モデルエディター [cmdb_ot_isa_editor]	アサインされた ISA 設備階層モデル [cmdb_ci_ot_isa_entity] レコードを表示および編集できます。 詳細については、「 での 製造業プロセスマネージャー の使用 オペレーショナルテクノロジーマネージャー 」と「 設備モデルの管理 」を参照してください。
機器モデルアドミン [cmdb_ot_isa_admin]	cmdb_ot_isa_editor ロールを継承し、次のアクションも実行できます。 • 産業用ガイド付きセットアップを使用し、製造業プロセスマネージャーとオペレーショナルテクノロジーマネージャーを設定します。 • 機器モデルテンプレート [isa_entity_template]、[isa_entity_level]、

ロール	説明
	および機器エンティティタイプ [isa_entity_type] テーブルレコードを編集する。 詳細については、「産業用ワークスペースアドミン アプリケーションメニューとガイド付き セットアップ」を参照してください。
機器モデルのダウタイムプランナー [sn_isa_schedule_admin]	機器エンティティスケジュールを作成、変更、および削除できます。スケジュールを機器エンティティに関連付けることもできます。
機器モデルビューアー すべて [cmdb_ot_isa_viewer_all]	すべての ISA Equipment Model (ISA 設備階層モデル) レコード (cmdb_ci_ot_isa_entity) と、関連する機器モデルプレートレコード (isa_entity_template、isa_entity_level、isa_entity_type) を表示できます。 cmdb_ot_admin に含まれるロール。
素晴らしいアドミン [sn_ot_amazing_admin]	すべての機器モデルエンティティの OT サブネットシステムプロパティの OT サブネットレコード (ot_subnet_mapping) を作成、変更、削除できます。
素晴らしいエディター [sn_ot_amazing_write]	ユーザーに関連付けられているすべての機器モデルエンティティの OT サブネットレコード (ot_subnet_mapping) を作成、変更、削除できます。
素晴らしいビューアー [sn_ot_amazing_read]	すべての機器モデルエンティティの OT サブネットレコード (ot_subnet_mapping) を表示できます。

手順

ServiceNow AI Platform ユーザー管理機能を使用して、ユーザーとグループにロールをアサインします。

タスク	ユーザー管理機能
ユーザーへのロールのアサイン	ユーザーへのロールの割り当て を参照してください。
グループへのロールのアサイン	グループへのロールのアサイン を参照してください。

OT システムプロパティの表示と編集

さまざまなアプリケーションのすべての オペレーショナルテクノロジー (OT) 関連のシステムプロパティを表示および編集します。

始める前に

必要なロール：admin

このタスクについて

次の OT アプリケーションのシステムプロパティは、ServiceNow AI Platform の [すべての OT プロパティ] モジュールから変更できます。

- OT ネットワークの IT ディスカバリー
- 製造業プロセスマネージャー
- ISA Equipment Model (ISA 設備階層モデル)
- オペレーショナルテクノロジーマネージャー
- オペレーショナルテクノロジーインシデント管理
- オペレーショナルテクノロジーのナレッジ管理
- オペレーショナルテクノロジー変更管理
- 産業用ワークスペース共通

手順

1. 移動先 **すべて** > **産業用ワークスペースアドミン** > **すべての OT プロパティ**.
2. [システムプロパティ] テーブルで、システムプロパティを編集するアプリケーションを選択します。
3. アプリケーションまたは機能の必要に応じて、利用可能なシステムプロパティを編集します。
4. **[Update (更新)]** を選択します。

機器モデルテンプレートの定義

ServiceNow AI Platformで作成した機器モデルエンティティにアサインできるテンプレートを作成します。これらのテンプレートを使用して、機器モデルを特徴付けたり、類似のタイプの機器モデルエンティティをグループ化することで物理的な産業施設を記述するデータを構造化したりできます。

機器モデルテンプレートの作成

テンプレートの使用方法を識別して説明する機器モデルテンプレートレコードを作成します。機器モデルテンプレートを作成した後、その階層レベルとタイプを作成できます。

始める前に

必要なロール:cmdb_ot_isa_admin

手順

1. 移動先 **すべて** > **産業用ワークスペースアドミン** > **産業用プロセスマネージャー** > **機器モデルテンプレート**.
2. **[New]** をクリックします。
3. フォームで、フィールドに入力します。

機器モデルテンプレートフォーム

フィールド	説明
名前	機器モデルテンプレートの名前。
説明	機器モデルテンプレートの説明。

フィールド	説明
アプリケーション	選択したアプリケーションスコープ。このスコープがグローバルアプリケーションスコープの場合は、[グローバル] と表示されます。

4. [Submit (送信)] を選択します。

次のタスク

機器モデルテンプレートの階層ソートレベルを作成します。

機器モデルテンプレートの階層ソートレベルの作成

機器モデルテンプレートの階層レベルを作成してアサインします。機器テンプレートを機器モデルに割り当てると、これらのレベルはそこに表示されるデータをソートして構造化します。

始める前に

必要なロール：admin

このタスクについて

ソートのために機器モデルテンプレートにレベルを割り当てることができます。たとえば、サイト、エリア、ワークセンタ、およびその他のレベルを設備に割り当て、それぞれのソート順序を指定できます。

手順

1. 移動先 **すべて** > **産業用ワークスペースアドミン** > **産業用プロセスマネージャー** > **機器モデルテンプレート**。
2. 機器モデルテンプレートを選択します。
3. [テンプレートレベル] 関連リストで、[新規] をクリックします。
4. フォームで、フィールドに入力します。

テンプレートレベルフォーム

フィールド	説明
レベル名	機器モデルを割り当てるレベルの名前。たとえば、次の例が挙げられます。 サイト 工業用地。 エリア 工業用地内のエリア。 ワークセンター 産業現場のワークセンター。
親	このレベルより上の機器モデルテンプレートレベルの識別子。空のままにすると、このレベルはモデルのトップレベルになります。たとえば、次のアクションを実行できます。

フィールド	説明
	○ サイトレベルを作成する場合、親を持たない機器モデル階層の最上位レベルであれば、このフィールドを空のままにします。 ○ エリアレベルを作成していて、それがサイトレベルの子である場合は、その親として サイト を選択します。 ○ ワークセンターレベルを作成していて、それがエリアレベルの子である場合は、その親として [エリア] を選択します。
アプリケーション	選択したアプリケーションスコープ。このスコープがグローバルアプリケーションスコープの場合は、 [グローバル] と表示されます。
テンプレート	選択した機器モデルテンプレートの名前。
順序	ソートのための設備モデル階層内のレベルの位置を示す番号。入力された最小の数値は、最上位の階層レベルを表します。たとえば、サイトが機器モデルテンプレートの階層の最上位レベルを表す場合は、サイトに 1 を入力します。

5. **[Submit (送信)]** を選択します。

次のタスク

機器モデルテンプレートの階層レベル内に詳細なタイプを作成します。

機器モデルレベルタイプの作成

作成した各機器モデルテンプレートレベル内に詳細なレベルタイプを作成します。そのレベル内で作成する詳細なレベルタイプは、そのレベル内の本番プロセスのタイプを示します。

始める前に

必要なロール：admin

このタスクについて

レベル内のさまざまなタイプの場所、エリア、または機能を表すタイプを作成できます。たとえば、ISA 95 テンプレートでは、ワークセンターレベルに次のレベルタイプがあります。

- 生産セル
- 生産単位
- 生産ゾーン
- ストレージゾーン

手順

1. 移動先 **すべて > 産業用ワークスペースアドミン > 産業用プロセスマネージャー > 機器モデルテンプレート**。
2. 機器モデルテンプレートを選択します。
3. **[テンプレートレベル]** 関連リストで、機器モデルテンプレートレベルを選択します。
4. **[テンプレートタイプ]** 関連リストで、**[新規]** をクリックします。
5. フォームで、フィールドに入力します。

テンプレートレベルタイプフォーム

フィールド	説明
レベルタイプ名	選択した機器モデルテンプレートレベルにアサインするレベルタイプの名前。たとえば、生産セルを割り当て、作業区レベルの生産セルタイプを作成します。
レベル名	選択した機器モデルテンプレートレベルの名前。
アプリケーション	選択したアプリケーションスコープ。このスコープがグローバルアプリケーションスコープの場合は、[グローバル] と表示されます。
テンプレート	選択した機器モデルテンプレートの名前。

6. [Submit (送信)] を選択します。

機器モデルデータのインポート

スケジュール済みインポート機能を使用すると、入力済みの Excel フラットファイルスプレッドシートから既存の機器モデルデータをインポート Microsoft。これを使用して、ISA-95 機器モデルデータを 構成管理データベース (CMDB) にインポートできます。

機器モデルデータをインポートする前に、製造業プロセスマネージャー をインストールする必要があります。

機器モデルデータを ServiceNow AI Platform にインポートするには、いくつかの方法を使用できます。

1. スプレッドシートを使用してデータをインポートする場合は、Microsoft Excel スプレッドシートに既存の ISA-95 設備階層モデルのデータを取り込み、**SG**:スプレッドシートを使用した設備階層モデルのインポートスケジュール済みインポートを実行する必要があります。多くの従来のレコードシステムには、このデータを Excel スプレッドシートにエクスポートできる機能が含まれているため、手動で入力する必要はありません。
2. いくつかの ServiceNow パートナーは、機器モデルデータを保存するサードパーティのレガシーレコードシステムとの統合も開発しています。
 - これらの統合が利用可能になったら、製造業プロセスマネージャー の オペレーショナルテクノロジー 認定統合を検索することで、ServiceNow Store で見つけることができます。
 - ご使用の環境に適用可能な統合をインストールし、必要に応じて実行します。

これらのインポート方法を使用すると、必要に応じて、信頼できるソースに保存されているデータで ServiceNow AI Platform 内の既存の機器モデルを更新できます。新しくインポートされたデータの場合、ServiceNow AI Platform は機器モデルエンティティの CI クラスレコードを 構成管理データベース (CMDB) に自動的に作成します。

インポート処理に影響するシステムプロパティ

次のシステムプロパティは、Microsoft Excel スプレッドシートに機器モデルデータを入力する方法と、機器モデルのインポート - ETL プロセスがどのように機能するかに影響します。

`sn_isa_model.cmdb_relationships_sync_levels`

ServiceNow AI Platform にインポートして構成管理データベース (CMDB) で同期できる機器モデルのレベル数を決定します。デフォルト値は 8 です。

sn_isa_model.short_code_validation_max_length

スプレッドシートのショートコード列の最大長を設定します。デフォルト値は 3 です。

sn_isa_model.user_search_matching_attribute

入力されたスプレッドシートからインポートされたユーザーデータ参照を、システムユーザー [sys_user] テーブルに保存されている対応するユーザーレコードと照合します。メールアドレスは各ユーザーレコードに対して一意であるため、デフォルトはユーザーのメールアドレスです。

glide.scriptable.excel.max_ファイル_サイズ

Excel ファイルの最大サイズをバイト単位で設定します。このプロパティはグローバルです。

- i** 注: システムの動作を制御するためのシステムプロパティの追加または作成の詳細については、「[システムプロパティを追加する](#)」を参照してください。

Microsoft Excel スプレッドシートに機器モデルデータを入力する

Microsoft Excel スプレッドシートを作成し、既存の ISA 設備階層モデルデータを入力します。アップロードを成功させるには、既存のデータを正しい列に配置することが重要です。

ServiceNow AI Platform の構成管理データベース (CMDB) を適切に入力する Microsoft Excel スプレッドシートを作成するには、次のアクションを実行します。

1. データソースレコードに添付されている Microsoft Excel スプレッドシートを使用して、アップロードするスプレッドシートを準備します。空のテンプレートを見つけるには、次のアクションを実行します。

a. 移動先 機器モデル: **ISA** > 機器のインポート。モデル - データソース

b. **[Import Equipment Model - Data Source - v2.xlsx]** をクリックします。

- i** 注: または、「機器モデルのインポート - データソース - v2.xlsx」スプレッドシートをダウンロードするには、Now Support ナレッジベースの記事「[ISA 設備階層モデル Excel サービスグラフコネクタ \[KB0966600\]](#)」に必要な [Microsoft Excel スプレッドシート](#)」を参照してください。

2. 添付の機器モデルのインポート - データソース - v2.xlsx スプレッドシートをダウンロードして、テンプレートとそのワークシートの詳細を確認してください。

- i** 注: v1 から v2 にアップグレードする ISA SGC ユーザーの場合は、以下の「v1 から v2 へのアップグレード」セクションを参照してください。

機器モデルをインポート - データソース - スプレッドシート v2.xlsx

ワークシート名	目的
データインポート用の空のテンプレート	インポートする機器モデルデータを入力します。詳細な例については、このトピックの残りの部分を参照してください。
データ列の説明	このトピックの情報と同様に、スプレッドシートのデータ列の説明を提供します。
インポート用のサンプルデータ	スプレッドシートにインポートする機器モデルの例を提供します。これらの例は、このトピックの残りの部分で表示できます。

3. Microsoft Excel スプレッドシートに入力したら、統合ハブ ETL 関数を実行するときに簡単にアクセスできるように、既知の場所に保存します。

i 注: 列名は変更できません。sn_isa_model.user_search_matching_attribute システムプロパティで指定されたとおりに、所有者を一意に識別するための列を追加して、追加のフィールドをサポートすることができます。

スプレッドシートに入力する

サンプルのオペレーショナルテクノロジーデータ、列 **A** から **J**

1 つのスプレッドシートで複数のサイトからデータをインポートできます。サンプル画像は、ATL と CTL の 2 つのサイトのデータを示しています。

	A	B	C	D	E	F	G	H	I	J
1	Path	Short Code	Entity Name	Location	Assigned to	Support Group	Description	Process criticality	Company	Template
2	ATL	ATL	Atlanta Site	Atlanta Car Facility	fred.luddy@example.com	Atlanta Plant Support	the site in Atlanta where we make cars	1 - most critical	Demo Car Corp	ISA 95 Default Template
3	ATL-B64	B64	Building 64	Atlanta Building 64	fred.luddy@example.com	Atlanta Plant Support	the building with the number 64 on the side	1 - most critical	Demo Car Corp	ISA 95 Default Template
4	ATL-B42	B42	Building 42	Atlanta Building 42	fred.luddy@example.com	Atlanta Plant Support	similar to building 64 except with a 42 on the side	2 - somewhat critical	Demo Car Corp	ISA 95 Default Template
5	ATL-B64-MASS	MASS	Model M	Atlanta Building MASS	fred.luddy@example.com	Atlanta Plant Support	model S needs to be assembled somewhere	1 - most critical	Demo Car Corp	ISA 95 Default Template
6	ATL-B64-QASS	QASS	Model Q	Atlanta Building QASS	fred.luddy@example.com	Atlanta Plant Support	a place for the Q model to get assembled	1 - most critical	Demo Car Corp	ISA 95 Default Template
7	ATL-B64-MPROD	MPROD	Model MPROD	Atlanta Building MPROD	fred.luddy@example.com	Atlanta Plant Support	Model S also needs a production line	1 - most critical	Demo Car Corp	ISA 95 Default Template
8	ATL-B64-QPROD	QPROD	Model QPROD	Atlanta Building QPROD	fred.luddy@example.com	Atlanta Plant Support	Model Q production line	1 - most critical	Demo Car Corp	ISA 95 Default Template
9	ATL-B64-MQSTOR	MQSTOR	Model M and Q	Atlanta Building MQSTOR	fred.luddy@example.com	Atlanta Plant Support	storage for the models we built	2 - somewhat critical	Demo Car Corp	ISA 95 Default Template
10	ATL-B64-QPROD-C1	C1	Cell 1	Atlanta Building C1	fred.luddy@example.com	Atlanta Plant Support	Q prod assembly cell 1	1 - most critical	Demo Car Corp	ISA 95 Default Template
11	ATL-B64-QPROD-C2	C2	Cell 2	Atlanta Building C2	fred.luddy@example.com	Atlanta Plant Support	Q prod assembly cell 2	1 - most critical	Demo Car Corp	ISA 95 Default Template
12	ATL-B64-MQSTOR-Z1	Z1	Zone 1	Atlanta Building Z1	fred.luddy@example.com	Atlanta Plant Support	storage zone for MQ for transfer	2 - somewhat critical	Demo Car Corp	ISA 95 Default Template
13	ATL-B64-MQSTOR-Z6	Z6	Zone 2	Atlanta Building Z6	fred.luddy@example.com	Atlanta Plant Support	storage zone for MQ to just store the stuff	2 - somewhat critical	Demo Car Corp	ISA 95 Default Template
14	CTL	CTL	California Site	California Car Facility	fred.luddy@example.com	California Plant Support	the site in California where we make cars	1 - most critical	Demo Car Corp	ISA 95 Default Template
15	CTL-C64	C64	Building 64	California Building 64	fred.luddy@example.com	California Plant Support	the building with the number 64 on the side	1 - most critical	Demo Car Corp	ISA 95 Default Template

列 **A** から **J**

列	名前	タイプ	説明	必須
A	パス	文字列	このエンティティとそのすべての親エンティティの短縮コードの連結。例えば、ATL-B42-MQSTOR-Z1 は、以下の短縮コードを連結したものです。 - アトランタサイトの ATL 短縮コード。 - 建物 B42 の B42 短縮コード。 - モデル M および Q の MQSTORE 短縮コード。 - Model M および Q のゾーン1転送ストレージゾーンのZ1ショートコード。	はい
B	短縮コード	文字列、英数字のみ	エンティティの簡単な説明コード。ショートコードの例については、前のパス列の説明を参照してください。 ショートコードは、sn_isa_model.short_code_validation_max_length システムプロパティで指定された最大長より長くすることはできません。	いいえ
C	エンティティ	文字列	エンティティの正式名称。たとえば、都市名、建物番号、モデル番号などです。	はい

列 A から J (続く)

列	名前	タイプ	説明	必須
	ティ 名			
D	場所	文字 列	エンティティの場所。たとえば、そこに配置されている機器モデルごとに Atlanta Building 64 をリストします。ServiceNow AI Platform内の構成管理データベース (CMDB)に格納され、参照として使用する cmn-location 値。	い い え
E	アサ イン 先	文字 列	このエンティティレコードを所有および管理する担当者のメールアドレス。 i 注: <code>sn_isa_model.user_search_matching_attribute</code> システムプロパティで指定された設定に基づいて、追加の属性を使用できます。	い い え
F	サ ポー トグ ループ	文字 列	このエンティティのメンテナンスと管理をサポートするグループの名前。	い い え
G	説明	文字 列	この機器モデルエンティティとその目的の詳しい説明。	い い え
H	プロ セス の重 要度	文字 列	エンティティが産業プロセスにとってどの程度重要または重要であることを示す測定値。次に例を示します。 • 1 - 最重要。 • 2 - ある程度重要。	い い え
I	会社	文字 列	エンティティが属する会社の名前。ServiceNow AI Platform内のCMDBに格納され、参照として使用する cmn-location 値。	い い え
J	テ ンプ レー ト	文字 列	データのインポートに使用するテンプレート。 i 注: データをインポートした後、テンプレートを設定することはできません。	はい

v1 から v2 へのアップグレード

v1 から v2 にアップグレードする ISA SGC ユーザーの場合は、一意のパスを持つ新しい ISA 設備階層モデルエンティティをインポートし、修正スクリプトのあるパス値が既にある既存の ISA 設備階層モデルエンティティを更新できます。

データソースとインポートスケジュールを使用した機器モデルデータのインポート

機器モデルデータで Microsoft Excel スプレッドシートを完成させたら、データソースとインポートスケジュールを使用して、ServiceNow AI Platform にインポートします。

始める前に

このプロセスを実行する前に、インポートする Microsoft Excel スプレッドシートを準備する必要があります。詳細については、「[Microsoft Excel スプレッドシートに機器モデルデータを入力する](#)」を参照してください。

必要なロール:cmdb_inst_admin、import_admin

このタスクについて

このプロセスを実行すると、スプレッドシートに含まれる機器モデルレコードの 構成管理データベース (CMDB) に一意の機器モデルエンティティ CI クラスレコードが作成されます。

手順

1. 移動先 [すべて > 機器モデル : ISA > 機器のインポート](#)。モデル - データソース。
2. **SG** 設備モデルのデータソースレコードで、作成した Microsoft Excel スプレッドシートを添付します。
 - a. [添付ファイルを管理] を選択します。
 - b. [添付ファイル] ダイアログ ボックスで、[ファイルを選択] を選択します。
 - c. 作成した Microsoft Excel スプレッドシートを選択し、[添付ファイル] ダイアログ ボックスを閉じます。
 - d. スプレッドシートを添付した後、[すべてのレコードをロード] 関連リンクを選択して、スプレッドシートからインポートテーブルにすべてのレコードをロードします。操作が完了すると、エラーなしでデータがロードされた場合、成功 完了コードを含む次の確認メッセージが表示されます。

Progress

Name	ImportProcessor
State	Complete
Completion code	Success
Message	Processed: 25, inserts 0, updates 0, errors 0, empty and ignored 25, ignored errors 0 (0:00:00.087)

Next steps...

- [Import sets](#) Go to the import sets for this data load
- [Loaded data](#) Go to the newly imported data inside the staging table: sg_isa_entity_import
- [Run Robust Transform](#) Transform a loaded import set using a robust transform
- [Import log](#) View the import log

す。

e. 確認メッセージで、[強力な変換を実行] 関連リンクを選択します。

f. **[Transform (変換)]** を選択します。インポートが成功すると、成功 完了コードを含む次の確認メッセージが表示されます。

Progress

Name	Transforming: ISET0010001
State	Complete
Completion code	Success
Message	Transformation complete

Next steps...

[ISET0010001](#) Go to the import sets for this data load

[Transform history](#) Show the transform history, related errors and log

[Import log](#) View the import log

す。

アドミニストレーター以外の機器モデルサイトアクセスの割り当てまたは削除

アドミニストレーター以外の機器モデルサイトアクセス権をアサインまたは削除します。ユーザー基準を作成して、特定のユーザーが特定のサイトの機器モデルエンティティにアクセスできるかどうかを決定できます。

始める前に

必要なロール：admin

このタスクについて

ユーザー基準を使用して、特定のユーザーが特定のサイトの機器モデルエンティティを読み取りまたは編集できるかどうかを決定します。ユーザー基準レコードを作成したら、それをサイトにアサインして、機器モデルエンティティの読み取りと編集が可能なユーザーを制御できます。さらに OT ロールをユーザーまたはグループにアサインして、同じサイトにアサインされている OT デバイスにアクセスできるようにすることができます。詳細については、「[オペレーショナルテクノロジー マネージャー ロールの割り当て](#)」を参照してください。

i 注：バージョン 1.0.12 にアップグレードするユーザーの場合、サイト ユーザー アクセスはユーザー条件とグループに移行されます。詳細については、「[サイトユーザーアクセスをユーザー基準とグループに移行する](#)」を参照してください。

手順

1. 移動先 [すべて > ナレッジ管理 > アドミニストレーション > ユーザー基準](#)
2. **[New (新規)]** を選択します。
3. フォームのフィールドに入力します。
フィールド値の説明については、「[\[ユーザー基準\] フォーム](#)」を参照してください。

次のタスク

ユーザー基準を作成したら、それをサイトに割り当てることができます。サイトへの編集可能アクセス権の割り当ての詳細については、「[サイトへの編集可能アクセスのユーザー基準を割り当てる](#)」を参照してください。サイトに [読み取り可能] アクセスを追加する方法の詳細については、「[サイトへの読み取り可能アクセスのユーザー基準を割り当てる](#)」を参照してください。

サイトへの読み取り可能アクセスのユーザー基準を割り当てる

サイトにユーザー基準をアサインして、選択したサイトに属する機器モデルエンティティを読み取りまたは表示できるユーザーを定義します。

始める前に

必要なロール:cmdb_ot_isa_admin または admin

このタスクについて

[読み取り可能] アクセスのユーザー基準は、次の 2 つの場所で割り当てることができます。

- 機器モデルエンティティビューアクセステーブルから
- サイトレコードの [機器モデルの読み取りが可能] 関連リストから

手順

1. テーブルまたは関連リストに移動します。

場所	ナビゲーション
機器モデルエンティティビューアクセステーブル	すべて > 機器モデル: ISA > ユーザー基準: 読み取り可能
機器モデルの読み取り可能関連リスト	すべて > 機器モデル: ISA > 拠点 をクリックし、サイトレコードを開きます。[機器モデルの読み取りが可能] 関連リストを選択します。

2. 新規 を選択してレコードを作成します。

3. [サイト] フィールドで、必要な機器モデルサイトレコードを選択します。

4. [ユーザー基準] フィールドで、ユーザー基準を選択して、選択したサイトの機器モデルエンティティを読み取りまたは表示できるユーザーを定義します。

i 注: ユーザーが cmdb_ot_viewer ロールを持っている場合、選択したサイトにアサインされている オペレーショナルテクノロジー (OT) デバイスを表示することもできます。

ユーザーがcmdb_ot_editorロールを持っている場合、ユーザーは選択したサイトに割り当てられている OT デバイスを編集できます。

5. [Submit (送信)] を選択します。

サイトへの編集可能アクセスのユーザー基準を割り当てる

サイトにユーザー基準をアサインして、選択したサイトに属する機器モデルエンティティを編集できるユーザーを定義します。

始める前に

必要なロール:cmdb_ot_isa_admin または admin

このタスクについて

[編集可能] アクセスのユーザー基準は、次の 2 つの場所で割り当てることができます。

- 機器モデルエンティティ編集アクセステーブルから
- サイトレコードの [機器モデルを編集可能] 関連リストから

手順

1. 次のいずれかに移動します。

場所	ナビゲーション
機器モデルエンティティビューアクセステーブル	すべて > 機器モデル: ISA > ユーザー基準: 編集可能
[機器モデルを編集可能] 関連リスト	すべて > 機器モデル: ISA > 拠点 をクリックし、サイトレコードを開きます。[機器モデルを編集可能] 関連リストを選択します。

2. 新規 を選択してレコードを作成します。
3. [サイト] フィールドで、必要な機器モデルサイトレコードを選択します。
4. [ユーザー基準] フィールドでユーザー基準を選択し、選択したサイトの機器モデルエンティティを編集できるユーザーを定義します。

i 注: ユーザーが cmdb_ot_viewer ロールを持っている場合、選択したサイトにアサインされている オペレーショナルテクノロジー (OT) デバイスを表示することもできます。

ユーザーが cmdb_ot_editor ロールを持っている場合、ユーザーは選択したサイトに割り当てられている OT デバイスを編集できます。

5. [Submit (送信)] を選択します。

機器モデルエンティティスケジュールの管理

製造業プロセスマネージャー アプリケーションで機器モデルエンティティスケジュールを管理できます。スケジュールを使用すると、1 つの機器モデルエンティティに対する複数のメンテナンスタスクを追跡できます。

機器モデルエンティティのスケジュールの概要

スケジュールは、任意の機器モデルエンティティにリンクできます。機器モデルのダウンタイムプランナーロール (sn_isa_schedule_admin) を持っている場合は、機器モデルエンティティのスケジュールエントリを追加、変更、または削除し、次のタスクを実行できます。

- さまざまな機器モデルエンティティのスケジュールを管理します。
- これらのスケジュールを機器モデルエンティティに関連付けます。
- オペレーショナルテクノロジー (OT) インシデントまたは修復タスクで作業できるように、スケジュールからタイムスロットを選択します。詳細については、「[OT 修復タスクの開始時間の選択](#)」を参照してください。

例

1 つの機器モデルエンティティスケジュールに複数のスケジュールエントリを設定するとします。これらのエントリは、さまざまなタスクを完了し、異なる時間に発生します。これを行うには、既存の機器モデルエンティティスケジュールレコードの [スケジュールエントリ] 関連リンクでスケジュールエントリを作成します。

機器モデルエンティティに関連付けられたスケジュールが不要になった場合は、機器モデルエンティティレコードの [スケジュール] 関連リンクを使用してスケジュールをデタッチできます。

機器モデルエンティティの既存のスケジュールを表示する場合は、機器モデルマネージャーまたはプラットフォームの計画されたダウンタイムモジュールで表示できます。

機器モデルエンティティスケジュールの作成

製造業プロセスマネージャー アプリケーションで機器モデルエンティティスケジュールを作成します。これらのスケジュールを使用すると、複数の機器モデルエンティティを簡単に管理できます。

始める前に

必要なロール:sn_isa_schedule_admin

手順

1. 移動先 **すべて > 産業用ワークスペースアドミン > 産業用プロセスマネージャー > 機器モデルエンティティのスケジュール**.
2. **[New (新規)]** を選択します。
3. フォームで、フィールドに入力します。

機器モデルエンティティのスケジュールフォーム

フィールド	説明
名前	スケジュールの一意の名前です。
タイムゾーン	スケジュールのタイムゾーンです。[浮動] を選択した場合、タイムゾーンは、アイテムにアクセスしているプロセスに比例します。 たとえば、アムステルダムのリソースマネージャーがフローティングスケジュールを 8:00 から 17:00 に設定した場合、カリフォルニア州サンノゼのユーザーにもそのスケジュールが 8:00 から 17:00 として表示されます。1 つのタイムゾーンでスケジュールを定義すると、異なるタイムゾーンのユーザーには、それぞれのタイムゾーンでスケジュールが表示されます。
タイプ	スケジュールの目的を説明するテキストラベル。
説明	スケジュールの説明。

4. **[Submit (送信)]** を選択します。

次のタスク

これで、機器モデルエンティティスケジュールのエントリを作成できます。詳細については、「[スケジュールエントリの作成](#)」を参照してください。

スケジュールエントリの作成

製造業プロセスマネージャーアプリケーションで、既存の機器モデルエンティティスケジュールのスケジュールエントリを作成します。1 つのスケジュールに対して複数のエントリを作成できます。スケジュールエントリを使用すると、1 つの機器モデルエンティティに対して複数のメンテナンスタスクを実行できます。

始める前に

必要なロール:sn_isa_schedule_admin

手順

1. 移動先 **すべて > 産業用ワークスペースアドミン > 産業用プロセスマネージャー > 機器モデルエンティティのスケジュール.**
2. 既存の機器モデルエンティティスケジュールレコードを選択します。
3. [**スケジュールエントリ**] タブを選択します。
4. **[New (新規)]** を選択します。
5. フォームで、フィールドに入力します。

スケジュールエントリフォーム

フィールド	説明
名前	スケジュールエントリの一意の名前。
タイプ	スケジュールの目的を説明するラベル。
表示方法	カレンダーアプリケーションでスケジュールエントリを表示する方法を示すオプション。
繰り返し	スケジュールエントリの繰り返し間隔 (存在する場合)。繰り返し間隔を選択すると、他のフィールドが表示され、繰り返し間隔をさらに指定できます。
繰り返し間隔	スケジュールの繰り返し頻度 (週次、月次、または年次)。このフィールドは、[繰り返し] フィールドで [日次]、[週次]、[月次]、または [年次] が選択されている場合にのみ表示されます。
繰り返し	週次スケジュールが繰り返される曜日。このフィールドは、[繰り返し] フィールドで [週次] が選択されている場合にのみ表示されます。
月次タイプ	月次スケジュールの繰り返し頻度。このフィールドは、[繰り返し] フィールドで [月次] が選択されている場合にのみ表示されます。次のオプションが含まれます。 ○ 毎月特定の日に繰り返します。 ○ 月の特定の週の特定の日に繰り返します。 ○ 月の最終日に繰り返します。 ○ 月の最終週の特定の曜日に繰り返します。
年次タイプ	年次スケジュールの繰り返し頻度。このフィールドは、[繰り返し] フィールドで [年次] が選択されている場合にのみ表示されます。次のオプションが含まれます。 ○ 年の特定の日に繰り返します。 ○ 浮動日に繰り返します。

フィールド	説明
浮動週	浮動年次スケジュールが繰り返される月の週。このフィールドは、[年次] フィールドで [フロート中] が選択されている場合にのみ表示されます。
浮動日	浮動年次スケジュールが繰り返される曜日。このフィールドは、[年次] フィールドで [フロート中] が選択されている場合にのみ表示されます。
月	浮動年次スケジュールが繰り返される月。このフィールドは、[年次] フィールドで [フロート中] が選択されている場合にのみ表示されます。
繰り返し期限	繰り返し終了日。このフィールドを空のままにすると、スケジュールが無期限に繰り返されます。

6. [Submit (送信)] を選択します。

結果

スケジュールエントリが作成され、必要に応じてエントリを編集および更新できるようになります。

機器モデルエンティティへのスケジュールの関連付け

製造業プロセスマネージャー アプリケーションで、機器モデルエンティティの 1 つ以上のメンテナンススケジュールの作成、既存のスケジュールの編集、またはスケジュールの削除を行います。

始める前に

必要なロール:sn_isa_schedule_admin

手順

1. 移動先 すべて > 機器モデル：ISA > 機器モデルエンティティ。
2. スケジュールに関連付ける機器モデルエンティティを選択します。
3. [スケジュール] タブを選択します。
4. オプション: 選択した機器モデルエンティティに新しいスケジュールを追加するには、次のアクションを実行します。
 - [New (新規)] を選択します。
 - フォームに入力し、[送信] を選択します。
5. オプション: 選択した機器モデルエンティティのスケジュールを削除するには、次のアクションを実行します。
 - 削除するスケジュールを選択します。
 - [削除] を選択します。
6. オプション: 選択した機器モデルエンティティのスケジュールを編集するには、次のアクションを実行します。
 - 編集するスケジュールを選択します。
 - 変更を追加して [更新] を選択します。

結果

メンテナンススケジュールが作成、削除、または編集されます。従った手順に応じて、適格なユーザーは新しいスケジュールを表示したり、削除されたスケジュールが表示されなくなったり、スケジュールの編集されたバージョンを表示したりできます。

機器モデルエンティティへのスケジュールの添付

製造業プロセスマネージャアプリケーションを使用して、既存のスケジュールを機器モデルエンティティに添付します。機器モデルエンティティにスケジュールを添付すると、スケジュールとそのエントリがそのエンティティに適用されます。

始める前に

必要なロール:sn_isa_schedule_admin

手順

1. 移動先 **すべて > 機器モデル : ISA > 機器モデルエンティティ**.
2. 機器モデルエンティティレコードを選択します。
3. [**スケジュール**] タブを選択します。
4. **[Edit (編集)]** を選択します。
5. [コレクション] リストで、機器モデルエンティティに添付するスケジュールを選択します。
6. 中央矢印を使用して、選択したスケジュールを [スケジュール] リストに移動します。
7. **[Save (保存)]** を選択します。

結果

これで、添付されたスケジュールが機器モデルエンティティに適用されました。機器モデルエンティティレコードで添付されたスケジュールを表示および管理できます。

機器モデルエンティティからのスケジュールのデタッチ

製造業プロセスマネージャアプリケーションを使用して、機器モデルエンティティから既存のスケジュールをデタッチします。スケジュールが機器モデルエンティティに適用されなくなった場合は、そのエンティティに表示されないように簡単に削除できます。

始める前に

必要なロール:sn_isa_schedule_admin

手順

1. 移動先 **すべて > 機器モデル : ISA > 機器モデルエンティティ**.
2. 機器モデルエンティティレコードを選択します。
3. [**スケジュール**] タブを選択します。
4. **[Edit (編集)]** を選択します。
5. [スケジュール] リストで、機器モデルエンティティからデタッチするスケジュールを選択します。
6. 中央矢印を使用して、選択したスケジュールを [コレクション] リストに移動します。
7. **[Save (保存)]** を選択します。

機器モデルエンティティのスケジュールの表示

製造業プロセスマネージャアプリケーションで既存の機器モデルエンティティのスケジュールを表示します。

始める前に

必要なロール:cmdb_ot_isa_viewer

このタスクについて

機器モデルエンティティのスケジュールは、作業場所に応じて次の 2 つの場所に表示できます。

- 機器モデルマネージャー
- プラットフォーム上の計画されたダウンタイムモジュール

手順

1. 機器モデルマネージャーで機器モデルエンティティのスケジュールを表示するには、次のアクションを実行します。
 - a. 機器モデルマネージャーに移動します。
 - b. 機器モデルエンティティレコードを選択します。
 - c. [スケジュールを表示] を選択します。
 - d. その機器モデルエンティティのダウンタイムスロットを表示します。
2. 計画されたダウンタイムモジュールで機器モデルエンティティのスケジュールを表示するには、次のアクションを実行します。
 - a. 移動先 **すべて > 産業用ワークスペースアドミン > 産業用プロセスマネージャー > 計画されたダウンタイム**.
 - b. スケジュールと機器モデルエンティティの関連付けを表示します。

子スケジュールを追加

製造業プロセスマネージャーアプリケーションを使用して、既存の機器モデルエンティティスケジュールに子スケジュールを追加します。子スケジュールを調整すると、親スケジュールにも適用されます。たとえば、特定の日のスケジュール時刻を延長したり、スケジュールから休日を削除したりできます。

始める前に

必要なロール:sn_isa_schedule_admin

手順

1. 移動先 **すべて > 産業用ワークスペースアドミン > 産業用プロセスマネージャー > 機器モデルエンティティのスケジュール**.
2. 既存の機器モデルエンティティスケジュールのレコードを選択します。
3. [子スケジュール] タブを選択します。
4. [Edit (編集)] を選択します。
5. [コレクション] リストで目的のスケジュールを選択します。
6. 中央矢印を使用して、選択したスケジュールを [子スケジュール] リストに移動します。
7. [Save (保存)] を選択します。

結果

選択した子スケジュールが親スケジュールに適用されます。

での 製造業プロセスマネージャー の使用 オペレーショナルテクノロジー ジーマネージャー

機器モデルのインポートなど、必要なすべてのセットアップタスクを完了すると、産業用ワークスペースアドミンメニューのオペレーショナルテクノロジージーマネージャー機能と製造業プロセスマネージャー機能を使用できます。これらの機能には、機器モデルマネージャーと産業用ワークスペースが含まれます。

次の図は、企業の運用上の問題について産業担当者がよく尋ねるいくつかの一般的な質問と、それらに回答するために使用する ServiceNow AI Platform 機能を示しています。これらの機能は、担当者が産業施設内のデータの関係を視覚化するのに役立ちます。

運用上の問題に関する産業担当者の質問



構成マネージャーの Betty は、エンタープライズ レベルで作業しており、OT デバイスが企業内のどこにあるかを知りたいと考えています。この質問に答えるために、Configuration Manager は 産業用ワークスペースアドミン メニューのオペレーショナルテクノロジージーマネージャー機能を使用できます。詳細については、「[産業用ワークスペースアドミン アプリケーションメニューとガイド付きセットアップ](#)」を参照してください。

OT エンジニアである Bhuvnesh は、サイトレベルで作業しており、OT デバイスが特定の生産プロセスにどのようにマッピングされるかを知りたいと考えています。たとえば、「産業プロセスのこの特定の部分を制御しているのはどのHMIとPLCですか? この質問に答えるために、サイトレベルの OT マネージャーは 産業用ワークスペースアドミン メニューの製造業プロセスマネージャー機能を使用できます。

設備モデルの管理

産業用ワークスペースの機器モデルマネージャーを使用すると、ISA-95 機器モデルデータを確認および管理できます。これを使用して、インポートされた機器モデルデータを確認したり、機器モデルを手動で作成したりします。

の機器モデルマネージャー 産業用ワークスペース

機器モデルは、特定の施設の運用要素をマッピングします。たとえば、アトランタにある、材料を保管し、それらを使用して自動車を生産する産業施設などです。機器モデルマネージャーを使用すると、特定の産業サイトの選択した機器モデルエンティティと関連レコードを表示できます。機器モデルマネージャーには、OT 環境で機器モデルエンティティを管理するのに役立つ次の機能が含まれています。

- 機器モデル階層と他の機器モデルエンティティとの関係をグラフィカルに表現して表示します。
- 上流または下流の生産プロセスを表示またはマッピングします。
- 子機器モデルエンティティを確認します。

- 選択した機器モデルエンティティに追加の OT デバイスを確認または関連付けます。
- 子機器モデルエンティティをお気に入りに追加し、お気に入りのみを表示するようにビューを更新します。
- 複数のレコードを表示または作成するときに、レコードを 1 行のタブで開くことで、レコードコンテキストを維持します。

i 注: cmdb_ot_isa_admin ロールがアサインされたユーザーは、任意のサイトの機器モデルエンティティを表示できます。ただし、cmdb_ot_isa_editor または cmdb_ot_isa_viewer ロールが割り当てられているユーザーは、管理者が特定のユーザーにアクセス権を付与したサイトのみアクセスできます。サイト アクセスの許可の詳細については、「[アドミニストレーター以外の機器モデルサイトアクセスの割り当てまたは削除](#)」を参照してください。

機器モデルの詳細の確認と更新

ServiceNow AI Platform にインポートした機器モデルの詳細を確認して更新し、情報が正しいことを確認できます。新しい機器モデルエンティティを手動で作成し、それに詳細を追加することもできます。

始める前に

機器モデルデータを ServiceNow AI Platform にインポートします。詳細については、「[機器モデルデータのインポート](#)」を参照してください。

必要なロール: cmdb_ot_isa_viewer、cmdb_ot_isa_editor、cmdb_ot_isa_admin。

このタスクについて

cmdb_ot_isa_viewer ロールが割り当てられている場合は、機器モデルエンティティのみを表示できます。他にアサインされている cmdb_ot_isa ロールがある場合は、機器モデルエンティティを編集することもできます。

手順

1. 移動先 **すべて > 産業用ワークスペースアドミン > 産業用プロセスマネージャー > 機器モデルマネージャー**。
2. [機器モデルビュー対象] フィールドで、機器モデル情報を表示するサイトを選択します。サイト名またはその短縮コードを入力することで、サイトを検索できます。
3. 既存の機器モデルエンティティをレビューするか、新しいエンティティを作成します。

タスク	説明
既存の機器モデルのレビューと更新	セレクトターペインで、次のアクションを実行します。 a. 機器モデル階層を展開します。 b. 表示するエンティティをクリックします。
機器モデルエンティティの作成と詳細の入力	a. [新しいエンティティの作成] をクリックします。 b. [新しいエンティティを作成] フォームで、詳細を入力します。詳細については、「新しい機器モデルのエンティティを作成」を参照してください。

タスク	説明
	c. [Save (保存)] をクリックします。 d. 機器モデルビューの詳細フォームを使用して、新しい機器モデルエンティティの残りの詳細を入力します。

4. フォームで、フィールドを確認および更新します。

機器モデルの詳細フォーム

フィールド	説明
エンティティ名	機器モデルエンティティの名前。 i 注: 機器モデルエンティティが作成された後、[エンティティ名] フィールドを更新できます。このフィールドを更新すると、ツリーコンポーネントとサイトフィルターも更新されます。 詳細については、「機器モデルエンティティのエンティティ名または親を更新します」を参照してください。
親	この機器モデルエンティティの親であるエンティティの名前 (存在する場合)。このフィールドは、親を持たない最上位の親エンティティでは空です。最上位の親エンティティは、サイトと呼ばれます。 i 注: 機器モデルエンティティが作成された後、[親] フィールドを更新できます。 このフィールドを更新すると、ツリーコンポーネントとサイトフィルターも更新されます。詳細については、「機器モデルエンティティのエンティティ名または親を更新します」を参照してください。
テンプレート	手動で作成した機器モデルエンティティにアサインされた機器モデルテンプレート。 i 注: 統合ハブ ETL またはサードパーティ統合を使用してServiceNow AI Platform にインポートした機器モデルに機器モデルテンプレートをアサインすることはできません。
レベル	データのソートと構造化の目的で、選択した機器モデルテンプレートからアサインされる階層レベル。次に例を示します。 サイト 工業用地。

フィールド	説明
	エリア 工業用地内のエリア。 ワークセンター 産業現場のワークセンター。 機器モデルエンティティにアサインする機器レベルを検索して選択します。詳細については、「機器モデルテンプレートの階層ソートレベルの作成」を参照してください。
タイプ	機器モデルテンプレートレベルに割り当てられているレベルタイプの名前。たとえば、作業区レベルの品目組立や生産セルなどです。詳細については、「 機器モデルレベルタイプの作成 」を参照してください。
簡単な説明	この機器モデルエンティティとその目的の簡単な説明。
短縮コード	この機器モデルエンティティにアサインされた短縮コード。
パス	この機器モデルエンティティとそのすべての親エンティティの短縮コードの連結。例えば、ATL-B42-MQSTOR-Z1 は、以下のショート・コードを連結したものです。 ○ アトランタサイトの ATL 短縮コード。 ○ 建物 B42 の B42 短縮コード。 ○ モデル M および Q の MQSTORE 短縮コード。 ○ Model M および Q のゾーン1転送ストレージゾーンのZ1ショートコード。
場所	機器モデルエンティティの場所。たとえば、アトランタの建物 64 は、そこに配置されている各関連機器モデルの場所です。機器モデルエンティティにアサインする場所を検索して選択します。
会社	機器モデルエンティティに関連付けられている会社の名前。エンティティにアサインする会社を検索して選択します。
アサイン先	この機器モデルエンティティを操作および処理するアサインされたユーザー。エンティティにアサインするユーザーを検索して選択します。
管理担当者	このエンティティレコードを所有し、管理を担当するアサインされたユーザーの名前。機器モデルエンティティにアサインするユーザーを検索して選択します。
プロセスの重要度	機器モデルエンティティが産業プロセスにとってどの程度重要かを示す測定値。エンティティ

フィールド	説明
	のプロセスの重要度を選択します。たとえば、次のようになります。 ○ 1 - 最重要。 ○ 2 - ある程度重要。
サポートグループ	この機器モデルエンティティをサポートするグループの名前。機器モデルエンティティにアサインするユーザーグループを検索して選択します。
Managed by Group	このエンティティレコードを所有し、管理を担当するアサイン先グループの名前。エンティティにアサインするユーザーグループを検索して選択します。
会社	機器モデルエンティティが属する会社の名前。core_company値は、ServiceNow AI Platform内のCMDBに参照として保存されます。
運用ステータス	機器モデルエンティティの現在の運用ステータス: 稼働 本番プロセスで完全に運用可能なエンティティ。 非稼働 本番プロセスで稼働していないエンティティ。 未使用 運用中であるが意図的にオフラインになっているエンティティ。この値を使用して、ライセンスの目的に含めるサイトを指定できません。 [未使用] としてマークされたサイトは、産業用ワークスペースの機器モデルマネージャーには表示されません。

5. 以下の関連リストタブで、関連する機器モデルデータを確認します。

タスク	説明
機器モデル階層の表示	「 機器モデル階層の表示 」を参照してください。
機器モデルエンティティの上流生産プロセスをマッピングします。	a. [上流プロセス] をクリックします。 b. 詳細については、「選択した機器モデルエンティティの上流生産プロセスをマッピングします」を参照してください。

タスク	説明
機器モデルエンティティの下流生産プロセスをマッピングします。	a. [下流プロセス] をクリックします。 b. 詳細については、「選択した機器モデルエンティティの下流生産プロセスをマッピングします」を参照してください。
機器モデルエンティティの子エンティティを表示します。	a. [子エンティティ] をクリックします。 b. 詳細については、「機器モデルエンティティの子エンティティを確認する」を参照してください。
現在の機器モデルエンティティとその子エンティティに関連付けられている OT デバイスを表示します。	a. [マッピングされた OT デバイス] をクリックします。 b. 詳細については、「選択した機器モデルエンティティに関連付けられている OT デバイスを追加します」を参照してください。  注: デフォルトでは、このリストに OT コントロールモジュールは表示されません。

6. 機器モデルの詳細の確認と更新が完了したら、次のいずれかのアクションを実行します。

アクション	説明
更新された機器モデルエンティティを保存	[Save (保存)] をクリックします。
機器モデルエンティティを削除	[削除] をクリックします。

次のタスク

機器モデルエンティティとその子エンティティに関連付けられた OT データのロールアップを表示するには、機器モデルエンティティレコードの次の関連リストを使用します。ロールアップビューには、機器モデルエンティティの階層全体を自動化する OT デバイス、OT インシデント、OT 変更などが表示されます。

- マッピングされた OT デバイス
- OT インシデント
- OT 変更要求
- 脆弱性一致アイテム
- 修復タスク

新しい機器モデルのエンティティを作成

新しい機器モデルのエンティティを作成します。このタスクは、外部ソースから機器モデルデータをインポートするのではなく、ServiceNow AI Platform 内で直接新しい機器モデルエンティティを手動で作成する場合に実行します。

始める前に

必要なロール:cmdb_ot_isa_editor、cmdb_ot_isa_admin。

このタスクについて

cmdb_ot_isa_admin ロールがアサインされたユーザーは、任意のサイトの機器モデルエンティティを表示できます。ただし、cmdb_ot_isa_editor ロールが割り当てられているユーザーは、管理者が特定のユーザーにアクセス権を付与したサイトにのみアクセスできます。サイト アクセスの許可の詳細については、「[アドミニストレーター以外の機器モデルサイトアクセスの割り当てまたは削除](#)」を参照してください。

手順

1. 移動先 **すべて > 産業用ワークスペースアドミン > 産業用プロセスマネージャー > 機器モデルマネージャー**.
2. [機器モデルビュー対象] フィールドで、機器モデル情報を表示するサイトを選択します。サイト名またはその短縮コードを入力することで、サイトを検索できます。
3. [新しいエンティティの作成] を選択します。
4. [新しいエンティティを作成] ウィンドウで、親エンティティを検索して選択します。

i 注: 短縮コードまたは名前で親エンティティを検索できます。

5. フォームで、フィールドに入力します。

新しいエンティティの作成フォーム

フィールド	説明
親	このエンティティの親であるエンティティの名前 (存在する場合)。 現在選択されている機器モデルが親エンティティとして表示されます。親を変更するには、作成しているエンティティの親であるエンティティを検索して選択します。
エンティティ名	機器モデルエンティティの名前。
短縮コード	このエンティティにアサインされた短縮コード。
エンティティタイプ	機器モデルテンプレートレベルに割り当てられているレベルタイプの名前。たとえば、作業区レベルの品目組立や生産セルなどです。 エンティティタイプを検索して選択します。詳細については、「 機器モデルレベルタイプの作成 」を参照してください。

6. [Save (保存)] を選択します。
7. [詳細] フォームで、新しい機器モデルエンティティの残りの詳細を入力します。詳細については、「[機器モデルの詳細の確認と更新](#)」を参照してください。

機器モデル階層の表示

選択した機器モデルエンティティの階層構造と、生産プロセス内の他のエンティティとの関係をグラフィカルに表示します。

始める前に

必要なロール:cmdb_ot_isa_editor、cmdb_ot_isa_admin。

このタスクについて

cmdb_ot_isa_adminロールがアサインされたユーザーは、任意のサイトの機器モデルエンティティを表示できます。ただし、cmdb_ot_isa_editor または cmdb_ot_isa_viewer ロールが割り当てられているユーザーは、管理者が特定のユーザーにアクセス権を付与したサイトにのみアクセスできます。サイト アクセスの許可の詳細については、「[アドミニストレーター以外の機器モデルサイトアクセスの割り当てまたは削除](#)」を参照してください。

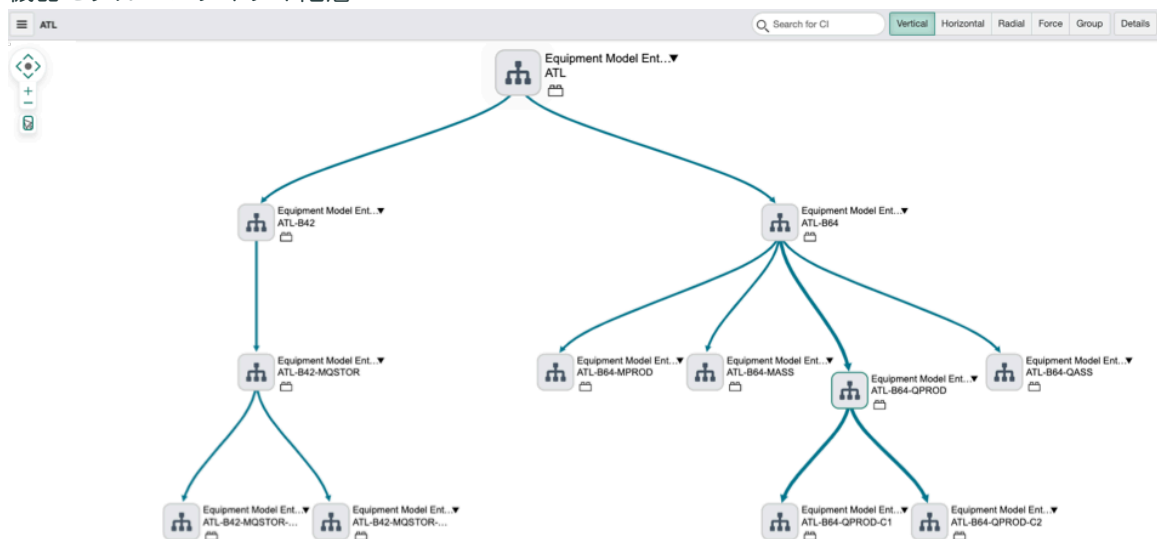
手順

1. 移動先 **すべて > 産業用ワークスペースアドミン > 産業用プロセスマネージャー > 機器モデルマネージャー**。
2. [機器モデル] ビューフィールドで、機器モデル情報を表示するサイトを選択します。
サイト名またはその短縮コードを入力することで、サイトを検索できます。
3. セレクターペインで、階層と他のエンティティとの関係をグラフィカルに表示する機器モデルエンティティをクリックします。
たとえば、サイト全体の表現を表示するには、トップレベルサイトエンティティをクリックします。
4. 機器モデルエンティティの階層構造を表示するには、[階層を表示] をクリックします。

結果

選択した機器モデルエンティティについて、次の図が表示されます。現在選択されている機器モデルは、階層内の親エンティティとして表示されます。

機器モデルエンティティ階層



機器モデルの表示 OT デバイスマップ

選択した機器モデルエンティティと、本番プロセス内の他の オペレーショナルテクノロジー (OT) デバイスとの関係をグラフィカルに表示します。

始める前に

必要なロール: cmdb_ot_isa_editor、cmdb_ot_isa_admin。

このタスクについて

cmdb_ot_isa_adminロールがアサインされたユーザーは、任意のサイトの機器モデルエンティティを表示できます。ただし、cmdb_ot_isa_editor または cmdb_ot_isa_viewer ロールが割り当てられているユーザーは、管理者が特定のユーザーにアクセス権を付与したサイトにのみアクセスできます。サイト アクセスの許可の詳細については、「[アドミニストレーター以外の機器モデルサイトアクセスの割り当てまたは削除](#)」を参照してください。

手順

1. 移動先 **すべて > 産業用ワークスペースアドミン > 産業用プロセスマネージャー > 機器モデルマネージャー**.
2. フィールド **の機器モードビュー** で、機器モデル情報を表示するサイトを選択します。
サイト名またはその短縮コードを入力することで、サイトを検索できます。
3. セレクターペインで、他のデバイスとの関係をグラフィカルに表現する機器モデルエンティティを選択します。
たとえば、サイト全体の表現を表示するには、トップレベルサイトエンティティを選択します。
4. 機器モデルエンティティとデバイスの関係を表示するには、[**OT デバイスマップを表示**] を選択します。

機器モデル **OT** 依存関係マップを表示

選択した機器モデルエンティティの階層構造と、生産プロセス内の他のエンティティおよびデバイスとの関係をグラフィカルに表示します。

始める前に

必要なロール:cmdb_ot_isa_editor、cmdb_ot_isa_admin。

このタスクについて

cmdb_ot_isa_adminロールがアサインされたユーザーは、任意のサイトの機器モデルエンティティを表示できます。ただし、cmdb_ot_isa_editor または cmdb_ot_isa_viewer ロールが割り当てられているユーザーは、管理者が特定のユーザーにアクセス権を付与したサイトにのみアクセスできます。サイト アクセスの許可の詳細については、「[アドミニストレーター以外の機器モデルサイトアクセスの割り当てまたは削除](#)」を参照してください。

手順

1. 移動先 **すべて > 産業用ワークスペースアドミン > 産業用プロセスマネージャー > 機器モデルマネージャー**.
2. フィールド **の機器モードビュー** で、機器モデル情報を表示するサイトを選択します。
サイト名またはその短縮コードを入力することで、サイトを検索できます。
3. セレクターペインで、階層および他のデバイスやエンティティとの関係をグラフィカルに表示する機器モデルエンティティを選択します。
たとえば、サイト全体の表現を表示するには、トップレベルサイトエンティティを選択します。
4. 機器モデルエンティティと他のデバイスやエンティティとの関係の階層構造を表示するには、[**OT 依存関係マップを表示**] を選択します。

選択した機器モデルエンティティの上流生産プロセスをマッピングします

上流プロセスを使用して、選択した機器モデルエンティティの上流生産プロセスをレビューします。機器モデルエンティティの新しい上流生産プロセスを作成してマッピングすることもできます。

始める前に

必要なロール:cmdb_ot_isa_editor、cmdb_ot_isa_viewer、cmdb_ot_isa_admin

このタスクについて

cmdb_ot_isa_adminロールがアサインされたユーザーは、任意のサイトの機器モデルエンティティを表示できます。ただし、cmdb_ot_isa_editor ロールが割り当てられているユーザーは、管理者が特定のユーザーにアクセス権を付与したサイトにのみアクセスできます。サイト アクセスの許可の詳細については、「[アドミニストレーター以外の機器モデルサイトアクセスの割り当てまたは削除](#)」を参照してください。

手順

1. 移動先 **すべて > 産業用ワークスペースアドミン > 産業用プロセスマネージャー > 機器モデルマネージャー**.
2. [機器モデル] ビューフィールドで、機器モデル情報を表示するサイトを選択します。
サイト名またはその短縮コードを入力することで、サイトを検索できます。
3. セレクターペインで、機器モデル階層を展開し、表示するエンティティをクリックします。
4. 機器モデルエンティティの上流生産プロセスを表示するには、[上流プロセス] をクリックします。
5. 機器モデルのアップストリーム生産プロセスをレビューするか、新しいモデルをマッピングします。

タスク	説明
選択した機器モデルエンティティの上流生産プロセスをレビューします	次のステップに進み、アップストリームプロセスフォームを確認します。
上流生産プロセスをマッピング	a. [追加] をクリックします。 b. [上流プロセスをマップ] フォームで、作成する新しい生産プロセスエンティティの名前を入力します。 c. [Save (保存)] をクリックします。
上流プロセスの削除	依存関係マップビューを使用します。 a. [プロセスの表示] をクリックします。 b. 削除する関係を右クリックします。 c. [関係を削除] をクリックします。 アップストリームプロセスレコードを使用します。 a. 削除するアップストリームプロセスの横にあるチェックボックスを選択します。 b. [削除] を選択します。 c. 確認メッセージで、[確認] を選択します。

6. [Submit (送信)] を選択します。

選択した機器モデルエンティティの下流生産プロセスをマッピングします

下流プロセスを使用して、選択した機器モデルエンティティの下流生産プロセスをレビューします。機器モデルエンティティの新しい下流生産プロセスを作成してマッピングすることもできます。

始める前に

必要なロール:cmdb_ot_isa_editor、cmdb_ot_isa_viewer、cmdb_ot_isa_admin

このタスクについて

cmdb_ot_isa_adminロールがアサインされたユーザーは、任意のサイトの機器モデルエンティティを表示できます。ただし、cmdb_ot_isa_editor ロールが割り当てられているユーザーは、管理者が特定のユーザーにアクセス権を付与したサイトにのみアクセスできます。サイト アクセスの許可の詳細については、「[アドミニストレーター以外の機器モデルサイトアクセスの割り当てまたは削除](#)」を参照してください。

手順

1. 移動先 **すべて > 産業用ワークスペースアドミン > 産業用プロセスマネージャー > 機器モデルマネージャー**.
2. [機器モデルビュー対象] フィールドで、機器モデル情報を表示するサイトを選択します。サイト名またはその短縮コードを入力することで、サイトを検索できます。
3. セレクターペインで、機器モデル階層を展開し、表示するエンティティをクリックします。
4. 機器モデルエンティティの下流生産プロセスを表示するには、[下流プロセス] をクリックします。
5. 機器モデルの下流生産プロセスをレビューするか、新しいモデルをマッピングします。

タスク	説明
選択した機器モデルエンティティの下流生産プロセスをレビューします	次のステップに進み、ダウンストリームプロセスフォームを確認します。
下流の生産プロセスをマッピングする	a. [追加] をクリックします。 b. [下流プロセスをマップ (Map Downstream Process)] フォームで、作成する新しい本番プロセスエンティティの名前を入力します。 c. [Save (保存)] をクリックします。
下流プロセスの削除	依存関係マップビューを使用します。 a. [プロセスの表示] をクリックします。 b. 削除する関係を右クリックします。 c. [関係を削除] をクリックします。 下流プロセスレコードを使用します。 a. 削除するダウンストリームプロセスの横にあるチェックボックスをオンにします。 b. [削除] を選択します。 c. 確認メッセージで、[確認] を選択します。

6. [Submit (送信)] を選択します。

機器モデルエンティティの子エンティティを確認する

選択した機器モデルエンティティに関連付けられている子エンティティを確認します。上位レベルのエンティティに従属する関連エンティティの関係を確認できます。

始める前に

必要なロール:cmdb_ot_isa_editor、cmdb_ot_isa_admin。

このタスクについて

cmdb_ot_isa_adminロールがアサインされている場合は、任意のサイトの機器モデルエンティティを表示できます。ただし、cmdb_ot_isa_editor ロールが割り当てられている場合、管理者がアクセスを許可したサイトにのみアクセスできます。サイト アクセスの許可の詳細については、「[アドミニストレーター以外の機器モデルサイトアクセスの割り当てまたは削除](#)」を参照してください。

手順

1. 移動先 **すべて > 産業用ワークスペースアドミン > 産業用プロセスマネージャー > 機器モデルマネージャー**.
2. [機器モデルビュー対象] フィールドで、機器モデル情報を表示するサイトを選択します。サイト名またはその短縮コードを入力することで、サイトを検索できます。
3. セレクターペインで、機器モデル階層を展開し、表示するエンティティを選択します。
4. 子エンティティを作成するには、新しいエンティティの作成 ボタンを選択し、新しいエンティティの作成 フォームに詳細を入力します。
詳細については、「[新しい機器モデルのエンティティを作成](#)」を参照してください。
5. 機器モデルエンティティの子エンティティを表示するには、[子エンティティ] を選択します。
6. さらに、[関連リスト] セクションでは、[処理順序] フィールドに値を割り当てて、特定のサイトの子エンティティに優先順位を付けることができます。

i 注: [処理順序] 値を使用すると、重要性和機能に従って子エンティティをソートし、優先順位を付けることができます。

- 機器モデル階層では、処理順序の値が低いほど優先されます。1 つ以上の子エンティティに割り当てられた値が同じ場合、子エンティティはアルファベット順にソートされます。
- Industrial Workspace の [機器モデル] メニューでは、機器モデルエンティティの階層は、子エンティティにアサインされた [処理順序] の値に基づきます。
- [OT リスク管理] タブでは、すべての機器モデルエンティティは、子エンティティにアサインされた [処理順序] の値に従って順番に表示されます。

選択した機器モデルエンティティに関連付けられている **OT** デバイスを追加します

OT デバイスを使用して、選択した機器モデルエンティティとその子エンティティに関連付けられている OT デバイスを確認します。他の OT デバイスを選択して、選択した機器モデルエンティティに関連付けることもできます。

始める前に

選択した機器モデルエンティティに追加の OT デバイスに関連付けるには、オペレーショナルテクノロジーマネージャー アプリケーションと 製造業プロセスマネージャー アプリケーションの両方をインストールする必要があります。

必要なロール:OT デバイスを追加するには、ログインユーザーに次のロールがアサインされている必要があります。

- cmdb_ot_viewer、cmdb_ot_editor、または cmdb_ot_admin ロール
- cmdb_ot_isa_editorまたはcmdb_ot_isa_adminロール

i 注: ユーザーロールの割り当ての詳細については、「[製造業プロセスマネージャーユーザーロールのアサイン](#)」を参照してください。

このタスクについて

cmdb_ot_isa_adminロールがアサインされたユーザーは、任意のサイトの機器モデルエンティティを表示できます。ただし、cmdb_ot_isa_editor または cmdb_ot_isa_viewer ロールが割り当てられているユーザーは、管理者が特定のユーザーにアクセス権を付与したサイトにのみアクセスできます。サイト アクセスの許可の詳細については、「[アドミニストレーター以外の機器モデルサイトアクセスの割り当てまたは削除](#)」を参照してください。

手順

1. 移動先 **すべて > 産業用ワークスペースアドミン > 産業用プロセスマネージャー > 機器モデルマネージャー**.
サイト名またはその短縮コードを入力することで、サイトを検索できます。
2. [機器モデル] ビューフィールドで、機器モデル情報を表示するサイトを選択します。
3. セレクターペインで、機器モデル階層を展開し、表示するエンティティをクリックします。
4. 機器モデルエンティティとその子エンティティに関連付けられた OT デバイスを表示するには、[マッピングされた **OT** デバイス] をクリックします。
5. 関連する OT デバイスを確認するか、選択した機器モデルエンティティに追加の OT デバイスを関連付けます。

タスク	説明
選択した機器モデルエンティティに関連付けられた OT デバイスをレビューします	次のステップに進み、OT デバイスフォームを確認します。
選択した機器モデルエンティティに追加の OT デバイスを関連付けます	a. [追加] をクリックします。 b. OT デバイスフォームで、機器モデルエンティティに関連付ける追加の OT デバイスを選択します。 c. [追加] をクリックして、OT デバイスフォームに追加します。 d. テーブルの列を編集するには、[リストアクション] () アイコンを選択します。[列の編集] を選択して、表示する列を選択します。たとえば、OT デバイスの [IP アドレス] 列を表示する場合は、[利用可能] 列から [IP アドレス] を選択し、[OK] をクリックします。
選択した機器モデルエンティティから OT デバイスを削除します	a. [マッピングされた OT デバイス] リストビューで、削除する OT デバイスを選択します。 b. [削除] をクリックします。

6. [保存] をクリックします。

機器モデルエンティティのエンティティ名または親を更新します

必要に応じて機器モデルエンティティレコードのエンティティ名または親フィールドを更新して、機器モデル情報を最新の状態に保ちます。

始める前に

必要なロール:cmdb_ot_isa_editor

手順

1. 移動先 **すべて > 産業用ワークスペース**.
2. 機器モデル () ボタンを選択します。

または、すべて > 産業用ワークスペースアドミン > 産業用プロセスマネージャー > 機器モデルマネージャー。

3. 更新する機器モデルエンティティレコードを選択します。
4. 必要に応じて、[エンティティ名] フィールドまたは [親] フィールドを更新します。
5. **[Save (保存)]** を選択します。

結果

[エンティティ名] または [親] フィールドを更新すると、機器モデルマネージャーのツリーコンポーネントのフィールドと、産業用ワークスペースのオペレーショナルテクノロジー (OT) ランディングページのサイトフィルターのフィールドも更新されます。

サイトのオペレーショナルテクノロジー脆弱性対応 アサイン先グループの一括編集

一括編集機能を使用して、複数のサイトレコードのオペレーショナルテクノロジー脆弱性対応 (OT VR) アサイン先グループフィールドを一度に更新します。

始める前に

必要なロール:cmdb_ot_isa_admin

手順

1. 移動先 **すべて > 産業用ワークスペース**。
2. リスト () ビューを開きます。
3. 産業用プロセスマネージャーモジュールで、[サイト] リストを選択します。
4. 編集する各 OT サイトの横にあるチェックボックスをオンにします。
5. **[編集]** ボタンを選択します。
6. **[OT VR アサイン先グループ]** フィールドで、選択したサイトのオペレーショナルテクノロジー脆弱性対応アサイン先グループを追加します。
7. **[Update (更新)]** を選択します。

結果

選択したサイトごとに **[OT VR アサイン先グループ]** フィールドが更新されます。

機器モデルエンティティの検索

エンティティをより迅速かつ効率的に見つけることができるように、産業用ワークスペース内の機器モデルエンティティを検索します。

始める前に

必要なロール:cmdb_ot_isa_editor

手順

1. 移動先 **すべて > 産業用ワークスペース**。
2. 機器モデルマネージャー () アイコンを選択します。

3. 検索バーで、表示する機器モデルエンティティを検索します。

Show Favorites ☐

Search
🔍

▼ Atlanta

> Finished Goods Storage Area ☆

> Manufacturing Area ☆

結果

リストが自動的に展開され、検索された機器モデルエンティティが表示されます。[お気に入りを表示] 切り替えをオンにしても、リストは展開され、検索された機器モデルエンティティが表示されません。

管理対象ネットワーク別にすべての **OT** デバイスを表示

ServiceNow AI Platform 上の管理対象ネットワーク別に オペレーショナルテクノロジー (OT) デバイスを表示します。

始める前に

必要なロール:cmdb_ot_isa_viewerおよびcmdb_ot_viewer

このタスクについて

ServiceNow AI Platform の [管理対象ネットワーク別のすべての OT デバイス] リストは、次のテーブルからデータが入力されたデータベースビューです。

- OT エンティティ [cmdb_ot_entity]
- 構成アイテム [cmdb_ci]
- 構成アイテムの関係 [cmdb_rel_ci]
- 割り当て済み IP アドレス [cmdb_ci_allocated_ip_address]
- IP ネットワークサブネット [cmdb_ci_ip_network_subnet]
- 管理対象ネットワーク [cmdb_ci_managed_network]

[管理対象ネットワーク別のすべての OT デバイス (All OT Devices by Managed Network)] リストを使用すると、OT デバイスとそのネットワークの関係を理解するのに役立ちます。

OT デバイスネットワーク接続データモデルの詳細については、「[オペレーショナルテクノロジー \(OT\) 拡張クラス](#)」の「**OT** デバイスネットワーク接続データモデル」セクションを参照してください。

手順

1. 移動先 すべて > 産業用ワークスペースアドミン > 産業用プロセスマネージャー.
2. 管理対象ネットワーク別のすべての **OT** デバイスを選択します。
3. リストでは、次の情報を表示できます。

[管理対象ネットワーク別のすべての **OT** デバイス] フィールド

フィールド	説明
管理対象ネットワーク	OT デバイスが属する管理対象ネットワークの名前。
IP ネットワークサブネット名	OT デバイスが属する特定の IP サブネットの識別子。
デバイスの IP アドレス	通信とデバイス管理に使用される OT デバイスにアサインされた IP アドレス。
OT デバイス	OT デバイスの名前。
親管理対象ネットワーク	現在の管理対象ネットワークを含む、または監督する上位レベルの管理対象ネットワーク。

運用ステータスで機器モデルエンティティをフィルター

システムプロパティを使用して、産業用ワークスペースの機器モデルマネージャーで機器モデルエンティティがどのように表示されるかをフィルタリングします。機器モデルエンティティをフィルタリングすると、産業用ワークスペースに表示されるデータを整理するのに役立ちます。

始める前に

必要なロール:cmdb_ot_isa_viewerおよびcmdb_ot_isa_admin

手順

1. 移動先 すべて > 機器モデル: **ISA** > システムプロパティ.
2. [機器モデルページからフィルターで除外する必要がある機器モデルの運用ステータスのリスト] で、産業用ワークスペースビューから削除する機器モデルエンティティを運用ステータス別に一覧表示します。

次のオプションから選択できます。

- 運用 = 1
- 非稼働 = 2
- 修理中 = 3
- DR スタンバイ = 4
- 準備完了 = 5
- 廃止 = 6
- パイプライン = 7
- カタログ = 8
- 未使用 = 9

たとえば、[運用ステータス] フィールドの値が [廃止] および[未使用] である機器モデルエンティティを削除する場合は、リスト 6、9 を使用します。

子機器モデルエンティティをお気に入りに追加

産業用ワークスペースの機器モデルマネージャーで子機器モデルエンティティをお気に入りに登録して、作業中にお気に入りのカスタマイズされたビューにアクセスできるようにします。

始める前に

必要なロール：admin

手順

1. 移動先 **すべて > 産業用ワークスペース**.

2. 機器モデルマネージャー () アイコンを選択します。

3. お気に入りに追加する子機器モデルエンティティの横にある、お気に入りとしてマーク (☆) アイコンを選択します。

i 注：ISA サイトをお気に入りとして選択することはできません。

上位レベルのエンティティをお気に入りとして選択した場合、その下にある関連する子エンティティは表示されません。ただし、下位レベルの子エンティティを選択すると、親エンティティを含む完全な階層が表示されます。

4. オプション：お気に入りから子エンティティを削除するには、[お気に入りから削除] (★) アイコンを選択します。

結果

必要に応じて、子機器モデルエンティティがお気に入りに追加されます。

お気に入りの子機器モデルエンティティのみを表示するには、[お気に入りを表示] トグルを選択してオンに切り替えます。[お気に入りを表示] トグルは、お気に入りに追加された子エンティティに UI ビューを集中させ、機器モデルマネージャーで変更を加えながら順調に進めるのに役立ちます。

[お気に入りを表示] トグルをオンにすると、設定が保存されます。ログアウトしてから再度ログインするか、別のサイトを開いても、[お気に入りを表示] トグルはオンのままです。

機器モデルへの **OT** デバイスの自動マッピング

OT デバイスから本番プロセスへのマッピングを自動化します。

OT マネージャーが脆弱性に遭遇した場合、または OT デバイスに関連するワークフローを管理する必要がある場合、OT デバイスが自動化する本番プロセスにどのように接続するかというコンテキストは、作業の優先順位付けに重要です。OT デバイスを ISA 機器モデルエンティティに自動マッピングすることで、デバイスとプロセス間の関係を表示できます。

i 注：サイトごとに 1 つのサブネット範囲のみがサポートされています。2 つの異なるサイトが同じサブネットを持つことができます。例: 192.168.101.0/24。ただし、同じ範囲の複数のサブネットは、同じサイトではサポートされていません。このシナリオでは、手動マッピングを使用することをお勧めします。

主な特長

- 信頼できるソース (NetDB やファイアウォールなど) から OT サブネットを ServiceNow インスタンスのレコードとしてアップロードして保存します。
- IP アドレスと OT サブネットを使用して、ISA エンティティへの OT デバイスのアサインを自動化します
- 複数のサイトでプライベート IP アドレス範囲を再利用する場合の問題を最小限に抑える

産業用ネットワークでは、サブネットを使用してプライベート IP アドレス空間を 1 つのサブネットに分割し、多くの場合、生産プロセスの一部または機器モデルエンティティに配置します。例: 缶詰ラインは 192.168.101.0/24 ネットワーク上で動作し、すべての機器がインテグレーターによってプログラムされています。制御システム (OT デバイス) で使用される IP は、多くの場合、ラインの実行に使用される自動化ソフトウェアにハードコードされています。サブネットがアトランタサイトの缶詰ラインにマッピングされている場合、マネージャーは IP 192.168.101.66 を持つ検出された PLC を缶詰ラインに自動的にマッピングできます。

マッピング機能は、各サブネットを機器モデルエンティティに関連付けるため、OT 認定統合または ServiceNow の [OT ネットワークの IT ディスカバリー](#) からのインポート時に報告された IP アドレスに基づいて、機器モデルエンティティに関連付けられたサブネットに OT デバイスを自動的にマッピングできます。

システムアドミニストレーターは、OT サブネットマッピングレコードをインポートできます。ISA アドミニストレーターは、スケジュール済みジョブフローを使用して、機器モデルエンティティへのサブネットのマッピングを自動的に作成できます。ISA エディターは、個々の OT デバイスのマッピングをオンデマンドで手動で作成できます。

自動マッピング機能のペルソナ

自動マッピング機能は、次のペルソナを対象としています。

自動マッピングのペルソナ

ペルソナ	説明
システムアドミン	システム管理者は次のタスクを実行します。 - データを OT サブネットから機器モデルエンティティへのマッピングテーブルにインポートします - OT サブネットマッピングのスケジュール済みフローをアクティブ化、スケジュール、または手動でトリガーします
ISA アドミン	ISA アドミンは、[OT サブネットマッピング] リストビューから [すべての OT デバイスをマッピング] UI アクションを手動でトリガーします。
ISA エディター	ISA エディターは次のタスクを実行します。 - 特定のサイトの OT サブネットマッピングエントリを手動で作成して更新します - 個々の OT デバイスを OT デバイスレコードから機器モデルエンティティにマッピングします - OT サブネットマッピングレコードから機器モデルエンティティに複数の OT デバイスをマッピングします

プラグイン

マッピング機能を有効にするには、次のプラグインが必要です。

- オペレーショナルテクノロジーマネージャー
- 製造業プロセスマネージャー

必要なプラグインがインストールされている場合、ISA アドミニストレーターは 製造業プロセスマネージャー アプリケーションメニューからサブネットマッピング機能にアクセスできます。

自動マッピング機能のワークフロー

製造業プロセスマネージャーには、自動マッピング機能の自動フローが含まれています。

この機能には事前定義されたフローが含まれており、これを使用して機器モデルエンティティへの OT デバイスのアサインをスケジュールできます。

フローデザイナー  を使用すると、ビジネスニーズに合わせて事前定義されたフローを確認および設定できます。

この機能で利用可能なフロー

次の表に、オペレーショナルテクノロジーマネージャー とともにインストールしたときに 製造業プロセスマネージャー で使用できる事前定義されたフローを示します。

アプリケーション	フロー
製造業プロセスマネージャー 一緒にインストールする場合 オペレーショナルテクノロジーマネージャー	OT デバイスマッピングフロー

自動マッピング機能の一般的なユースケース

通常、自動マッピング機能には次のユースケースが適用されます。

- OT マネージャーが既存の OT デバイスを所有しており、個々の OT デバイスをオンデマンドでマッピングしたいと考えています。
- OT アドミンは、有効な IP アドレスを持つ新しく検出された OT デバイスを機器モデルエンティティに自動的にマッピングしたいと考えています。

自動マッピング機能の一般的なワークフローは次のとおりです。

- システムアドミンは、**Easy Import**  を使用して、Excel スプレッドシートから OT サブネットデータを OT サブネットマッピングテーブルにインポートします。
- Amazing アドミニストレーターがインポートされたデータレコードをレビューし、OT サブネットマッピングレコードをサイトまたはそのサイト内の機器モデルエンティティに関連付け (マップ) します。
- Amazing アドミニストレーターは、スケジュールされたフローをアクティブ化またはトリガーして、インスタンス上のすべてのサイトの OT デバイスを自動的にマッピングします。
- 優れたエディターは、編集アクセス権を持つサイトに属するレコードを更新できます。

ガイド付きセットアップを使用した **OT** デバイスの自動マッピングの構成

製造業プロセスマネージャーガイド付きセットアップを使用して、OT デバイスを ISA 設備階層モデルエンティティに自動的にマッピングします。

始める前に

必要なロール：admin

このタスクについて

admin ロールを持っている場合は、製造業プロセスマネージャー ガイド付きセットアップを使用して、OT デバイスを ISA 機器モデルエンティティにマッピングする手順を確認できます。アクセス権を持つサイトの OT デバイスをマッピングできます。

手順

1. 移動先 **すべて > 産業用ワークスペースアドミン > ガイド付きセットアップ**。
2. 製造業プロセスマネージャー アプリケーションで **[開始]** を選択します。
3. **[OT デバイスを自動的にマッピング]** タスクを選択します。
4. 次のタスクタブを選択し、**[構成]** を選択して構成タスクを完了します。

タスク	目的
OT サブネットのインポート	OT サブネットのスプレッドシートをアップロードして、ネットワーク管理プラットフォームからサブネットをインポートします。
サイトを追加	OT サブネットレコードと一致する IP アドレスを持つ OT デバイスをそのサイトに自動的にマッピングできるように、各 OT サブネットにサイトを追加します。
機器モデルエンティティを追加	機器モデルエンティティを OT サブネットレコードに追加すると、OT デバイスが機器モデルエンティティに自動的に関連付けられます。
ディスカバリーソースを選択	次の OT サブネットマッピングシステムプロパティを構成して、OT サブネットマッピングで考慮されるディスカバリーソースを制限します。 ◦ <code>sn_otsm.map_all_ot_devices.all_discovery_sources</code> ◦ <code>sn_otsm.map_all_ot_devices.discovery_sources</code>
テストマッピング	個々の OT デバイス、個々の OT サブネット、選択された複数の OT サブネット、またはすべてのアクティブな OT サブネットのアサインされたマッピングを検証します。
アクティブ化してスケジュール	スケジュール済みフローをアクティブ化して、すべての OT デバイスのスケジュール済みマッピングを定期的に行います。個別にトリガーできるサブフローは 2 つあります。 ◦ サイトを OT デバイスにアサインするサブフロー ◦ OT デバイスをサイトにマッピングするためのサブフロー

関連トピック

[ガイド付きセットアップ](#)

[機器モデルへの OT デバイスの自動マッピング](#)

すべての **OT** デバイスを機器モデルエンティティに自動的にマッピング

オペレーショナルテクノロジー (OT) 優れたアドミンは、すべての OT デバイスから適切な ISA 機器モデルエンティティへの自動マッピングをトリガーできます。

始める前に

次のプラグインをインストールする必要があります。

- [オペレーショナルテクノロジーマネージャー](#)
- [製造業プロセスマネージャー](#)

必要なロール:sn_ot_amazing_admin

手順

1. 移動先 産業用ワークスペースアドミン > 産業用プロセスマネージャー > **OT** サブネットマッピング.
2. [すべての **OT** デバイスをマッピング] を選択して、[OT デバイスをマッピング] フローを実行します。

結果

OT デバイスは、すべてのアクティブな OT サブネットマッピングレコードにリストされている機器モデルエンティティに自動的にマッピングされます。マッピングがトリガーされた後、リストビューから情報メッセージで利用可能なリンクを選択して、マッピング結果を表示できます。

- i** 注: サブネットマッピングは ディスカバリー ISA 機器モデルに対して作成された構成アイテム (CI) もサポートしています。

サブネット内のすべての **OT** デバイスをマッピング

OT アドミンは、選択したサブネット内のすべての OT デバイスの自動マッピングをトリガーできます。

始める前に

次のプラグインをインストールする必要があります。

- [オペレーショナルテクノロジーマネージャー](#)
- [製造業プロセスマネージャー](#)

必要なロール:sn_ot_amazing_write

手順

1. 移動先 産業用ワークスペースアドミン > 産業用プロセスマネージャー > **OT** サブネットマッピング.
2. [OT サブネットマッピング] リストから、デバイスをマッピングする OT サブネットマッピングレコードを開きます。

- i** 注: サブネットマッピングは ディスカバリー ISA 機器モデルに対して作成された構成アイテム (CI) もサポートしています。

3. [サイト] フィールドと [機器モデルエンティティ] フィールドが正しく入力されていることを確認します。
4. このサイトのすべての OT デバイスを選択した OT サブネットの IP アドレスに自動的にマッピングするには、[このサブネットの **OT** デバイスをマッピング] UI アクションを選択します。

結果

選択した IP 範囲内の IP アドレスを持つ OT デバイスが選択したサイトにある場合、サイト内のすべてのデバイスが OT サブネットにマッピングされます。マッピングがトリガーされた後、リストビューから情報メッセージで利用可能なリンクを選択して、マッピング結果を表示できます。

サイトにアサインされていない **OT** デバイスを表示する

サイトにアサインされていない オペレーショナルテクノロジー (OT) デバイスのリストを表示します。

始める前に

次のプラグインをインストールする必要があります。

- [オペレーショナルテクノロジーマネージャー](#)
- [製造業プロセスマネージャー](#)

必要なロール:cmdb_ot_isa_editorおよびcmdb_ot_editor

このタスクについて

OT デバイスマッピングの一環として、機器モデルエンティティにマッピングする前に、デバイスをサイトにアサインする必要があります。これを行うには、サイトにアサインされていないすべての OT デバイスのリストを表示できます。

手順

1. 移動先 **すべて > オペレーショナルテクノロジー (OT) > サイトアサインのない OT デバイス**。
2. デバイスをサイトに個別に割り当てるには、デバイスレコードを選択して [サイト] フィールドを更新します。
3. 一括編集を実行して [サイト] 列を更新し、複数のデバイスを同じサイトに割り当てるには、次の手順を実行します。
 - a. サイトにアサインする各 OT デバイスの横にあるチェックボックスをオンにします。
 - b. [サイト] 列ヘッダーで、[列オプション] ボタンを選択し、[選択項目の更新] を選択します。
 - c. [サイト] フィールドを更新します。
 - d. **[Update (更新)]** を選択します。

次のタスク

OT デバイスはサイトにアサインされますが、機器モデルエンティティにはマッピングされません。マッピングされていない OT デバイスのリストを表示して、デバイスマッピングを完了できます。詳細については、「[マッピングされていない OT デバイスを表示する](#)」を参照してください。

マッピングされていない **OT** デバイスを表示する

機器モデルエンティティにマッピングされていない IP アドレスを持つ オペレーショナルテクノロジー (OT) デバイスのリストを表示します。

始める前に

次のプラグインをインストールする必要があります。

- [オペレーショナルテクノロジーマネージャー](#)
- [製造業プロセスマネージャー](#)

必要なロール:cmdb_ot_isa_editorおよびcmdb_ot_editor

手順

1. 移動先 **すべて** > 産業用ワークスペース.
2. 産業用 ワークスペースリストビューのオペレーショナルテクノロジー (OT) モジュールの下で、[マッピングされていない OT デバイス] リストを選択します。
このリストには、IP アドレスと、アサインされたサイトの機器モデルエンティティにマッピングするために使用できるその他のフィールドを含む OT デバイスレコードが表示されます。
3. オプション: [サイト] 列ヘッダーで [フィルター] ボタンを選択し、[サイトでグループ化] を選択します。
このフィルターを使用すると、マッピングされていない OT デバイスをサイト別に整理できます。複数のサイトを管理する場合に役立ちます。

次のタスク

これで、OT デバイスを機器モデルエンティティにマッピングできるようになりました。詳細については、「[個々の OT デバイスを機器モデルエンティティにマッピングする](#)」を参照してください。

個々の OT デバイスを機器モデルエンティティにマッピングする

アクセス権を持つサイトの ISA 機器モデルエンティティへの OT デバイスのオンデマンドマッピングを実行します。

始める前に

次のプラグインをインストールする必要があります。

- [オペレーショナルテクノロジーマネージャー](#)
- [製造業プロセスマネージャー](#)

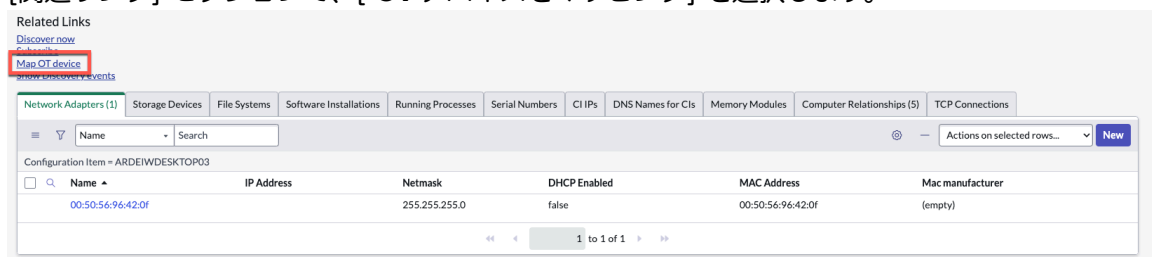
必要なロール:sn_ot_amazing_writeおよびcmdb_ot_viewer

手順

1. 移動先 **すべて** > オペレーショナルテクノロジー (OT) > すべての OT デバイス.
2. [OT デバイス] 列で、マッピングする OT デバイスを選択します。

i 注: サブネットマッピングは ディスカバリー ISA 機器モデルに対して作成された構成アイテム (CI) もサポートしています。

3. [関連リンク] セクションで、[OT デバイスをマッピング] を選択します。



結果

選択したデバイスの IP アドレスとサイトに一致するアクティブな OT サブネットがある場合、そのデバイスはマッピングされます。

OT サブネットマッピングのスケジュール済みフローの構成

OT デバイスをサイトと機器モデルエンティティに自動的にマッピングするように OT デバイスマッピングフローを構成します。

始める前に

次のプラグインをインストールする必要があります。

- オペレーショナルテクノロジーマネージャー
- 製造業プロセスマネージャー

必要なロール：admin

このタスクについて

OT デバイスマッピングフローをスケジュールに基づいて実行するように設定して、すべてのアクティブな OT サブネットマッピングレコードの OT デバイスを自動的にマッピングできます。

手順

1. 移動先 産業用ワークスペースアドミン > 産業用プロセスマネージャー > **OT** サブネットマッピングのスケジュール済みフロー。
2. オプション：サイトマッピングをアクティブ化します。
 - a. [フロー変数の設定] セクションを開きます。
 - b. [自動アサインサイトの実行] の横にあるチェックボックスをオンにして、[保存] を選択します。
3. フローを定期的に行うようにスケジュールするには、[トリガー] セクションのリンクを選択して間隔を定義します。
4. ヘッダーで [アクティブ化] を選択して、スケジュールされた OT デバイスマッピングフローの実行をアクティブ化します。
アクティブ化した後、このフローをスケジュールに基づいて実行して、インスタンス上のすべてのアクティブな OT サブネットマッピングレコードの OT デバイスを自動的にマッピングできます。

i 注：サブネットマッピングは ディスカバリー ISA 機器モデルに対して作成された構成アイテム (CI) もサポートしています。

OT サブネットマッピングの表示

機器モデルエンティティにアサインされているすべてのマッピング済み OT サブネットを表示します。

始める前に

必要なロール：

- sn_ot_amazing_write、cmdb_ot_isa_editor、および cmdb_ot_viewerまたは
- sn_ot_amazing_admin、cmdb_ot_isa_editor、cmdb_ot_viewer

手順

1. 次のいずれかのオプションを使用して、機器モデルマネージャーに移動します。
 - 移動先 すべて > 産業用ワークスペースアドミン > 産業用プロセスマネージャー > 機器モデルマネージャー。
 - 移動先 すべて > 産業用ワークスペース. 機器モデル () アイコンを選択します。
2. 機器モデルビューからサイトを選択するか、機器モデル階層を展開してマッピングを表示するエンティティを選択します。
3. エンティティフォームで、[マッピングされた **OT** サブネット] 関連リストタブを選択します。

マッピングされた OT サブネットは、アクティブまたは非アクティブとして表示されます。アクティブな OT サブネットのみが スケジュール済みフローに含まれます。詳細については、「[OT サブネットマッピングのスケジュール済みフローの構成](#)」を参照してください。

4. オプション: OT デバイスレベルでマッピングに使用される OT サブネットを表示するには、OT デバイスレコードで [**OT サブネット**] 関連リストを選択します。

次のタスク

新しい OT サブネットマッピングレコードを作成します

新しい **OT** サブネットマッピングレコードを作成します

機器モデルエンティティに関連付ける新しい OT サブネットマッピングを作成します。

始める前に

必要なロール:sn_ot_amazing_write または sn_ot_amazing_admin

- i** 注: 新しい OT サブネットマッピングレコードを作成すると、デフォルトでは新しいレコードは非アクティブになります。OT デバイスマッピングフローがトリガーされたときにレコードを自動的にマッピングするには、OT サブネットマッピングレコードをアクティブにする必要があります。

手順

1. 移動先 産業用ワークスペースアドミン > 産業用プロセスマネージャー > 機器モデルエンティティ。
2. 新しいマッピングを作成するサイトまたは機器モデルエンティティを選択します。

- i** 注: サブネットマッピングは ディスカバリー ISA 機器モデルに対して作成された構成アイテム (CI) もサポートしています。

3. [マッピングされた **OT** サブネット] 関連リストを選択し、[新規] を選択します。

4. フォームで、フィールドに入力します。

OT サブネットから機器モデルへのエンティティマッピングフォーム

フィールド	説明
名前	サブネットのゾーンまたは VLAN 名。
サイト	ルックアップで、利用可能なサイトのリストから ISA サイトを選択します (まだ入力されていない場合)。
タイプ	次のオプションからサブネットタイプを選択します。 • IP 範囲 - サブネット内の IP アドレスのサブセット • IP ネットワーク - サブネット全体 (CIDR 表記)
開始 IP アドレス	IP 範囲の開始 IP このフィールドは、[タイプ] が [IP 範囲] の場合にのみ表示されます。
終了 IP アドレス	IP 範囲の終了 IP

フィールド	説明
	このフィールドは、[タイプ] が [IP 範囲] の場合に 表示されます。
ソース名	ソースの名前 (NetDB やファイアウォールな ど)。
ファイアウォール名	ゾーンを管理するファイアウォールの名前 (該当 する場合)。
説明	サブネットマッピングの説明。
アクティブ	[アクティブ] を選択すると、OT サブネット マッピングのスケジュール済みフローの実行時 にサブネットが自動マッピングに含まれます。
設備モデルのエンティティ	ルックアップで、使用可能なエンティティのリ ストから機器モデルエンティティを選択します (まだ入力されていない場合)。
サブネット	サブネットアドレス (CIDR 形式) を入力しま す。このフィールドは、[タイプ] が [IP ネット ワーク] の場合に表示されます。
場所	サブネットレコードに場所を追加して、マッピ ングされた OT デバイスの場所を自動的に追加 または更新します。  注: 場所 は、sn_otsm.subnet_mapping.location_auto_update システムプロパティに基づいてマッピング されます。OT サブネットマッピングに使用 されるシステムプロパティの詳細につい ては、「OT サブネットマッピング機能で 使用されるシステムプロパティ」を参照し てください。
インターフェイス名	該当する場合、ファイアウォールインターフェ イスの名前。
VLAN ID	該当する場合は、VLAN ID を指定します。

5. [Submit (送信)] を選択します。

マッピングされたすべての **OT** デバイスを表示

機器モデルエンティティにマッピングされているすべての オペレーショナルテクノロジー (OT) デバイスのリストを表示します。

始める前に

必要なロール:sn_ot_amazing_write または sn_ot_amazing_admin

このタスクについて

CI 関係性テーブルで親レコードを開くと、[マッピングされた OT デバイス] 関連リストを表示できます。関連リストは、親 ISA 設備階層モデルエンティティを開いた後に、子 ISA 設備階層モデルエンティティにマッピングされているすべてのデバイスを表示するロールアップビューです。これには、機器モデルエンティティとデバイス間のマッピングを表すレコードが含まれています。

手順

1. マッピングされた OT デバイスを 産業用ワークスペースに表示するには、次のアクションを完了します。
 - a. 産業用ワークスペース に移動します。
 - b. 機器モデル () アイコンを選択します。
 - c. マッピングされたデバイスを表示する機器モデルエンティティを開きます。
 - d. **[Mapped OT Devices (マッピングされている OT デバイス)]** タブを選択します。

i 注: [マップされた機器モデルエンティティ] 列には、デバイスがマッピングされている機器モデルエンティティが表示されます。デバイスを複数の機器モデルエンティティにマッピングできます。

2. マッピングされた OT デバイスを ServiceNow AI Platformに表示するには、次に移動します: すべて > 産業用ワークスペースアドミン > 産業用プロセスマネージャー > マッピングされた **OT** デバイス。

このリストには、さまざまな機器モデルエンティティにマッピングされているすべてのデバイスが含まれています。[自動化基準:: 自動化 CI 関係] は、親エンティティと子エンティティに適用されます。

このリストでは、[マップされた機器モデルエンティティ] 列を使用して、デバイスがマッピングされている機器モデルエンティティを特定できます。リストに列を追加する方法の詳細については、「 [リストのカスタマイズ](#) 」を参照してください。

OT サブネットマッピング機能で使用するシステムプロパティ

優れたアドミンは、OT サブネットマッピング機能をサポートするシステムプロパティを表示および設定できます。

Amazing Admin ロールを持つユーザーは、次の場所に移動して OT サブネットマッピングプロパティ設定にアクセスできます 産業用ワークスペースアドミン > 産業用プロセスマネージャー > **OT** サブネットマッピングプロパティ。

OT サブネットマッピングのシステムプロパティ

プロパティ	説明
<code>sn_otsm.map_all_ot_assets.all_discovery_sources</code>	すべてのディスカバリーソースの OT デバイスのマッピングを制御します。すべてのディスカバリーソースの OT デバイスをマッピングします。オンにすると、以下の特定のディスカバリーソースが上書きされます。デフォルトは [はい] (true) です。 デフォルト値: True
<code>sn_otsm.map_all_ot_assets.discovery_sources</code>	指定されたディスカバリーソースの OT デバイスをマッピングします (カンマ区切り形式)。上記の [すべてのディスカバリーソースの OT デバイスをマッピング] がオフの場合にのみ適用されます。
<code>sn_otsm.subnet_mapping.auto_assign_ot_owners</code>	Owner-Owned by 関係に基づいて、すべての OT コントロールモジュールを機器モデルエン

OT サブネットマッピングのシステムプロパティ (続く)

プロパティ	説明
	ティティに自動的にアサインします。デフォルトは [はい] (true) です。
<code>sn_otsm.subnet_mapping.location_auto_update</code>	OT デバイスの場所をサブネットの場所で上書きします。オンにすると、サブネットにマッピングされるときに、サブネットの場所が OT デバイスの場所よりも優先されます。デフォルトは [はい] です。

製造業プロセスマネージャー と オペレーショナルテクノロジーマネージャー の両方がインストールされている場合にインストールされる自動マッピングコンポーネント

オペレーショナルテクノロジーマネージャーもアクティブな場合、いくつかのタイプの自動マッピングコンポーネント (テーブル、システムプロパティ、スケジュール設定済みフローなど) が、製造業プロセスマネージャーのアクティブ化とともにインストールされます。

これらの自動マッピングコンポーネントは、製造業プロセスマネージャーオペレーショナルテクノロジーマネージャーと一緒にインストールされるか、またはインストール時に利用できます。

テーブル

テーブル	説明
OT サブネットから機器モデルエンティティへのマッピング [ot_subnet_mapping]	OT サブネットから機器モデルエンティティへのマッピングを保存します。

プロパティ

プロパティ	説明
<code>sn_otsm.map_all_ot_assets.all_discovery_sources</code>	すべてのディスカバリーソースの OT デバイスのマッピングを制御します。 デフォルト値: True
<code>sn_otsm.map_all_ot_assets.discovery_sources</code>	指定されたディスカバリーソースの OT デバイスをマッピングします (カンマ区切り形式)。
<code>sn_otsm.subnet_mapping.auto_assign_ot_controls</code>	OT デバイスと OT コントロールモジュールに基づいて、すべての OT コントロールモジュールを機器モデルエンティティに自動的にアサインします。デフォルトは [はい] (true) です。
<code>sn_otsm.subnet_mapping.location_auto_update</code>	OT デバイスの場所をサブネットの場所で上書きします。オンにすると、サブネットにマッピングされるときに、サブネットの場所が OT デバイスの場所よりも優先されます。デフォルトは [はい] です。

フローデザイナーフロー

アプリケーション	フロー
製造業プロセスマネージャーとオペレーショナルテクノロジーマネージャーとの統合	OT デバイスマッピングフロー

製造業プロセスマネージャーの参照

参照トピックには、製造業プロセスマネージャー アプリケーションに関する追加情報が記載されています。

製造業プロセスマネージャーとともにインストールされるコンポーネント

ユーザーロールなど、製造業プロセスマネージャー アプリケーションをアクティブ化すると、いくつかのタイプのコンポーネントをインストールできます。

- i** 注: アプリケーションファイルテーブルには、このアプリケーションとともにインストールされたコンポーネントがリストされています。このテーブルへのアクセス手順については、「[アプリケーションとともにインストールされているコンポーネントの検索](#)」を参照してください。

インストールされているロール

ロール	説明
機器モデルビューア [cmdb_ot_isa_viewer]	アサインされた ISA 設備階層モデル [cmdb_ci_ot_isa_entity] テーブルレコードを表示することのみ可能です。詳細については、「 での 製造業プロセスマネージャー の使用 オペレーショナルテクノロジーマネージャー 」と「 設備モデルの管理 」を参照してください。
機器モデルエディター [cmdb_ot_isa_editor]	アサインされた ISA 設備階層モデル [cmdb_ci_ot_isa_entity] レコードを表示および編集できます。 詳細については、「 での 製造業プロセスマネージャー の使用 オペレーショナルテクノロジーマネージャー 」と「 設備モデルの管理 」を参照してください。
機器モデルアドミン [cmdb_ot_isa_admin]	cmdb_ot_isa_editor ロールを継承し、次のアクションも実行できます。 - 産業用ガイド付きセットアップを使用して、製造業プロセスマネージャーとオペレーショナルテクノロジーマネージャーを設定します。 - 機器モデルテンプレート [isa_entity_template]、[isa_entity_level]、および機器エンティティタイプ [isa_entity_type] テーブルレコードを編集する。

ロール	説明
	詳細については、「 産業用ワークスペースアドミン アプリケーションメニューとガイド付き セットアップ 」を参照してください。
ISA サイトビューアー [cmdb_ot_isa_bypass_qbr]	OT 進捗状況スコアカードですべてのサイトを表示できます。
機器モデルのダウタイムプランナー [sn_isa_schedule_admin]	機器エンティティスケジュールを作成、変更、および削除できます。スケジュールを機器エンティティに関連付けることもできます。
機器モデルビューアー すべて [cmdb_ot_isa_viewer_all]	すべての ISA Equipment Model (ISA 設備階層モデル) レコード (cmdb_ci_ot_isa_entity) と、関連する機器モデルテンプレートレコード (isa_entity_template、isa_entity_level、isa_entity_type) を表示できます。 cmdb_ot_admin に含まれるロール。
素晴らしいアドミン [sn_ot_amazing_admin]	すべての機器モデルエンティティの OT サブネットシステムプロパティの OT サブネットレコード (ot_subnet_mapping) を作成、変更、削除できます。
素晴らしいエディター [sn_ot_amazing_write]	ユーザーに関連付けられているすべての機器モデルエンティティの OT サブネットレコード (ot_subnet_mapping) を作成、変更、削除できます。
素晴らしいビューアー [sn_ot_amazing_read]	すべての機器モデルエンティティの OT サブネットレコード (ot_subnet_mapping) を表示できます。

サイトユーザーアクセスをユーザー基準とグループに移行する

ISA 設備階層モデルのバージョン 1.0.12 にアップグレードすると、サイトユーザーアクセスからユーザー基準およびユーザーグループへの移行が自動的に開始されます。

ISA 設備階層モデルのバージョン 1.0.12 にアップグレードすると、次の変更が行われます。

- ユーザー基準を使用して機器モデルエンティティサイトへの読み取りまたは書き込みレベルのユーザーアクセスを定義するサイトレベルのアクセス制御が改善されました。OT ビューアー (cmdb_ot_viewer) または OT エディター (cmdb_ot_editor) ロールの追加アサインにより、そのロールに応じてアサインされたサイト内の OT デバイスの表示や編集のアクセス権を持つこともできます。
- ISA 設備階層モデルのバージョン 1.0.12 にアップグレードすると、既存のサイトユーザーレコードは、改善されたアクセス制御モデルにユーザー基準に従って移行され、同じアクセス許可が保持されます。ISA エンティティサイトユーザーレコードを持つサイトごとに、次の変更が行われます。

- 表示アクセス権を持つユーザーの場合：
 - 新しいユーザー基準レコードが作成され、「**Read User Criteria for <サイト名> サイト#**[システム生成]」という名前が付けられます。
 - このサイトのすべてのサイトユーザーを含む新しいユーザーグループが作成され、「**Read Group for <サイト名> サイト** [システム生成]」という名前が付けられます。
 - 新しい [機器モデルエンティティ閲覧アクセス] テーブル (isa_entity_m2m_user_criteria_can_view) に、新しいユーザー基準とユーザーグループで新しいレコードが作成されます。
- 編集アクセス権を持つユーザーの場合：
 - 新しいユーザー基準レコードが作成され、「**Edit User Criteria for <サイト名> サイト** [システム生成]」という名前が付けられます。
 - このサイトのすべてのサイトユーザーを含む新しいユーザーグループが作成され、「**Edit Group for <サイト名> サイト** [システム生成]」という名前が付けられます。
 - 新しい [機器モデルエンティティ編集アクセス] テーブル (isa_entity_m2m_user_criteria_can_edit) に、新しいユーザー基準とユーザーグループで新しいレコードが作成されます。
- サイトの機器モデルエンティティレコードの [サイトユーザー] アプリケーションメニューと [サイトユーザー] 関連リストが削除されます。
- すべてのサイトユーザー (isa_entity_site_user) レコードが非アクティブに設定されます。
- [サイトユーザー：読み取り可能] および [サイトユーザー：編集可能] アプリケーションメニュー項目が ServiceNow AI Platform に追加されます。
- [機器モデルの読み取りが可能] および [機器モデルの編集が可能] 関連リストがサイトの機器モデルエンティティレコードに追加されます。

[ユーザー基準] フォーム

ユーザー基準フォームを使用して、特定のユーザーが特定のサイトの機器モデルエンティティにアクセスできるかどうかを判断できます。

次の表で、ユーザー基準フォームのフィールドについて説明します。

[ユーザー基準] フォーム

フィールド	説明
名前	ユーザー基準の名前
簡単な説明	サイトの機器モデルエンティティにアクセスするためのユーザー基準の簡単な説明。
ユーザー	ユーザー基準を適用するときにサイトの機器モデルエンティティにアクセスできるユーザー。ユーザーのロック解除アイコン (🔓) を選択して、エンティティにアクセスできるユーザーを選択します。[自分を追加] アイコン (👤) を選択して、自分をユーザーとして追加します。
グループ	ユーザー基準を適用するときにサイトの機器モデルエンティティにアクセスできるグループ。グループのロック解除アイコン (🔓) を選択してグループを選択します。

[ユーザー基準] フォーム (続く)

フィールド	説明
ロール	ユーザー基準を適用するときにサイトの機器モデルエンティティにアクセスできるロール。グループのロック解除アイコン () を選択してグループを選択します。
詳細	ユーザー基準のスクリプトを作成するオプション。
アプリケーション	自動的に [グローバル] に設定されるフィールド。
アクティブ	ユーザー基準を使用可能にするオプション。
会社	ユーザー基準を適用するときにサイトの機器モデルエンティティにアクセスできる会社。会社のロック解除アイコン () を選択して、会社を選択します。
所在地	ユーザー基準を適用するときにサイトの機器モデルエンティティにアクセスできる場所。場所のロック解除アイコン () を選択して、場所を選択します。
部門	ユーザー基準を適用するときにサイトの機器モデルエンティティにアクセスできる部門。部門のロック解除アイコン () を選択して、部門を選択します。
すべて一致	ユーザー基準が適用されるときにすべての条件を必須にするオプション。条件は、[場所]、[部門] フィールドなど、前述のフィールドで設定されます。

ISA 設備階層モデルシステムプロパティ

必要に応じて、ISA 設備階層モデルのシステムプロパティを有効にします。

ISA 設備階層モデルのシステムプロパティにアクセスするには、次に移動します: [すべて > 産業用ワークスペースアドミン > すべての OT プロパティ](#). OT システムプロパティを表示および編集する方法の詳細については、「[OT システムプロパティの表示と編集](#)」を参照してください。

次の表に、ISA 設備階層モデルのシステムプロパティを示します。

ISA 設備階層モデルシステムプロパティ

システムプロパティ	説明	タイプ
sn_isa_model.cmdb_relationships	同期される CMDB 関係のレベル数。	整数
sn_isa_model.short_code_validation_max_length	短コード検証の最大長。	整数
sn_isa_model.user_search_match_criteria	検索条件内のユーザーと一致するユーザーテーブル [sys_user] の列。デフォルトでは、ユー	文字列

ISA 設備階層モデルシステムプロパティ (続く)

システムプロパティ	説明	タイプ
	ザーテーブルの [メール] 列が使用されます。	

の事前定義フィルター 製造業プロセスマネージャー

製造業プロセスマネージャー アプリケーションでは、事前定義されたフィルターが使用されるため、産業用 ワークスペースで利用可能な UI アクションを選択して機器モデルの依存関係マップを表示できます。

製造業プロセスマネージャーでは、次の事前定義フィルターを使用できます。

ISA 設備階層モデル:階層プロセス

選択した機器モデルエンティティの階層構造と、生産プロセス内の他のエンティティとの関係。

ISA 設備階層モデル:OT 依存関係マップ

選択した機器モデルエンティティの階層構造と、他のエンティティおよび オペレーショナルテクノロジー (本番プロセスの OT デバイス) との関係。

ISA 設備階層モデル:OT デバイスマップ

選択した機器モデルエンティティと、本番プロセス内の他の OT デバイスとの関係のグラフィカル表現。

ISA 設備階層モデル:プロセス

選択した機器モデルエンティティと生産プロセスとの関係のグラフィカル表現。

説明されている事前定義フィルターを使用して機器モデルの依存関係マップを表示するには、産業用ワークスペース に移動して機器モデルビューを開きます。次に、依存関係マップを表示する機器モデルエンティティを選択できます。レコードを開くと、次の UI アクションが表示され、そこから選択できます。

- OT 依存関係マップを表示

i 注: レコードヘッダーの [マップを表示] を選択して、OT デバイスレコードの OT 依存関係マップを表示することもできます。

- OT デバイスマップを表示
- 階層を表示
- プロセスを表示

組織の必要に応じて、事前定義フィルターを更新することもできます。詳細については、「[事前定義フィルターの変更](#)」を参照してください。

事前定義フィルターの変更

組織の必要に応じて、ISA 設備階層モデルアプリケーションの事前定義フィルターを変更します。

始める前に

必要なロール: ecmdb_admin

手順

1. 移動先 **すべて > 依存関係ビュー > 事前定義フィルター**.
2. フィルター [アプリケーション] [次の値に等しい] **[ISA 設備階層モデル]** を適用します。
3. 編集する事前定義フィルターレコードを選択します。
4. 必要に応じて、[構成タイプ]、[CI フィルター]、および [関係性タイプ] 関連リストを変更します。
これらの関連リストを変更する方法の詳細については、「[事前定義フィルターの作成](#)」を参照してください。
5. **[Update (更新)]** を選択します。

サイトと場所

サイト属性と場所属性では、オペレーショナルテクノロジー (OT) のさまざまな用途があります。

サイト

サイトは ISA 設備階層モデルエンティティの一部であり、生産プロセスが行われる工業用地を記述します。サイトは論理的であり、それらを使用して機器モデルを定義できます。その後、その機器モデルを使用してアクセス制御を提供できます。アクセス制御の詳細については、「[アドミニストレーター以外の機器モデルサイトアクセスの割り当てまたは削除](#)」を参照してください。

サイトには場所を設定できますが、場所とは見なされません。OT デバイスには場所があり、機器モデルエンティティサイトにアサインすることができます。

場所

場所は、場所 (cmn_location) テーブルに格納されている値を参照します。機器モデルまたはデバイスの物理的な場所です。たとえば、設備モデルの 1 つがサイト「アトランタ」に属し、ジョージア州アトランタにある場合、その場所を「ジョージア州アトランタ」としてリストします。

関連情報

ネットワーク侵入検知システム (NIDS) 拡張クラス、OT 拡張クラス、および関連アプリケーションの詳細を確認してください。

拡張クラスの概要

拡張クラスは、オペレーショナルテクノロジー管理 が 構成管理データベース (CMDB) でどのように機能するかを理解するのに役立ちます。

ネットワーク侵入検知システム (NIDS) CI 拡張クラス

ネットワーク侵入検知システム (NIDS) [cmdb_ci_nids] クラスは、パッシブネットワークモニタリングアプライアンスと、それが検出するネットワーク上のデバイスとの間の関係をビルドします。

オペレーショナルテクノロジー (OT) 拡張クラス

構成管理データベース (CMDB) は OT のクラスを更新します。

関連アプリケーション

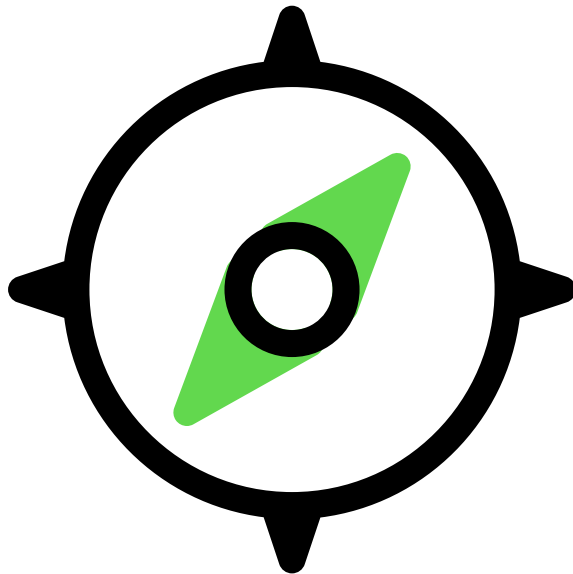
オペレーショナルテクノロジーマネージャー

オペレーショナルテクノロジーマネージャー アプリケーションを使用すると、複数のソースから OT デバイスデータを集計できるため、産業用ソリューションで使用される基本的なデータ関係をビルドできます。

オペレーショナルテクノロジー脆弱性対応

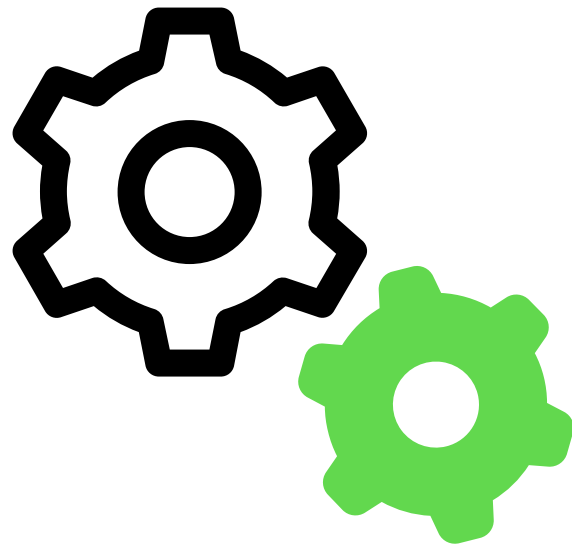
オペレーショナルテクノロジー脆弱性対応により、サイトレベルでの OT デバイスの脆弱性を効果的に優先順位付けたり修正したりできます。OT デバイスの CMDB 関係を活用することで、自動化する本番プロセスの重要度に基づいて脆弱なデバイスまたはアイテムに優先順位を付けることができます。

探索



オペレーショナルテクノロジー脆弱性対応の探索

構成



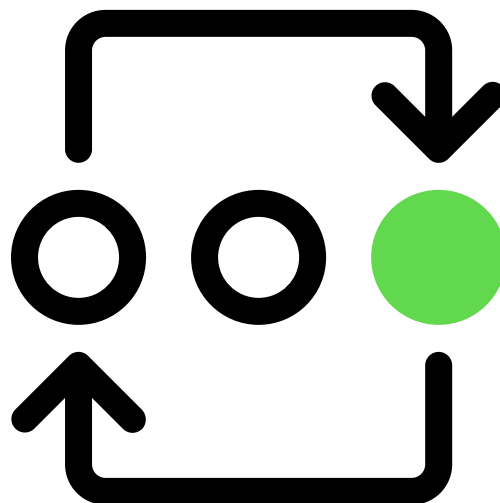
オペレーショナルテクノロジー脆弱性対応の構成

使用方法



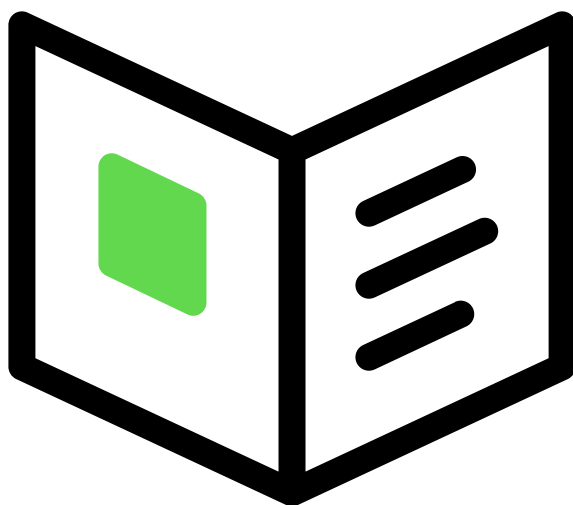
オペレーショナルテクノロジー脆弱性対応の使用

統合



他のアプリケーションと統合してオペレーショナルテクノロジー脆弱性対応を拡張します

参照



関連情報とアプリケーションの詳細を取得

オペレーショナルテクノロジー脆弱性対応の探索

オペレーショナルテクノロジー脆弱性対応を工業生産プロセスの統合ソリューションとして使用します。

オペレーショナルテクノロジー脆弱性対応の概要

https://player.vimeo.com/video/1020858131?h=c90c2ff89a&badge=0&autoplay=0&player_id=0&app_id=58479

OT エンジニアまたは OT 脆弱性マネージャーは、オペレーショナルテクノロジー脆弱性対応 を使用して次のような質問に対する回答を見つけることができます。

- 使用している OT デバイスにどのような脆弱性があるか？ ☑
- OT 固有のリスクを使用して脆弱性の修正を優先するにはどうすればよいか？
- OT の脆弱性の修正に向けてどのような進捗状況がありますか？

修復タスクと脆弱性一致アイテムの状況

ユースケースが複雑なため、脆弱性一致アイテム (VIT) とその修復タスクの状況が異なる場合があります。修復タスクと脆弱性一致アイテムの状況とそのワークフローの詳細については、「[脆弱性対応 修復タスクと脆弱性一致アイテム状況](#)」を参照してください。

主な機能

オペレーショナルテクノロジー脆弱性対応では、次の主要な機能を使用できます。

- オペレーショナルテクノロジー脆弱性対応 (PA) ダッシュボードは、OT VIT の初期分析と検出から封じ込めや修復までのボリューム、パフォーマンス、および進捗状況を追跡します。
- オペレーショナルテクノロジー (OT) 脆弱性リスクロールアップダッシュボードには、機器モデルの各レベルの OT デバイスのリスクスコアが含まれています。

オペレーショナルテクノロジー 脆弱性ソリューション管理

Xanadu バージョン以降、オペレーショナルテクノロジー (OT) 脆弱性ソリューション管理は オペレーショナルテクノロジー脆弱性対応 アプリケーション内で利用可能な機能です。

多くの場合、セキュリティチームと IT チームは、脆弱性の検出結果を調査し、環境にとって最も効果的なソリューションを特定するために、多大な時間と労力を費やしています。大規模な組織では、脆弱性の量と複雑さのために、脆弱性の検出結果を修復タスクに変換するのは手作業で面倒でエラーが発生しやすいプロセスです。

OT 脆弱性ソリューション管理 は、環境内の脆弱性の検出結果を、それを修復する可能性のあるソリューションと自動的に関連付けます。脆弱性に適用される修復アクションを特定し、脆弱性リスクの重大度別に優先順位を付けることができます。また、OT の補完コントロールを使用することで、すぐにパッチを適用できない脆弱性によってもたらされるリスクを軽減できます。詳細については、「[の補完コントロールの使用 オペレーショナルテクノロジー](#)」を参照してください。

OT 脆弱性ソリューション管理 機能は、脆弱性対応 アプリケーションで利用可能な機能に基づいています。脆弱性ソリューション管理の詳細については、「[脆弱性ソリューション管理](#)」を参照してください。

OT 脆弱性ソリューション管理 は、ソリューションインテリジェンス統合の汎用形式をサポートしています。ソリューションインテリジェンス統合の汎用フレームワークは、ソリューションベンダーからさまざまなファイル形式でデータを取り込みます。これらの形式は、情報の交換と処理を高速化します。また、標準化されたレポート形式での重要なセキュリティ関連情報の共有を改善します。サポートされているファイル形式は、JSON ベースの構造化された機械可読セキュリティアドバイザリーを提供するオープンソース規格の Common Security Advisory Framework (CSAF) です。米国サイバーセキュリティ社会基盤安全保障庁 (CISA)、Siemens、Hitachi、Schneider Electric などの主要ベンダーが CSAF 形式をサポートしています。

CSAF でサポートされているソリューション管理には、次の主要な機能が含まれています。

- セットアップアシスタントによる構成。詳細については、「[脆弱性ソリューションプロバイダーの構成](#)」を参照してください。
 - ファイルインポートによる CSAF データのインポートのサポート。詳細については、「[ファイルインポートによる Common Security Advisory Framework データのインポート](#)」を参照してください。
 - CSAF URL を介した CSAF データのインポートのサポート。詳細については、「[CSAF URL による Common Security Advisory Framework \(CSAF\) データのインポート](#)」を参照してください。OT 脆弱性ソリューション管理 を使用すると、以下から CSAF データをインポートできます。
 - CSAF 形式をサポートし、CSAF URL ROLIE フィードを持つ個々のベンダー。ベンダーから提供された CSAF URL ROLIE フィードを使用して、CSAF データをインポートできます。たとえば、Siemens URL ROLIE フィードなどです。
 - ROLIE フィードをサポートする URL インポートを介した CSAF アグリゲーターまたは信頼できるプロバイダー。信頼できるプロバイダーから複数のベンダーの CSAF データをインポートできます。たとえば、CISA は信頼できるプロバイダーであり、[CISA の GitHub CSAF リポジトリ](#)にある産業用制御システム (ICS) CSAF アドバイザリから複数のベンダーの CSAF データをインポートできます。これらの脆弱性ソリューションは、共通脆弱性識別子 (CVE) に基づいて、正しいベンダーおよび脆弱性一致アイテム (VIT) に自動的にマッピングされます。信頼できるプロバイダーを使用すると、個々のベンダーの CSAF URL から CSAF データをインポートするために必要な時間と労力が削減されます。
 - アドバイザリーまたは API を使用した CSAF データのインポートのサポート。詳細については、「[アドバイザリーからの Common Security Advisory Framework データのインポート](#)」を参照してください。
- i 注:** 移動先 [すべて > 脆弱性対応 > ソリューション > すべて](#) をクリックして、上記の方法を使用してインポートしたソリューションのリストを表示します。

脆弱性対応プラグインは、作成されたソリューションのメトリクスステータスを更新します。

関連トピック

[での脆弱性一致アイテムとソリューションの表示](#) [産業用ワークスペース](#)

オペレーショナルテクノロジー脆弱性対応の構成

オペレーショナルテクノロジー (OT) アサインルール、修復ターゲット、リスク算出、およびリスクロールアップ計算を構成してから、脆弱性一致アイテムレコードを作成するように統合を構成します。

i 注:

sn_vul.vulnerability_admin ロールを持っている場合は、産業用 ガイド付きセットアップを使用して、オペレーショナルテクノロジー脆弱性対応 アプリケーションのセットアップ手順を実行できます。

ガイド付きセットアップにアクセスするには、次に移動します: 産業用ワークスペースアドミン > ガイド付きセットアップ。

タスク	目的
1. ServiceNow Storeからオペレーショナルテクノロジー脆弱性対応をインストールします。	オペレーショナルテクノロジー脆弱性対応 アプリケーションをインストールします。

タスク	目的
2. 必要に応じて、アドミンユーザーまたはユーザーグループにロールをアサインします。	ロールを割り当てて、各ユーザーが使用できるアクションをコントロールします。
3. OT 脆弱性修正オーナーにロールをアサインします。	OT 脆弱性修正オーナーが利用できるアクションを制御するロールをアサインします。
4. アサイン先グループを作成し、ユーザーをサイトとグループにアサインします。 1. 機器モデルマネージャーにある各サイトの オペレーショナルテクノロジー脆弱性対応 サイトアサイン先グループを作成します。 2. cmdb_ot_isa_viewer ロールまたは cmdb_ot_isa_editor ロールを既に持っているユーザーをサイトにアサインします。 3. サイトのアサイン先グループにユーザーを追加します。	- OT 修復オーナーユーザーに、サイトの脆弱性一致アイテムのみの表示を許可します。 - ユーザーがアサインされているサイトの脆弱性一致アイテムを表示できるようにします。
5. OT 修復ターゲットルールを構成します。	- OT 脆弱性一致アイテムをサイトレベルのグループまたは分類に基づくグループにアサインします。 - 脆弱性一致アイテムの修正予定期間を定義します。
6. オペレーショナルテクノロジー脆弱性対応 アプリケーションのデモデータレコードをロードします。	OT 脆弱性一致アイテムの修復ターゲットを計算します。
7. OT リスク算出を設定します。	OT デバイスの脆弱性一致アイテムのリスクを計算するときに使用する OT リスク要因を決定します。
8. OT リスクロールアップ算出を設定します。	機器モデルエンティティの各レベルで OT デバイスのリスクスコアを計算します。
9. お使いの環境に適用可能な オペレーショナルテクノロジー脆弱性対応 アプリケーションの オペレーショナルテクノロジー 認定統合をインストールします。	OT 脆弱性管理の機能を強化する認定サードパーティアプリケーションを統合します。

オペレーショナルテクノロジー脆弱性対応 をインストール

admin ロールを持っている場合は、オペレーショナルテクノロジー脆弱性対応 アプリケーションをインストールします。このアプリケーションには、デモデータが含まれています。まだインストールされていない場合は、関連するストアアプリケーションとプラグインをインストールします。

始める前に

- アプリケーションとその関連するすべての ServiceNow Store アプリケーションに有効な ServiceNow エンタイトルメントがあることを確認してください。詳細については、次を参照してください。 [のエンタイトルメントを取得する ServiceNow 製品またはアプリケーション](#)。
- アプリケーションに必要なプラグインや他のストアアプリケーションがあり、まだインストールされていない場合は、先にこれらをインストールします。

- オペレーショナルテクノロジー脆弱性対応 には次のプラグインが必要です。オペレーショナルテクノロジー脆弱性対応 をインストールする前に、これらのプラグインがアクティブ化されていることを確認してください。

必須の ServiceNow プラグイン

脆弱性対応 (sn_vul)

ServiceNow 脆弱性対応アプリケーションは、脆弱性一致アイテムをインポートして、グループルールに従って自動的にグループ化し、脆弱性を修正できるようにします。「[脆弱性対応のインストール](#)」を参照してください

製造業プロセスマネージャー (sn_otsm)

ServiceNow 産業用ソリューションに必要な ISA-95 機器モデルデータ基盤を作成します。「[製造業プロセスマネージャー をインストールする](#)」を参照してください。

オペレーショナルテクノロジー マネージャー

オペレーショナルテクノロジー Manager アプリケーションは、企業がServiceNow 産業用ソリューションを使用できるようにする基盤データと関係を作成します。オペレーショナルテクノロジーManager は、ServiceNow AI Platform内の 構成管理データベース (CMDB)、サービスグラフコネクタ、およびディスカバリーアプリケーションの使用をサポートしています。[オペレーショナルテクノロジーマネージャー \(OTM\) の構成](#)を参照してください。

必要なロール：admin

このタスクについて

次のアイテムは、オペレーショナルテクノロジー脆弱性対応 アプリケーションのインストール時にインストールされます。

- プラグイン
- ストアアプリケーション
- ロール
- ビジネスルール

アプリケーションとともにインストールされているコンポーネントの表示の詳細については、以下を参照してください。

- [オペレーショナルテクノロジー脆弱性対応とともにインストールされるコンポーネント](#)
- [アプリケーションとともにインストールされているコンポーネントを検索します](#)。

手順

1. 移動先 [すべて > システムアプリケーション > 利用可能なすべてのアプリケーション > すべて](#)。
2. フィルター基準と検索バーを使用して オペレーショナルテクノロジー脆弱性対応 アプリケーションを検索します。

名前または ID でアプリケーションを検索できます。アプリケーションが見つからない場合は、ServiceNow Store へのリクエストが必要になることもあります。

[ServiceNow Store](#) Web サイトにアクセスして利用可能なすべてのアプリを表示し、ストアにリクエストを送信する方法について確認してください。リリースされたすべてのアプリのリリース

ノート情報については、「[ServiceNow Storeバージョン履歴のリリースノート](#)」を参照してください。

3. リストからバージョンを選択し、[インストール] を選択します。

表示される [インストールの詳細を確認] ダイアログボックスに、アプリケーションとともにインストールされている依存関係が一覧表示されます。

4. プロンプトが表示された場合は、ServiceNow Store へのリンクに従って、依存関係のエンタイトルメントを取得します。

5. オプション: 利用できるデモデータをインストールするには、[デモデータのロード] チェックボックスをオンにします。

デモデータは、一般的なユースケース向けのアプリケーション機能を説明するサンプルレコードです。開発またはテストインスタンスで初めてアプリケーションをインストールする場合は、デモデータを読み込みます。

6. [Install (インストール)] を選択します。

オペレーショナルテクノロジー脆弱性対応 ロールの割り当て

ユーザーにロールをアサインすると、オペレーショナルテクノロジー脆弱性対応 アプリケーションの各機能やデータへのアクセスを制御できます。

始める前に

必要なロール: admin

このタスクについて

次のテーブルにリストされているロールを持つユーザーは、オペレーショナルテクノロジー脆弱性対応 アプリケーションを使用できます。

必要に応じてアドミンユーザーまたはユーザーグループにロールをアサインします。

アドミンユーザーまたはグループへのロールのアサイン

ロール	説明
OT VR 統合ビューアー [sn_otvr.integration_viewer]	OT VR 統合レコードを表示できます。
OT VR 統合アドミン [sn_otvr.integration_admin]	OT VR 統合レコードを表示および編集できます。
OT 脆弱性修正オーナー [sn_otvr.remediation_owner]	修復タスクを作成できます。脆弱性一致アイテムの既存の修復タスクをスケジュールすることもできます。

手順

ServiceNow AI Platform ユーザー管理機能を使用して、ユーザーとグループにロールをアサインします。

タスク	ユーザー管理機能
ユーザーへのロールのアサイン	ユーザーへのロールの割り当て を参照してください。
グループへのロールのアサイン	グループへのロールのアサイン を参照してください。

次のタスク

サイトのアサイン先グループを作成する。

サイトのアサイン先グループを作成する

機器モデルマネージャーで、サイトごとに 1 つの オペレーショナルテクノロジー脆弱性対応 アサイン先グループを作成します。これにより、OT の修復オーナーであるユーザーは、自分のサイトの脆弱性一致アイテムに限って表示できるようになります。

始める前に

オペレーショナルテクノロジー脆弱性対応アサイン先グループを作成し、可能であれば関連するサイトと同じ名前で作成します。たとえば、サイトがミラノにある場合、グループに「ミラノの OT VR アサイン先グループ」という名前を付けます。

必要なロール:cmdb_ot_isa_admin

手順

1. 移動先 **すべて > 産業用ワークスペースアドミン > 産業用プロセスマネージャー > 拠点**.
2. サイトレコードを選択します。
サイトレコードは、それ自体が親を持たない親機器モデルエンティティです。
3. **[OT VR assignment group (OT VR アサイン先グループ)]** フィールドで、検索アイコンを選択すると既存のユーザーグループが表示されます。
4. 該当するアサイン先グループを選択します。
 - 目的のグループが存在する場合は、リストからそれを選択します。
 - 目的のグループが存在しない場合は、**[New (新規)]** を選択してグループを作成し、**[Submit (送信)]** を選択します。
5. サイト レコードに戻った後、 **更新** を選択します。
新しい OT VR アサイン先グループが作成されます。

次のタスク

サイトにユーザーをアサインする

サイトにユーザーをアサインする

製造業プロセスマネージャーの構成時にまだ行っていない場合は、cmdb_ot_isa_viewer ロールまたは cmdb_ot_isa_editor ロールを既に持っているユーザーをサイトにアサインします。

始める前に

OT デバイスが CMDB にある場合、サイトアクセスを構成して、OT デバイスの表示を cmdb_ot_viewer、editor または admin ロールと、cmdb_ot_isa_viewer または editor ロールの両方を持つユーザーに制限できます。

必要なロール:cmdb_ot_isa_admin

手順

1. [機器モデルエンティティ] フォームから、親機器モデルエンティティを選択します。
機器モデルの詳細については、「[機器モデルの管理](#)」を参照してください。
2. [サイトユーザー] タブで、[新規] を選択します。
3. ISA エンティティサイトのユーザーフォームで、フィールドに入力します。
4. **[Submit (送信)]** を選択します。
ユーザーがサイトにアサインされます。

次のタスク

ユーザーのアサイン先グループへのアサイン

ユーザーのアサイン先グループへのアサイン

アサイン先グループにユーザーを追加すると、そのユーザーはアサインされたサイトの脆弱性一致アイテムを表示できるようになります。

始める前に

アサインしたサイトの脆弱性一致アイテムをユーザーが表示できるようにするには、サイトの OT VR アサイン先グループにユーザーを追加します。

OT 脆弱性一致アイテムが作成されると、可視化は次のものに制限されます。

- VR 修正オーナー (sn_vul.remediation_owner) ロールを持つユーザー
- OT デバイスが属するサイトに関連付けられた オペレーショナルテクノロジー脆弱性対応 アサイン先グループのメンバーシップ

必要なロール：admin

手順

1. サイトの オペレーショナルテクノロジー脆弱性対応 アサイン先グループに対応するグループを開きます。
2. [Group Members (グループメンバー)] タブから、**[Edit (編集)]** を選択します。
3. [Collection (コレクション)] リストから、[Group Members List (グループメンバーリスト)] にユーザーを追加します。
4. **[Save (保存)]** を選択します。
ユーザーはグループにアサインされ、アサインされたサイトの脆弱性一致アイテムを表示できます。グループへのユーザーの追加などの管理タスクの詳細については、「[ユーザー管理](#)」を参照してください。

次のタスク

脆弱性一致アイテムのグループへのアサイン。

脆弱性一致アイテムのグループへのアサイン

OT 脆弱性アサインルールを構成します。

始める前に

OT 脆弱性一致アイテムは、修正戦略に応じて、サイトレベルのグループまたは分類に基づくグループにアサインできます。

必要なロール:sn_vul.manage_assignment_rules または sn_vul.vulnerability_admin

このタスクについて

脆弱性一致アイテムがインポートされると、脆弱性アサインルールに基づいて適切なグループにアサインされます。オペレーショナルテクノロジー脆弱性対応 には、サイトに基づいて対応する OT VR アサイングループに OT 脆弱性一致アイテムレコード (VIT) をアサインする、オペレーショナルテクノロジー (**OT**) アサインルールという 1 つの OT 脆弱性アサインルールが付属しています。OT VR アサイン先グループがどのサイトにも属していない場合、またはサイトにグループが指定されていない場合、ルールは OT VR のデフォルトのアサイン先グループにアサインされる。

脆弱性対応アサインルールの作成の詳細については、「[脆弱性対応アサインルールの作成または編集](#)」を参照してください。

手順

1. [Vulnerability Assignment Rules (脆弱性アサインルール)] リストから、**[Operational Technology (OT) assignment rule (オペレーショナルテクノロジー (OT) アサインルール)]** を選択します。
2. 修復戦略に基づいてルールを構成します。
 - 修正戦略がすべての OT 脆弱性一致アイテムをサイトにアサインすることである場合は、OT VR アサインルールの実行順序を他のすべてのルールよりも小さくなるように設定します。
 - クラスごとに割り当ててから他のすべてのクラスのサイトにアサインする場合は、OT VR アサインルールの実行順序をすべてのクラススペースのルールよりも大きくなるように設定します。
3. 実行順序が更新されたら、OT VR アサインルールのアクティブ状態を **true** に設定します。

次のタスク

OT 修復ターゲットルールを構成する。

OT 修復タスクルールの構成

産業用 ワークスペースで作成された修復タスクの場合は、既存の修復タスクルールを更新して、インポートされた脆弱性一致アイテムによって OT デバイスが自動的に追加されないようにします。

始める前に

必要なロール:sn_vul.manage_group_rules または sn_vul.vulnerability_admin

脆弱性一致アイテムがインポートされると、構成された修復タスクルールに基づいてそのアイテムが修復タスクに追加されることがあります。IT と OT ネットワークの両方に 脆弱性対応 を使用する場合は、修正のために脆弱性一致アイテムを IT と OT ネットワーク間で異なる方法でグループ化する場合は、構成を変更する必要があります。 オペレーショナルテクノロジー脆弱性対応 では、OT ネットワークの脆弱性を自動的にグループ化から除外する方法を示すサンプルの修復タスクルールレコードを提供しています。

修正戦略に基づいて、新規または既存の修復タスクルールを設定します。

- IT 環境内の脆弱性のみを対象として修復タスクを自動作成するという修正戦略の場合は、既存の修復タスクルールそれぞれに、OT の脆弱性を除外する次の条件を追加します。
 - 構成アイテム。OT デバイスの詳細 = (空)
- すべての OT 脆弱性一致アイテムの修復タスクを自動作成するという修正戦略の場合は、適切なルールを作成します。

OT VR デモデータに付属するサンプル:修復タスクルール:脆弱性 (OT を除く)

A remediation task rule defines how a set of vulnerable items are automatically grouped for remediation. Define your rules such that all vulnerable items within a group are remediated by the same team, same remediation action, and same timeframe. For example, group by vulnerable item "Assignment group", "Vulnerability", and CI "Used for" (ex. Production, Staging, Development) if those environments have different maintenance windows. Vulnerable items that are not in the Open state are always excluded.

* Name: Vulnerability (exclude OT) Active ☐

Description: NOTE - this rule is necessary to avoid including OT assets automatically into remediation tasks - every remediation task rule will need to add an "AND" clause to do this. This is a copy of the existing "Vulnerability" remediation task rule, just renamed with the additional condition "Configuration item. Ot asset details = is empty"

Case sensitive ☐

Condition: All of these conditions must be met

Active is true AND Configuration item. OT asset details is empty

Group by: Choose the vulnerable item fields to group by. If an extended table field is chosen, the field will be used only for vulnerable items that use the extended table.

Group vulnerable items from: Vulnerable Item Using field: Assignment group

And then from: Vulnerable Item Using field: Vulnerability

And then from: Vulnerable Item Using field: Click to select...

Assignment: If this rule groups vulnerable items by a user group field, such as vulnerable item "Assignment group", the remediation tasks can be assigned to match (Recommended). Use Assignment Rules to automatically set the vulnerable item "Assignment group" field for use in remediation task rules. Assign remediation tasks using the "Group by" field that specifies the desired user group field.

For example, a rule that groups on vulnerable item "Assignment group" could create separate groups for vulnerable items assigned to Windows Server, Database and Network. Each remediation task itself would then be assigned to Windows Server, Database and Network respectively.

Alternatively, remediation tasks created by this rule can be set to a static user group.

Assign remediation tasks by: Group by field

* Group by field: Assignment group

手順

1. 移動先 脆弱性対応 > アドミニストレーション > 修復タスクルール。

2. 更新するルールの名前を選択します。

- グループ内のすべての脆弱性一致アイテムが同じチーム、同じ修復アクション、同じ時間枠によって修正されるようにルールを定義します。たとえば、脆弱性一致アイテムの「アサイン先グループ」、「脆弱性」、および CI の「使用目的」でグループ化します (例: 本番、ステージング、開発) の環境のメンテナンス期間が異なる場合。
- 修復タスクルールの詳細については、「[脆弱性対応ワークスペース](#)」を参照してください。
- 修復タスクの詳細については、「[IT 修復ワークスペースの探索](#)」を参照してください。

OT 修復ターゲットルールを構成する

OT 脆弱性一致アイテムの修復ターゲットルールを構成します。

OT 脆弱性一致アイテムの修復ターゲット日を計算するには、オペレーショナルテクノロジー脆弱性対応 アプリケーションのデモデータレコードをロードし、修復ターゲットルールを構成します。

必要なロール:sn_vul.manage_remediation_target_rules または sn_vul.vulnerability_admin

産業環境ではメンテナンスを実行する機会が少ないため、OT 修復ターゲットが異なる場合があります。修復ターゲットルールは、最小のターゲットから最大のターゲットの順に適用されます。

他の脆弱性と同じ期間内にメンテナンス期間がない OT デバイスの脆弱性に対しては、別の修復ターゲット日が必要になる場合があります。この状況で修復ターゲット日を設定する方法を示すために、重大なリスク評価に対してこれを管理する方法を示す 2 つのデモデータレコードが提供されています。

- 重大なリスク評価ルール (OT のみ) - このルールでは、構成アイテムの条件を使用します。OT デバイスの詳細が空ではない、かつリスク評価 = 1:重大。[Target (days) (ターゲット (日数))] を更新し、レコードを有効化します。
- 重大なリスク評価ルール (OT を除く):重大なリスクの非 OT アイテムにのみ短いターゲットを適用するには、最初に OT デバイスを除外する必要があります。このルールでは、条件 [構成アイ

テム]を使用します。OT デバイスの詳細が空で、かつリスク評価 = 1: 重大。[Target (days) (ターゲット (日数))] を更新し、既存の重大なターゲットルールを無効にして、代わりにこのルールを有効にします。

- i 注:** OT の重大なリスクの脆弱性が非 OT 修復ターゲットルールから除外されるように、これらのルールの両方をアクティブ化する必要があります。

脆弱性対応アサインルールの作成の詳細については、以下を参照してください。

- [脆弱性対応修復ターゲットルール](#)
- [脆弱性対応修復ターゲットルールの作成または編集](#)

リスク算出の設定

リスク算出の設定

OT デバイスの脆弱性一致アイテムのリスクを計算するときに使用する OT リスク要因を決定します。

始める前に

オペレーショナルテクノロジー では、追加要素として、OT デバイスの重要度、Purdue レベル、および OT デバイスが自動化する本番プロセスの重要度を含めることができます。

必要なロール: sn_vul.manage_risk_score_configuration または sn_vul.vulnerability_admin

このタスクについて

このステップについては、オペレーショナルテクノロジー脆弱性対応 アプリケーションに付属する OT 脆弱性算出を備えたデフォルトリスク算出を参照してください。OT を使用したデフォルトのリスク算出は、OT 脆弱性一致アイテムと非 OT 脆弱性一致アイテムに対して別々にリスクを計算する必要がある場合に使用されます。

i 注:

- プラグインのインストール中にデモデータをロードしなくても、オペレーショナルテクノロジー脆弱性対応 リスク算出に直接アクセスして使用できます。以前のリリースでは、リスク計算はデモデータの一部として含まれていました。
- 一度にアクティブにできる脆弱性算出は 1 つだけであるため、OT 以外のすべての脆弱性一致アイテムのリスクを計算する例として、指定されたデフォルトのリスクルール (非 OT) が使用されます。

詳細については、「[Define fields and weights for the risk rule \(リスクルールのフィールドと重み付けを定義する\)](#)」を参照してください。

OT 脆弱性一致アイテムのリスクスコアを設定するには、デモデータの OT デフォルトリスクルールのリスクルールレコードの重み付けを調整します。デモデータの OT で利用可能なその他のフィールドは次のとおりです。

- 機器モデルエンティティの重要度: サービス事業上の重要度ルールを使用します。
- OT デバイスの重要度: 構成アイテムの OT デバイスの詳細のデバイスの重要度ルールを使用します。
- Purdue レベル: 構成アイテム OT デバイスの詳細 [Purdue レベル] フィールドを使用します。

手順

1. 脆弱性算出に移動します。
2. [Vulnerability Calculators (脆弱性算出)] リストから、**[Default Risk Calculator with OT (OT を使用したデフォルトリスク算出)]** を選択します。
3. [Vulnerability Calculators Rules (脆弱性算出ルール)] リストから、編集するリスクルールを開きます。
たとえば、**[OT Default Risk Rule (OT デフォルトリスクルール)]** を選択します。
4. [Vulnerability Risk Rules (脆弱性リスクルール)] ページの [Risk Calculator Criteria (リスク算出基準)] セクションで、リスクルールフィールドを 1 つ選択します。
5. [リスクルール] フィールドレコードで、全体的なリスクスコア計算における重要性に従って、各基準の重み付けまたは重み付け % を更新します。
6. **[Update (更新)]** を選択します。

次のタスク

他のすべての脆弱性一致アイテムのリスクスコアを設定するには、既存のリスクルールを OT を使用したデフォルトリスク算出にコピーし、OT デフォルトリスクルールの後に実行するように順序を設定します。

OT 脆弱性リスクロールアップ算出を構成する

OT 脆弱性リスクロールアップ算出を使用して、機器モデルの各レベルで OT デバイスのリスクスコアを計算します。全体的なリスクスコアは、親の機器モデルエンティティにロールアップされます。

始める前に

- スケジュール済みジョブを実行して、すべての機器モデルエンティティのリスクスコアを計算します。

i 注: すべての機器モデルエンティティのリスクスコア計算は、日次スケジュールジョブの後の実行に対してのみ行われます。

- [機器モデルエンティティ] リストの [Service Populator] 列が **[OTDynamicManualServicePopulator]** に設定されていることを確認するには、次の場所に移動します。すべて > 機器モデル: **ISA** > 機器モデルエンティティ。他の値に設定されている場合は、*Update ISA entity service populator* オンデマンドジョブを実行する必要があります。

- 移動先 すべて > システム定義 > スケジュール済みジョブ。
- [*Update ISA entity service populator*] ジョブを選択します。
- **[Execute Now (今すぐ実行)]** を選択します。

i 注: [機器モデルエンティティ] リストに [Service Populator] 列が表示されない場合は、リストをカスタマイズして追加できます。詳細については、「[リストのカスタマイズ](#)」を参照してください。

- 必要なロール: `sn_vul.vulnerability_admin`

このタスクについて

このステップについては、オペレーショナルテクノロジー脆弱性対応 アプリケーションのデモデータに付属する OT 脆弱性算出を使用した脆弱性ロールアップ算出を参照してください。

詳細については、「[脆弱性対応ロールアップ算出](#)」を参照してください。

機器モデルエンティティのリスクスコアを計算するには、次のフィールドの重み付けを設定します。

- 機器モデルエンティティに関連付けられた脆弱性一致アイテム (VIT) の最大リスクスコア。
- 機器モデルエンティティに関連付けられた VIT の平均リスクスコア。
- 機器モデルエンティティあたりの脆弱性一致アイテムの数。

手順

1. 移動先 **すべて > 脆弱性対応 > アドミニストレーション > 脆弱性ロールアップ算出**.
2. [Vulnerability Rollup Calculator (脆弱性ロールアップ算出)] リストから、**[Equipment Model Entity Rollup (機器モデルエンティティロールアップ)]** を選択します。
3. 必要に応じて、[Rollup Weights (ロールアップの重み付け)] セクションで、各基準の重み付けを更新します。
4. **[Update (更新)]** を選択します。

次のタスク

これで、機器モデルエンティティのレベルで関連付けられたリスクを計算できるようになりました。

1. すべての機器モデルエンティティのリスクロールアップを計算します。
 - a. 移動先 **すべて > 産業用ワークスペースアドミン > ガイド付きセットアップ**.
 - b. [オペレーショナルテクノロジー脆弱性対応] を選択します。
 - c. [リスクロールアップ計算] セクションで、リスクロールアップ構成タスクを選択します。
 - d. **[Configure]** を選択します。
 - e. ガイド付きセットアップで説明されている手順に従います。
2. *Risk Rollup for VITs by Equipment Model Entity* スケジュール済みジョブを設定します。
 - a. 移動先 **すべて > 産業用ワークスペースアドミン > ガイド付きセットアップ**.
 - b. [オペレーショナルテクノロジー脆弱性対応] を選択します。
 - c. [リスクロールアップ計算] セクションで、リスクロールアップタスクの日次スケジュールジョブを選択します。
 - d. **[Configure]** を選択します。
 - e. ガイド付きセットアップで説明されている手順に従います。

 **注:** デフォルトでは、ジョブは毎日実行するように設定されています。これは、[実行]、[タイムゾーン]、および [時間] フィールドを編集することで、ビジネスニーズに合わせて変更できます。

3. リスクスコアロールアップのエンティティを構成します。
 - a. 移動先 **すべて > 産業用ワークスペースアドミン > ガイド付きセットアップ**.
 - b. [オペレーショナルテクノロジー脆弱性対応] を選択します。
 - c. [リスクロールアップ計算] セクションで、[リスクスコアロールアップジョブのすべてのエンティティを設定] タスクを選択します。
 - d. **[Configure]** を選択します。
 - e. ガイド付きセットアップで説明されている手順に従います。
4. 修復タスクのリスクスコアと評価が間違わないようにするには、サイトがアサインされていない OT デバイスのロールアップレコードの [テーブル] フィールドを変更します。

- a. 移動先 **すべて > システム定義 > スクリプト - バックグラウンド**.
- b. [スクリプトを実行] フィールドに、次のスクリプトを追加します。

```
var gr = new GlideRecord('sn_vul_rollup');

gr.get('sys_id','24973dc4939e42900b1566f4548918eb');

gr.table = 'sn_ot_metric';

gr.update();
```

- c. [Run Script] を選択します。
- d. サイトがアサインされていない **OT** デバイスのロールアップレコードの [テーブル] フィールドの値を確認し、スケジュール済みジョブを実行するには、 **すべて > 脆弱性対応 > アドミニストレーション > 脆弱性ロールアップ算出**.
- e. サイトが割り当てられていない **OT** デバイスのロールアップレコードを選択します。
- f. [テーブル] フィールドが **[OT メトリクス [sn_ot_metric]]** に設定されていることを確認します。
- g. スケジュール済みジョブを実行します。

ジョブの実行後、正しい VIT リスクスコアと評価が修復タスクにロールアップされます。

認定 脆弱性対応 統合のインストール

OT 脆弱性管理の機能を強化する認定サードパーティアプリケーションを統合します。

オペレーショナルテクノロジー脆弱性対応アプリケーションのオペレーショナルテクノロジー認定統合をServiceNow Storeで検索し、ご使用の環境に適用可能な統合をインストールします。

オペレーショナルテクノロジー脆弱性対応 統合

オペレーショナルテクノロジー脆弱性対応 アプリケーションには、サードパーティ統合のサポートが入っています。

現在、下記のサードパーティ統合をサポートしています。

- 脆弱性対応 for Microsoft Defender for IoT (オンプレミス管理コンソール)
- 脆弱性対応 Claroty CTD との統合。

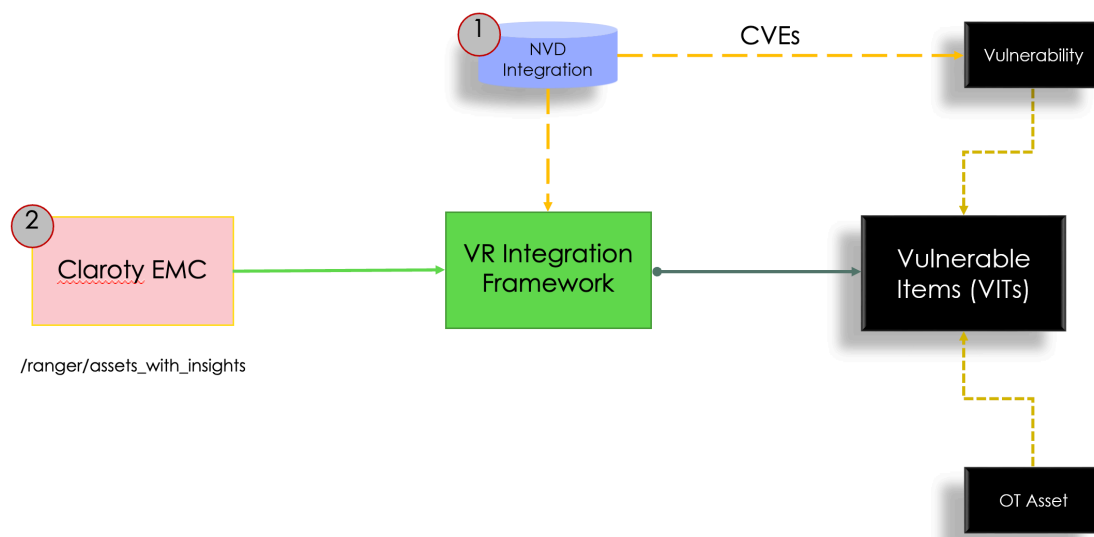
脆弱性対応 **Claroty CTD** との統合

Claroty Continuous Threat Detection (CTD) との 脆弱性対応 統合では、Claroty CTD からインポートされた脆弱性データを使用して、本番プロセス内でリスクベースのアクションを有効にします。

ServiceNow オペレーショナルテクノロジー脆弱性対応アプリケーションとのこの脆弱性対応統合を使用して、本番プロセスで使用される脆弱性を追跡、優先順位付け、および解決します。

次の画像は、Claroty CTD との 脆弱性対応 統合のプロセスを示しています。

Claroty CTD の脆弱性対応統合のプロセス



脆弱性対応 Integration with Claroty CTD を実行する前に、脆弱性情報データベース (NVD) 統合を実行する必要があります。NVD 統合は、公開されている共通脆弱性識別子 (CVE) を NVD からフェッチし、ServiceNow に入力します。その後、脆弱性対応 Integration with Claroty CTD アプリケーションを実行すると、アプリケーションは各デバイスの脆弱性を特定し、脆弱性一致アイテム (VIT) を作成します。

各 VIT は、オペレーショナルテクノロジー (OT) デバイスまたは構成アイテム (CI)、および検出された脆弱性との関係を持ちます。脆弱性統合フレームワークが Claroty Enterprise Management Console (EMC) との接続を確立し、すべての OT デバイスの脆弱性を取得します。

- 注:** Claroty CTD EMC プラットフォームインサイト API には、10 個の CVE の制限があります。したがって、Claroty によって ServiceNow に提供される CVE は 10 件のみです。ただし、xDome プラットフォームにはこの制限はありません。

主な機能

- オペレーショナルテクノロジー (OT) デバイスに関連する一般的な脆弱性とエクスポージャー (CVE) を Claroty CTD からインポートします。脆弱性一致アイテム (VIT) を作成すると、OT デバイスの脆弱性データとそれが本番プロセスに与える影響を一元的に把握できます。
- 新しく検出された脆弱性のインポートを独自のスケジュールで自動的に実行する。
- アサインルールを使用して、リスクベースのアクションを実行できるローカルサイトベースのチームに、修復のために VIT を自動的にルーティングする。

脆弱性対応 Integration with Claroty CTD のインストール

Claroty CTD (sn_clarotyctdvr) との脆弱性対応 統合をインストールし。このアプリケーションには、インストール、関連する ServiceNow Store アプリケーション、およびプラグインがまだインストールされていない場合が含まれます。

始める前に

- アプリケーションとその関連するすべての ServiceNow Store アプリケーションに有効な ServiceNow エンタイトルメントがあることを確認してください。詳細については、次を参照してください。 [のエンタイトルメントを取得する ServiceNow 製品またはアプリケーション](#)。
- 依存関係、ライセンスやサブスクリプションの要件、およびリリースの互換性については、ServiceNow Storeにある [Vulnerability Response Integration with Claroty CTD](#) アプリケーションリストを確認してください。

- 脆弱性対応 Claroty CTD との統合には、次の ServiceNow Store アプリケーションが必要です。脆弱性対応 Integration with Claroty CTD をインストールする前に、これらのアプリケーションがインストールされていることを確認してください。

CMDB CI クラスモデルストアアプリ

この統合では、オペレーショナルテクノロジー [拡張クラス](#) CMDB CI クラスモデルアプリケーションの一部です。詳細については、「[CMDB CI クラスモデル](#)」を参照してください。

Claroty CTD のサービスグラフコネクタ統合

この統合では、オペレーショナルテクノロジーマネージャー アプリケーションを使用して、サイト、各サイトで検出されたデバイス、接続 (またはベースシステム)、およびインストール済みプログラムのインポートを自動化し 構成管理データベース (CMDB)。Claroty CTD のサービスグラフコネクタ統合をインストールするには、「[脆弱性対応 Integration with Claroty CTD のインストール](#)」を参照してください。

必要なロール：admin

このタスクについて

次のアイテムは、脆弱性対応 Integration with Claroty CTD とともにインストールされます。

- 脆弱性対応プラグイン
- NVD の脆弱性対応統合

手順

- 移動先 [すべて > システムアプリケーション > 利用可能なすべてのアプリケーション > すべて](#)。
- フィルター基準と検索バーを使用して、脆弱性対応 Integration with Claroty CTD アプリケーション (sn_clarotyctdvr) を検索します。

名前または ID でアプリケーションを検索できます。アプリケーションが見つからない場合は、ServiceNow Store に要求する必要がある場合があります。

[インストール] ボタンの横のリストに、使用可能なバージョンが表示されます。

- リストからバージョンを選択し、[インストール] を選択します。

表示される [インストールの詳細を確認] ダイアログボックスに、アプリケーションとともにインストールされている依存関係が一覧表示されます。

- プロンプトが表示された場合は、ServiceNow Store へのリンクに従って、依存関係のエントリメントを取得します。
- [Install (インストール)] を選択します。

Claroty CTD との脆弱性対応 統合ロールのアサイン

ユーザーにロールをアサインして、Claroty CTD アプリケーションとの 脆弱性対応 統合の機能やデータへのアクセスを制御できるようにします。

始める前に

必要なロール：admin

このタスクについて

次のテーブルにリストされているロールがアサインされている場合は、脆弱性対応 Integration with Claroty CTD アプリケーションを使用できます。

必要に応じてアドミンユーザーまたはユーザーグループにロールをアサインします。

脆弱性対応 Integration with Claroty CTD アプリケーションで使用するロールの詳細については、「[脆弱性対応 Claroty CTD ロールとの統合](#)」を参照してください。

手順

ServiceNow AI Platformユーザー管理機能を使用して、ユーザーまたはグループにロールを割り当てます。

タスク	ユーザー管理機能
ユーザーへのロールのアサイン	ユーザーへのロールの割り当て を参照してください。
グループへのロールのアサイン	グループへのロールのアサイン を参照してください。

脆弱性対応 **Claroty CTD** ロールとの統合

ロールは、脆弱性対応 Integration with Claroty CTD の機能へのアクセスを制御します。

次の表に、脆弱性対応 Integration with Claroty CTD のロールと権限を示します。

脆弱性対応 **Claroty CTD** ロールとの統合

ロール	説明
OT VR 統合ビューアー [sn_otvr.integration_viewer]	OT VR 統合レコードを表示できます。
OT VR 統合アドミン [sn_otvr.integration_admin]	OT VR 統合を構成して実行できます。
MID サーバー [mid_server]	MID サーバーを設定できます。

Claroty CTD で必要な権限

Claroty CTDからServiceNowにデータを収集するために、次のユーザー権限での表示Claroty CTDアクセス権が有効になっていることを確認します。

- ヴィジビリティ
- 調査
- 脅威の検出
- リスクと脆弱性

National Vulnerability Database 統合の実行

脆弱性情報データベース (NVD) 統合を実行して、米国国立標準技術研究所 (NIST) の NVD 製品からデータをインポートします。NVD 統合を実行すると、環境内で見つかった共通脆弱性識別子 (CVE) の重大度と詳細を判断する際に役立ちます。

始める前に

インスタンスで NIST NVD 統合を実行する前に、インストールと構成の手順を完了する必要があります。インストールと構成を完了すると、NVD 製品が オペレーショナルテクノロジー脆弱性対応アプリケーションと適切に統合されます。

NVD プラグインをインストールするには、「[脆弱性対応 Integration with the NIST National Vulnerability Database のインストール](#)」を参照してください。

必要なロール：admin

手順

1. 移動先 **すべて** > **脆弱性対応** > **アドミニストレーション** > **統合**.
2. [NIST NVD integration - API (CVE only) (NIST NVD 統合- API (CVE のみ))] レコードを選択します。

Name	Active	Class	Updated	Source Instance
Claroty CTD Vulnerability Closure Integration	false	Claroty CTD Vulnerability Integration	2023-06-09 09:52:27	Claroty CTD
Claroty CTD Vulnerability Detection Integration - Delta Import	false	Claroty CTD Vulnerability Integration	2023-06-22 10:23:09	Claroty CTD
Claroty CTD Vulnerability Detections - Full Import	true	Claroty CTD Vulnerability Integration	2023-06-22 10:23:16	Claroty CTD
CWE Comprehensive 2000 Integration	true	Vulnerability Integration	2015-11-25 10:58:50	(empty)
Manual Ingestion CSV Integration	true	Vulnerability Integration	2022-05-22 20:50:20	Manual Ingestion
Manual Ingestion Excel Integration	true	Vulnerability Integration	2022-05-24 01:02:35	Manual Ingestion
Manual Ingestion JSON Integration	true	Vulnerability Integration	2022-05-22 21:07:45	Manual Ingestion
Manual Ingestion XML Integration	true	Vulnerability Integration	2022-05-24 01:02:56	Manual Ingestion
Microsoft D4IoT Auto-close Resolved Vulnerable Items	false	Microsoft D4IoT VR Integration	2022-03-02 21:22:20	Microsoft D4IoT Vulnerability Response L...
Microsoft D4IoT Devices CVE Integration (Delta Import)	false	Microsoft D4IoT VR Integration	2021-09-03 01:12:50	Microsoft D4IoT Vulnerability Response L...
Microsoft D4IoT Devices CVE Integration (Full Import)	false	Microsoft D4IoT VR Integration	2021-09-03 01:12:54	Microsoft D4IoT Vulnerability Response L...
Microsoft Security Response Center Solution Integration	false	Microsoft Security Response Center Solut...	2019-03-13 21:21:01	Microsoft Security Response Center Solut...
NIST National Vulnerability Database Integration - API (CVE and CPE)	false	REST Integration	2020-11-10 20:30:02	National Vulnerability Database
NIST National Vulnerability Database Integration - API (CVE only)	true	REST Integration	2023-07-11 07:13:28	National Vulnerability Database
Red Hat Solution Integration	false	Red Hat Solution Integration	2020-03-03 23:10:43	Red Hat Solution Integration

3. [インポート開始日時] フィールドで、値を **NULL** に設定します。

4. **[Execute Now (今すぐ実行)]** を選択します。

脆弱性対応 **Integration with Claroty CTD** の構成

データのインポートを開始するには、脆弱性対応 **Integration with Claroty CTD** を構成します。

Claroty CTD 脆弱性統合 ガイド付きセットアップ を使用して、構成を完了します。

Claroty CTD 脆弱性統合 ガイド付きセットアップにアクセスするには、次の場所に移動します
Claroty CTD 脆弱性統合 > **管理者** > **セットアップ**.

Claroty CTD への接続

Claroty CTD に接続して、脆弱性統合のセットアップを開始します。

始める前に

セットアップを実行する前に、ナビゲーションバーの地球儀アイコン (🌐) を選択して、アプリケーションスコープを **Claroty CTD** の脆弱性対応統合に変更します。

必要なロール：admin

手順

1. 移動先 **すべて** > **Claroty CTD 脆弱性統合** > **管理者** > **セットアップ**.
2. [Claroty CTD に接続] セクションで、[接続のセットアップ] タスクを選択します。
3. [接続のセットアップ] タスクページで、[構成] を選択します。
 [Claroty CTD Connection Manager (Claroty CTD 接続マネージャー)] ページが開きます。
4. フォームで次のフィールドに入力します。

Claroty CTD に接続フォーム

フィールド	説明
Claroty EMC URL	Claroty CTD Enterprise 管理コンソール (EMC) の URL。

フィールド	説明
最小 CVSS スコア	このフィールドは、CTD バージョンとして 5.0.x または 5.1.x を選択した場合に表示されます。 該当する場合は、共通脆弱性スコアリングシステム (CVSS) スコアに基づいてインポートする脆弱性をフィルタリングできます。フィルターは実際には 0.0 ～ 10.0 の範囲の値であり、次のフィルターとして機能します。 たとえば、スコア値を 9 と入力すると、統合によって CVSS スコアが 9.0 ～ 10.0 の脆弱性がインポートされます。
EPSS スコア (オプション)	このフィールドは、CTD バージョンとして 5.1.x 以降を選択した場合に表示されます。 該当する場合は、Exploit Prediction Scoring System (EPSS) スコアに基づいて、インポートする脆弱性をフィルタリングできます。EPSS スコアでは、フィルターとして機能する [重大]、[高]、[中]、および [低] の値が使用されます。 選択できるオプションは 1 つだけです。たとえば、EPSS スコア値として [重大] を選択した場合、Claroty CTD は EPSS スコアが [重大] の脆弱性のみをインポートします。
ユーザー名	Claroty アカウントのユーザー名。
パスワード	Claroty アカウントのパスワード。
MID サーバー	Claroty EMC がオンプレミスにある場合は、MID サーバー が必要になることがあります。その場合は、ここで MID サーバー を選択します。

5. **[Update (更新)]** を選択します。

6. **[テスト接続]** を選択します。

接続テストが成功すると、「結果 200」出力メッセージが表示されます。接続に失敗すると、エラーコードと Claroty から受信したメッセージが表示されます。

デルタインポート統合のアクティブ化

デルタインポート統合をアクティブ化して、Claroty CTD から脆弱性をインポートします。

始める前に

Claroty CTD レコードのインポートをスケジュールする前に、NVD 統合を実行して問題を修正します。詳細については、「[National Vulnerability Database 統合の実行](#)」を参照してください。

必要なロール：admin

このタスクについて

デルタインポート統合は、前回成功した統合実行からの脆弱性を Claroty CTD からインポートします。デフォルトでは、最初の実行で過去 90 日間のデータがインポートされます。[開始時間] フィールドをクリアすると、完全インポートになります。

手順

1. 移動先 **すべて > Claroty CTD 脆弱性統合 > 管理者 > セットアップ**。
2. [統合スケジュール済みジョブを構成] セクションで、[デルタインポート統合のアクティブ化] タスクを選択します。
3. [Configure] を選択します。
4. デルタインポート統合レコードが [アクティブ] に設定されていることを確認します。
5. [実行] フィールドが [オンデマンド] に設定されていることを確認します。
6. オプション: 完全インポートを実行するには、[開始時間] フィールドをクリアします。
7. [Update (更新)] を選択します。

サービスグラフコネクタの後に脆弱性統合を実行します

Claroty CTD のサービスグラフコネクタを実行した後、Claroty CTD 脆弱性統合を実行します。サービスグラフコネクタを実行した直後に脆弱性統合を実行すると、Claroty CTD から最新の CMDB 情報が入力されます。

始める前に

サービスグラフコネクタの後に実行する 脆弱性対応 統合を実行するには、Claroty CTD のサービスグラフコネクタ統合を設定してアクティブにする必要があります。

Claroty CTD レコードのインポートをスケジュールする前に、NVD 統合を実行して問題を修正します。詳細については、「[National Vulnerability Database 統合の実行](#)」を参照してください。

必要なロール: admin

手順

1. 移動先 **すべて > Claroty CTD 脆弱性統合 > 管理者 > セットアップ**。
2. [統合スケジュール済みジョブを構成] タスクで、[サービスグラフコネクタの後に実行] タブを選択します。
3. [Configure] を選択します。
4. [SGC - Claroty CTD 脆弱性検出統合:デルタインポート後に実行] レコードで、[アクティブ] オプションを選択してアクティブ化します。
5. [実行] フィールドが [親の実行後] に設定されていることを確認します。
6. [親] フィールドが [SG-OT Claroty CTD 資産のスケジュール済みインポート] に設定されていることを確認します。
7. [Update (更新)] を選択します。

自動クローズ統合のアクティブ化

自動クローズ統合をアクティブ化して、対応する ServiceNow 脆弱性検出をクローズします。

始める前に

Claroty CTD レコードのインポートをスケジュールする前に、NVD 統合を実行して問題を修正します。詳細については、「[National Vulnerability Database 統合の実行](#)」を参照してください。

必要なロール：admin

このタスクについて

脆弱性対応と Claroty CTD の統合では、次の 2 つのクローズ統合ジョブを利用できます。

- Claroty CTD 解決済み脆弱性クローズ統合
- Claroty CTD 完全脆弱性クローズ統合

Claroty CTD の解決済み脆弱性クローズ統合は、ServiceNow 構成管理データベース (CMDB) で解決済みとしてマークされた脆弱性一致アイテム (VIT) をチェックします。次に、Claroty CTD にこれらの VIT を照会し、Claroty CTD から得られた応答に基づいて VIT をクローズします。

Claroty CTD の完全な脆弱性クローズ統合は、ServiceNow CMDB 内のステータス (解決済みかどうか) に関係なく、すべての VIT をチェックします。次に、Claroty CTD にすべての VIT のクエリを実行し、Claroty CTD に対応する CVE エントリーがない VIT をクローズします。

手順

1. 移動先 **すべて > Claroty CTD 脆弱性統合 > 管理者 > セットアップ**。
2. [統合スケジュール済みジョブを構成] タスクで、[自動クローズ統合のアクティブ化] タブを選択します。
3. [Configure] を選択します。

i 注：自動クローズ統合は、デルタインポート後に実行するように事前設定されているため、スケジュールは必要ありません。

4. [実行] フィールドが [オンデマンド] に設定されていることを確認します。
5. レコードが [アクティブ] に設定されていることを確認します。
6. [Update (更新)] を選択します。

Claroty CTD からの完全インポート統合の構成

Claroty CTD からデバイスの脆弱性インベントリ全体をインポートするように完全インポート統合を構成します。

始める前に

Claroty CTD レコードのインポートをスケジュールする前に、NVD 統合を実行して問題を修正します。詳細については、「[National Vulnerability Database 統合の実行](#)」を参照してください。

必要なロール：admin

このタスクについて

Claroty CTD 脆弱性検出:完全インポート統合では、特定の日付に関係なく、デバイスの脆弱性インベントリ全体を Claroty CTD からインポートします。この統合は、日次デルタインポートで必要な脆弱性データのすべてがインポートされていない場合に便利です。

- i** 注：Claroty CTD v5.1 を使用している場合、構成アイテム (CI) ごとにインポートできる共通脆弱性識別子 (CVE) の数に制限はありません。バージョン 5.0.x 以前のバージョンの Claroty CTD を使用している場合、インポートできる CVE の数は CI ごとに 10 に制限されています。

Claroty CTD のオペレーショナルテクノロジー脆弱性対応統合の使用の詳細については、「[Claroty CTD への接続](#)」を参照してください。

手順

1. 移動先 すべて > **Claroty CTD** 脆弱性統合 > 管理者 > セットアップ。
2. [統合スケジュール済みジョブを構成] タスクで、[完全インポート統合を構成] タブを選択します。
3. [Configure] を選択します。
4. [実行] フィールドが [オンデマンド] に設定されていることを確認します。
5. レコードが [アクティブ] に設定されていることを確認します。
6. [Update (更新)] を選択します。

Claroty CTD との脆弱性対応 統合のためにインストールされるシステムプロパティを設定します

脆弱性対応 Integration with Claroty CTD のシステムプロパティを設定して、必要に応じてプロパティを有効にできるようにします。

始める前に

セットアップを実行する前に、ナビゲーションバーの地球儀アイコン (🌐) を選択して、アプリケーションスコープを **Vulnerability Response Integration with Claroty CTD** に変更します。

必要なロール:sn_otvr.integration_admin

手順

1. 移動先 すべて > **Claroty CTD** 脆弱性統合 > 管理者 > プロパティ
2. 組織の要件に応じて、次のシステムプロパティレコードを設定します。

システムプロパティ

名前	説明	タイプ	デフォルト値
sn_clarotyctdvr.api_token_expiry	Claroty CTD API トークンが有効である時間の長さ。デフォルトは 480 分 (8 時間) です。	整数	480
sn_clarotyctdvr.api_token_scope	API のアクセスを確認します。	文字列	{"customer_name":"","first_name":"AFのサービス","id":1,"last_name":null,"mail":null,""
sn_clarotyctdvr.auto_close_old_detections	Claroty CTD の古い脆弱性検出を自動的にクローズします。	True、False	false
sn_clarotyctdvr.auto_close_old_detections_days	Claroty CTD の検出は、最後に検出されてから指定された日数が経過すると自動的にクローズされます。	整数	90
sn_clarotyctdvr.default_page_size	Claroty CTD API からページごとにプルするレコードの数。	整数	500
sn_clarotyctdvr.detect_start_buffer	Claroty CTD API からデータをインポートする場合、「開始時	整数	4

名前	説明	タイプ	デフォルト値
	間」の前に指定された時間数のバッファが追加されます。これにより、デルタインポートでレコードが失われることがなくなります。		
sn_clarotyctdvr.integration_delta_days	デフォルトでは、統合の最初の実行時に、過去の日数からデータがインポートされます。	整数	90
sn_clarotyctdvr.logging verbosity	アプリケーションログレベル	選択	情報
sn_clarotyctdvr.require_validation	脆弱性検出を作成するには、受信 CI が CMDB と一致する必要があります。	True、False	true

3. [更新] を選択し、変更を保存します。

Claroty CTD との脆弱性対応 統合のデータマッピング

このセクションでは、Claroty CTD API のフィールドを ServiceNow テーブルのフィールドにマッピングする方法を指定します。

脆弱性検出データマッピング

Claroty CTD フィールド	ServiceNow フィールド	メモ
	ソース	常に Claroty CTD に設定します。
Identified_on	初回検出	
Last_updated	前回検出	
ステータス	ステータス	ステータス 0 は オープンを意味します。 ステータス 2 は、[クローズ済み]/[修正済み] を意味します。
Resource_id	構成アイテム	構成アイテム (CI) は、sys_object_source テーブルでリソース ID を検索する CI ルックアップルールによって設定されます。例:33.1。

脆弱性エントリーデータのマッピング

脆弱性エントリーは、既存の共通脆弱性識別子 (CVE) レコードが脆弱性情報データベース エントリー [sn_vul_nvd_entry] テーブルに見つからない場合にのみ作成されます。Claroty CTD 統合で CVE を作成する必要がある場合は、テーブルにリストされている次のソースフィールドをマッピングします。

Claroty CTD フィールド	ServiceNowフィールド	メモ
Cve_id	ID	例:CVW-2017-17562
タイトル	サマリー	統合により、[Claroty] がサマリーに追加され、Claroty によってバックフィルされた NVD CVE が表示されるようになります。たとえば、SIPROTECの[Claroty]認証バイパスの脆弱性。
CVSS	V3_base_score	
公開済み	Date_published	
変更	Last_modified	

Claroty CTD との脆弱性対応 統合に関するエラー

脆弱性対応 Integration with Claroty CTD を使用しているときに、トラブルシューティングが必要なエラーが発生する場合があります。

脆弱性検出統合 (データ検索)

エラーメッセージ	考えられる原因
ユーザー名とパスワードの組み合わせなしで Claroty CTD 統合を実行することはできません。	統合構成にユーザー名またはパスワードが存在しません。
REST メッセージと REST メソッドを指定せずに統合を実行することはできません。	Claroty CTD 統合ジョブレコードで、[REST メッセージ] フィールドまたは [REST メソッド] フィールドに値が入力されません。
Claroty CTD サーバーの URL を指定せずに統合を実行することはできません。	統合構成に URL が存在しません。
検出 API リソースパスを指定せずに統合を実行することはできません。	統合構成では、detection_api_resource_path パラメーターが入力されていません。デフォルトは /ranger/assets_with_insights です。
Claroty CTD から無効な応答コード {応答コード} を受信しました。	Claroty API からの応答が無効でした。たとえば、Claroty CTD から「無効な応答コード 401」というメッセージを受信しました。この無効な応答コードは、権限がなく、認証情報 (ユーザー名/パスワード) が無効である可能性が高いことを意味します。
JSON データからcount_totalプロパティを読み取ることができません。	ページネーションに使用されるcount_total が API 応答に存在しませんでした。これは、Claroty CTD から無効なペイロードが受信されたことを意味します。 Claroty CTD インスタンスが MID サーバーを介して到達可能であることを確認し、データソースの添付ファイルの response.json ファイルを調べて、count_totalが存在することを確認します。

脆弱性検出統合 (データ処理)

エラーメッセージ	考えられる原因
添付ファイルの書き込み中にエラーが発生しました。	応答データをデータソースに添付できませんでした。詳細については、アドミニストレーターにお問い合わせください。 このエラーの一般的な原因は、MID サーバーユーザーに <code>sn_vul.vr_import_admin</code> ロールがないことです。
添付ファイルのコンテンツが null:添付ファイル <code>sys_id = {sys_id}</code> 。	データソースの添付ファイルの内容が null です。これは、Claroty API 自体の問題、または ServiceNow の問題を示している可能性があります。詳細については、アドミニストレーターにお問い合わせください。
<code>sys_id {sys_id}</code> の添付ファイルが見つかりませんでした。	データソースの添付ファイルが見つかりませんでした。前のエラーと同じ手順に従います。

脆弱性自動クローズ統合 (データ検索)

エラーメッセージ	考えられる原因
ユーザー名とパスワードの組み合わせなしで Claroty CTD 統合を実行することはできません。	統合構成にユーザー名またはパスワードが存在しません。
REST メッセージと REST メソッドを指定せずに統合を実行することはできません。	Claroty CTD 統合ジョブレコードで、[REST メッセージ] フィールドまたは [REST メソッド] フィールドに値が入力されません。
Claroty CTD サーバーの URL を指定せずに統合を実行することはできません。	統合構成に URL が存在しません。
検出 API リソースパスを指定せずに統合を実行することはできません。	統合構成では、 <code>detection_api_resource_path</code> パラメーターが入力されていません。デフォルトは <code>/ranger/assets_with_insights</code> です。
Claroty CTD から無効な応答コード {応答コード} を受信しました。	Claroty API からの応答が無効でした。たとえば、Claroty CTD から「無効な応答コード 401」というメッセージを受信しました。この無効な応答コードは、権限がなく、認証情報 (ユーザー名/パスワード) が無効である可能性が高いことを意味します。
JSON データから <code>count_total</code> プロパティを読み取ることができません。	ページネーションに使用される <code>count_total</code> が API 応答に存在しませんでした。これは、Claroty CTD から無効なペイロードが受信されたことを意味します。 Claroty CTD インスタンスが MID サーバーを介して到達可能であることを確認し、データソースの添付ファイルの <code>response.json</code> ファイルを調べて、 <code>count_total</code> が存在することを確認します。

エラーメッセージ	考えられる原因
応答本文の「オブジェクト」アレイの解析中にエラーが発生しました。	Claroty CTD から無効なペイロードが受信されたことを意味すると考えられます。Claroty CTD インスタンスが到達可能であることを確認し、送信 HTTP ログをチェックして有効な応答があったかどうかを確認します。

脆弱性自動クローズ統合 (データ処理)

エラーメッセージ	考えられる原因
データディクショナリ JSON の解析に失敗しました。	データソース添付ファイルからのペイロードが無効な JSON でした。このエラーが発生する前に、別のエラーが発生している可能性があります。Claroty CTD インスタンスが到達可能であることを確認し、送信 HTTP ログをチェックして有効な応答があったかどうかを確認します。

脆弱性対応 Microsoft Defender for IoT (Azure) との統合

脆弱性対応 Integration with Microsoft Defender for IoT (Azure) では、Microsoft Defender for IoT (Azure) からインポートされたデータを使用して、本番プロセスコンテキストでリスクベースのアクションを有効にします。

ServiceNow オペレーショナルテクノロジー脆弱性対応 アプリケーションとの 脆弱性対応 統合を使用して、本番プロセスで使用されるデバイスの脆弱性を追跡し、優先順位を付けて解決します。

主な機能

- Microsoft Defender for IoT (Azure) から OT に関連付けられた CVE をインポートし、脆弱性一致アイテム (VIT) を作成して、本番プロセスのコンテキストで OT デバイスの脆弱性データを一目で見られるビューを作成します。
- 脆弱性のインポートを独自のスケジュールで自動的に実行します。
- アサインルールを使用すると、リスクベースのアクションを実行できるローカルサイトベースのチームに、修復のために VIT を自動的にルーティングできます。

Microsoft Defender for IoT 用の 脆弱性対応 のインストール (Azure)

admin ロールをお持ちであれば、Microsoft Defender for IoT (Azure) 脆弱性対応をインストールできます。このアプリケーションには、インストール、関連する ServiceNow Store アプリケーション、プラグインが含まれます (まだインストールされていない場合)。

始める前に

- アプリケーションとその関連するすべての ServiceNow Store アプリケーションに有効な ServiceNow エンタイトルメントがあることを確認してください。詳細については、次を参照してください。 [エンタイトルメントを取得する ServiceNow 製品またはアプリケーション](#)。
- 次のものをレビュー [脆弱性対応 for Microsoft Defender for IoT \(Azure\)](#)。依存関係、ライセンスやサブスクリプションの要件、およびリリースの互換性については、ServiceNow Store のアプリケーションリスト。
- 脆弱性対応 for Microsoft Defender for IoT (Azure) には次の ServiceNow Store アプリケーションが必要です。Microsoft Defender for IoT との 脆弱性対応 統合をインストールする前に、これらのアプリケーションがインストールされていることを確認してください。

CMDB CI クラスモデルストアアプリ

この統合では、オペレーショナルテクノロジー [拡張クラス](#) CMDB CI クラスモデルアプリケーションの一部です。詳細については、「[CMDB CI クラスモデル](#)」を参照してください。

サービスグラフ コネクタ Microsoft Defender for IoT (Azure)

この統合では、オペレーショナルテクノロジーマネージャー アプリケーションを使用して、センサーアプライアンス、OT デバイス、およびネットワーク接続のインポートを自動化します。サービスグラフをインストールするには、「[サービスグラフ コネクタ Microsoft Defender for IoT \(Azure\)](#)」を参照してください。

必要なロール：admin

このタスクについて

次のアイテムは、脆弱性対応 for Microsoft Defender for IoT (Azure) とともにインストールされます。

- 脆弱性対応プラグイン
- NVD の脆弱性対応統合

手順

1. 移動先 **すべて > システムアプリケーション > 利用可能なすべてのアプリケーション > すべて**.
2. フィルター基準と検索バーを使用して、脆弱性対応 Integration for Microsoft Defender for IoT (Azure) を検索します。

名前またはアプリケーションスコープ ID でアプリケーションを検索できます。アプリケーションが見つからない場合は、アプリケーションを同期するか、ServiceNow Store に要求してインスタンスに資格を付与する必要があります。

[インストール] ボタンの横のリストに、使用可能なバージョンが表示されます。

3. リストからバージョンを選択し、[インストール] を選択します。

表示される [インストールの詳細を確認] ダイアログボックスに、アプリケーションとともにインストールされている依存関係が一覧表示されます。

4. プロンプトが表示された場合は、ServiceNow Store へのリンクに従って、依存関係のエントリメントを取得します。
5. **[Install (インストール)]** を選択します。

脆弱性対応 **Integration with Microsoft Defender for IoT (Azure)** のガイド付きセットアップに移動

脆弱性対応 Integration with Microsoft Defender for IoT (Azure) をインストールした後、ガイド付きセットアップに移動してアプリケーションの構成を順を追って説明します。

始める前に

ナビゲーションバーの地球アイコン (🌐) を選択して、アプリケーションスコープを Microsoft Defender for IoT (Azure) との脆弱性対応統合に変更します。

必要なロール：admin

手順

1. 移動先 **すべて > Azure D4IoT 脆弱性統合 > 管理者 > ガイド付きセットアップ**.
2. **[Get Started (開始する)]** を選択します。

Microsoft Defender for IoT (Azure) に接続

Microsoft Defender for IoT (Azure) に接続して、脆弱性統合のセットアップを開始します。

始める前に

Microsoft Defender for IoT Azure でセキュリティ閲覧者アクセス許可が有効になっており、次のユーザー アクションが提供されていることを確認します。

- センサーエンドポイントの詳細をダウンロード
- [サイトとセンサー] ページで値を表示する
- Azure デバイスインベントリの表示
- Azure ワークブックを表示
- Defender for IoT の設定を表示する
- OT 脅威インテリジェンスパッケージをダウンロード

詳細については、次を参照してください。 [Defender for IoT の Azure ユーザー ロールとアクセス許可](#)。

必要なロール：admin

手順

1. 移動先 **すべて > Azure D4IoT 脆弱性統合 > 管理者 > ガイド付きセットアップ**。
2. [Microsoft Defender for IoT (Azure) に接続] セクションで、[接続のセットアップ] タスクを選択します。
3. [接続のセットアップ] タスクページで、[構成] を選択します。
[Microsoft Azure Defender for IoT に接続] ページが開きます。
4. フォームで次のフィールドに入力します。

[Microsoft Azure Defender for IoT に接続] フォーム

フィールド	説明
OAuth トークン URL	login.microsoftonline.com の OAuth 2.0 トークン URL。例: https://login.microsoftonline.com/<your tenant id>/oauth2/v2.0/token。
OAuth クライアント ID	クライアント ID。
OAuth クライアントシークレット	クライアントシークレット。
ページサイズ制限	データの各ページにプルするレコードの最大数。デフォルトは 500 です。
最小 CVSS スコア	CVSS スコアがこの値以上の脆弱性のみがインポートされます。すべての脆弱性のデフォルトは 0.0 です。
サービスグラフコネクタのインポート後に実行	これは、Microsoft Defender for IoT (Azure) のサービスグラフコネクタデバイスのインポートが完了した直後に脆弱性インポートを実行する推奨フィールドです。これにより、受信する脆弱性データを CMDBと照合する可能性が最も高くなります。

フィールド	説明
	最も一般的な値は、SG-OT Microsoft Azure D4IoT デバイスのスケジュール済みインポートです。このフィールドを選択するときは、[Azure D4IoT 脆弱性検出統合 - フルインポート] スケジュール済みジョブを [オンデマンドで実行] に設定したままにしておきます。これにより、デバイスのインポートが完了した後、サービスグラフコネクタデバイスのインポートでこれを子ジョブとして実行できるようになります。
日次インポート時間	[サービスグラフコネクタのインポート後に実行] フィールドを使用していない場合は、このフィールドを使用して統合の日次インポート時間を設定できます。  注: [サービスグラフコネクタのインポート後に実行] フィールドでインポートスケジュールが選択されている場合、このフィールドは使用できません。

5. [Update (更新)] を選択します。

6. [テスト接続] を選択します。

接続テストが成功すると、「結果 200」出力メッセージが表示されます。接続に失敗すると、エラーコードと Microsoft Defender for IoT (Azure) から受信したメッセージが表示されます。

National Vulnerability Database 統合の実行

脆弱性情報データベース (NVD) 統合を実行して、米国国立標準技術研究所 (NIST) の NVD 製品からデータをインポートします。NVD 統合を実行すると、Microsoft Defender for IoT (Azure) の脆弱性によって参照される基本的な共通脆弱性識別子 (CVE) データが提供され、環境内の脆弱性の重大度と詳細を判断するのに役立ちます。

始める前に

インスタンスで NIST NVD 統合を実行する前に、統合のインストールと構成の手順を完了する必要があります。インストールと構成を完了すると、NVD 製品が オペレーショナルテクノロジー脆弱性対応 アプリケーションと適切に統合されます。

NVD プラグインをインストールするには、「[脆弱性対応 Integration with the NIST National Vulnerability Database のインストール](#)」を参照してください。

必要なロール：admin

手順

1. 移動先 **すべて > Azure D4IoT 脆弱性統合 > 管理者 > ガイド付きセットアップ**。
2. [統合を構成] セクションで、[脆弱性情報データベース (NVD) CVE エントリをインポート] タスクの横にある [構成] を選択します。
3. どちらがアクティブかに応じて、[NIST NVD 統合 - API (CVE のみ)] レコードまたは [NIST 脆弱性情報データベース統合 - API (CVE および CPE)] レコードのいずれかを選択します。

- i** 注: NIST NVD 統合 - API (CVE のみ) レコードは、デフォルトで最も一般的にアクティブです。

Name	Active	Class	Updated	Source Instance
Claroty CTD Vulnerability Closure Integration	false	Claroty CTD Vulnerability Integration	2023-06-09 09:52:27	Claroty CTD
Claroty CTD Vulnerability Detection Integration - Delta Import	false	Claroty CTD Vulnerability Integration	2023-06-22 10:23:09	Claroty CTD
Claroty CTD Vulnerability Detections - Full Import	true	Claroty CTD Vulnerability Integration	2023-06-22 10:23:16	Claroty CTD
CWE Comprehensive 2000 Integration	true	Vulnerability Integration	2015-11-25 10:58:50	(empty)
Manual Ingestion CSV Integration	true	Vulnerability Integration	2022-05-22 20:50:20	Manual Ingestion
Manual Ingestion Excel Integration	true	Vulnerability Integration	2022-05-24 01:02:35	Manual Ingestion
Manual Ingestion JSON Integration	true	Vulnerability Integration	2022-05-22 21:07:45	Manual Ingestion
Manual Ingestion XML Integration	true	Vulnerability Integration	2022-05-24 01:02:56	Manual Ingestion
Microsoft D4IoT Auto-close Resolved Vulnerable Items	false	Microsoft D4IoT VR Integration	2022-03-02 21:22:20	Microsoft D4IoT Vulnerability Response L...
Microsoft D4IoT Devices CVE Integration (Delta Import)	false	Microsoft D4IoT VR Integration	2021-09-03 01:12:50	Microsoft D4IoT Vulnerability Response L...
Microsoft D4IoT Devices CVE Integration (Full Import)	false	Microsoft D4IoT VR Integration	2021-09-03 01:12:54	Microsoft D4IoT Vulnerability Response L...
Microsoft Security Response Center Solution Integration	false	Microsoft Security Response Center Solut...	2019-03-13 21:21:01	Microsoft Security Response Center Solut...
NIST National Vulnerability Database Integration - API (CVE and CPE)	false	REST Integration	2020-11-10 20:30:02	National Vulnerability Database
NIST National Vulnerability Database Integration - API (CVE only)	true	REST Integration	2023-07-11 07:13:28	National Vulnerability Database
Red Hat Solution Integration	false	Red Hat Solution Integration	2020-03-03 23:10:43	Red Hat Solution Integration

4. レコードを編集するには、地球儀アイコン (🌐) を使用して、アプリケーションスコープを **NVD** の脆弱性対応統合に設定します。

5. [統合の詳細] タブの [次以降にインポート] フィールドで、値を過去の日付に設定します。

- i** 注: これは、NVD の完全インポートを実行するために必要です。推奨される日付は 1999-01-01 00:00:00 です。

6. [Save (保存)] を選択します。

7. [Execute Now (今すぐ実行)] を選択します。

統合スケジュール済みジョブの構成

脆弱性データをインポートするスケジュール済みジョブをアクティブ化します。

始める前に

Microsoft Defender for IoT (Azure) レコードのインポートをスケジュールする前に、NVD 統合を実行して問題を修正します。詳細については、「[National Vulnerability Database 統合の実行](#)」を参照してください。

必要なロール: admin

手順

1. 移動先 **すべて > Azure D4IoT 脆弱性統合 > 管理者 > ガイド付きセットアップ**。
2. [統合の構成] セクションで、[統合スケジュール済みジョブの検証とアクティブ化] タスクの横にある [構成] を選択します。
3. [Azure D4IoT 脆弱性検出統合 - 完全インポート] ジョブを選択します。
このジョブは、Microsoft Defender for IoT (Azure) から脆弱性検出をインポートします。
4. [アクティブ] フィールドの横にあるチェックボックスをオンにします。
追加の変更が必要な場合は、スケジュールを調整することもできます。[接続のセットアップ] タスクで [サービスグラフコネクタのインポート後に実行] に脆弱性統合を構成した場合は、このジョブをオンデマンドで実行するように設定したままにしておく必要があります。[接続のセットアップ] タスクの詳細については、「[Microsoft Defender for IoT \(Azure\) に接続](#)」を参照してください。
5. [Update (更新)] を選択します。

6. **[Azure D4IoT 脆弱性クローズ統合 (Azure D4IoT Vulnerability Closure Integration)]** ジョブを選択します。

Azure D4IoT 脆弱性クローズ統合 は、Microsoft Defender for IoT (Azure) から削除された検出を特定し、ServiceNowでクローズする検出ジョブです。

7. [アクティブ] フィールドの横にあるチェックボックスをオンにします。
[実行] フィールドは [オンデマンド] のままにすることをお勧めします。

8. **[Update (更新)]** を選択します。

[古い検出を自動クローズ] をアクティブ化

古い検出の自動クローズプロセスで使用されるシステムプロパティを構成して、環境に存在しなくなった脆弱性を自動的にクローズします。

始める前に

必要なロール：admin

手順

1. 移動先 すべて > **Azure D4IoT 脆弱性統合** > 管理者 > ガイド付きセットアップ。
2. [古い検出を自動クローズ (オプション)] セクションで、[古い検出の自動クローズをアクティブ化] タスクを選択します。
3. **[Configure]** を選択します。
4. **[Azure D4IoT VR 自動クローズのプロパティ]** ページの **[Microsoft Azure Defender for IoT の古い検出を自動クローズしますか?]** フィールドで、[はい] を選択します。
5. [Microsoft Azure Defender for IoT の検出は、更新されてから (値) 日後に自動的にクローズされます] フィールドに、検出が自動的にクローズされるまで待機する日数を入力します。
デフォルトは 90 です。
6. **[Save (保存)]** を選択します。

[古い検出を自動クローズ] ジョブのアクティブ化

スケジュール済みジョブをアクティブ化して、古い検出を繰り返し自動クローズします。

始める前に

必要なロール：admin

手順

1. 移動先 すべて > **Azure D4IoT 脆弱性統合** > 管理者 > ガイド付きセットアップ。
2. [古い検出を自動クローズ (オプション)] セクションで、[古い検出のスケジュール済みジョブの自動クローズをアクティブ化] タスクを選択します。
3. **[Configure]** を選択します。
4. [アクティブ] フィールドの横にあるチェックボックスをオンにします。
5. オプション: [実行] フィールドで、ニーズに合ったオプションを選択します。
デフォルトでは、このフィールドは [オンデマンド] に設定されていますが、必要に応じて変更できます。たとえば、[日次] を選択し、表示される [時間] フィールドでその日の時間と分を選択できます。
6. **[Save (保存)]** を選択します。

Microsoft Defender for IoT (Azure) との 脆弱性対応 統合のサポート

データマッピングとエラー処理に関する質問については、このセクションを参照してください。

データマッピング

次の表では、Microsoft Defender for IoT (Azure) アプリケーションの脆弱性検出と脆弱性情報データベース (NVD) エントリに使用されるデータマッピングフィールドと、データが ServiceNow CMDB にインポートされた後に同等のエントリが使用されるかどうかについて説明します。

脆弱性検出

[Microsoft Defender for IoT (Azure)] フィールド	ServiceNowフィールド
該当なし	ソース i 注: このフィールドは常に Microsoft Azure Defender for IoT に設定してください。
名前	detection_key
該当なし	ステータス i 注: このフィールドはデフォルトで 0 (オープンを意味する) に設定されています。

NVD エントリ

[Microsoft Defender for IoT (Azure)] フィールド	ServiceNowフィールド
プロパティ/vulnerabilityId	ID
	ソース i 注: このフィールドはデフォルトで NVD に設定されています。
プロパティ/説明	まとめ
プロパティ/スコア	score
プロパティ/エクスプロイトタイプ	エクスプロイト有無 API データがエクスプロイトが存在することを示している場合、統合によってこのフィールドは [はい] に設定されます。
プロパティ/エクスプロイトタイプ	public_exploit API データがエクスプロイトが存在することを示している場合、統合によってこのフィールドは [はい] に設定されます。

構成アイテム (CI) ルックアップ

CI ルックアップは、Microsoft Defender for IoT (Azure) の **deviceid** を使用して実行されます。サービスグラフコネクタによって入力される `sys_object_source` テーブルで、一致する `deviceid` が検索されます。一致が見つかったら、検出と脆弱性一致アイテムがその CI にリンクされます。

- i 注:** デフォルトでは、脆弱性検出を挿入するには CI 一致が必要です。これにより、CMDB内の未分類のハードウェア CI を最小限に抑えることができます。この動作を変更するには、**sn_msft4iotazvr.require_ci_matchsystem** プロパティを **false** に設定します。プロパティを **false** に設定すると、CI の一致が見つからない場合に、未分類のハードウェア CI を作成できます。

エラー処理

統合は、ほとんどが事前構成されるように設計されているため、Azure テナント ID、クライアント ID、クライアントシークレットを入力するだけで済みます。アプリケーションからのログメッセージは、**sn_msft4iotazvr** ソースからのシステムログで確認できます。追加の関連ログメッセージも、**sn_vul** ソースから表示できます。

統合の実行が失敗した場合、統合実行の [メモ] フィールドにエラーが表示されます。ステータスは [完了] に設定され、サブステータスは [失敗] になります。

インポートキュー (`sn_vul_ds_import_q_entry`) テーブルには、すべての処理待ちの変換要求が含まれています。このテーブルをフィルタリングしてステータスが [処理中] のアイテムのみを表示し、現在変換中のアイテムを表示できます。

次の表に、データ取得およびデータ処理中に考えられるエラーメッセージと考えられる原因を示します。

脆弱性検出統合 (データ検索)

エラーメッセージ	考えられる原因
REST メッセージと REST メソッドを指定せずに統合を実行することはできません	検出統合ジョブレコードで、[REST メッセージ] フィールドまたは [REST メソッド] フィールドに値が入力されません。
Microsoft Defender for IoT (Azure) <code>oauth_client_id</code> を指定せずに統合を実行することはできません	統合インスタンスで、 OAuth クライアント ID が入力されません。
Microsoft Defender for IoT (Azure) <code>oauth_client_secret</code> が指定されていないと統合を実行できません	統合インスタンスでは、 OAuth クライアントシークレット が入力されません。
Cannot run integration without the detection API resource path specified (検出 API リソースパスを指定しないと統合を実行できません)	統合インスタンスで、検出 API リソースパスが入力されていません。 デフォルトは https://management.azure.com/providers/Microsoft.ResourceGraph/resources です
指定された API バージョンとの統合を実行できません	統合インスタンスでは、API バージョンが入力されていません。 デフォルトは 2021-03-01 です。

脆弱性検出統合 (データ検索) (続く)

エラーメッセージ	考えられる原因
Microsoft Defender for IoT (Azure) から無効な応答コード {応答コード} を受信しました	Microsoft API からの応答が無効です。 たとえば、Microsoft Defender for IoT (Azure) から受信した無効な応答コード 401 は、権限がないことを意味します。認証情報または OAuth トークンが無効である可能性があります。
JSON 応答本文の解析に失敗しました	解析できない場合、受信した JSON 応答は無効です。これは、データが受信されなかったことを意味します。認証情報が正しいこと、および他のエラーが発生していないことを確認します。
Error writing attachment (添付ファイル書き込みエラー)	応答データをデータソースに添付できませんでした。さらにトラブルシューティングを行う場合は、システムアドミニストレーターに問い合わせる必要があります。このエラーの一般的な原因は、MID サーバーまたは 実行ユーザーに sn_vul.vr_import_admin ロールがないことです。
Attachment content is null: attachment sys_id = {sys_id} (添付ファイルの内容が null です: 添付ファイル sys_id = {sys_id})	データソースの添付ファイルの内容が null です。これは、Microsoft API 自体の問題、または ServiceNow の問題を示している可能性があります。より詳細なトラブルシューティングをシステムアドミニストレーターに依頼してください。
Could not find attachment with sys_id {sys_id} (sys_id {sys_id} の添付ファイルが見つかりませんでした)	データソースの添付ファイルが見つかりませんでした。これは、Microsoft API 自体の問題、または ServiceNow の問題を示している可能性があります。より詳細なトラブルシューティングをシステムアドミニストレーターに依頼してください。

脆弱性検出統合 (データ処理)

エラーメッセージ	考えられる原因
脆弱性 ID なしで検出を作成することはできません	レコードの脆弱性 ID が存在しません。これは、Microsoft API の問題が原因である可能性が最も高いです。

脆弱性対応 for Microsoft Defender for IoT (オンプレミス管理コンソール)

Microsoft Defender for IoT (オンプレミス管理コンソール) の脆弱性対応では、Microsoft Defender for IoT (オンプレミス管理コンソール) からインポートされたデータを使用して、本番プロセスコンテキストでリスクベースのアクションを有効にします。

脆弱性対応 for Microsoft Defender for IoT (オンプレミス管理コンソール) アプリケーションを使用して、本番プロセスで使用するデバイスの脆弱性を追跡し、優先順位を付けて解決します。

主な機能

- Microsoft Defender for IoT (オンプレミス管理コンソール) から OT デバイスに関連付けられた CVE をインポートし、脆弱性一致アイテム (VIT) を作成して、本番プロセスのコンテキストとともに OT デバイス脆弱性データの単一のビューを提供します。
- 新しく検出された脆弱性のインポートを独自のスケジュールで自動的に実行する。
- VIT のアサインルールを使用して、リスクベースのアクションを実行できるローカルサイトベースのチームに、修復のために VIT を自動的にルーティングできます。

Microsoft Defender for IoT 用の脆弱性対応のインストール (オンプレミス管理コンソール)

admin ロールを持っている場合は、Microsoft Defender for IoT (オンプレミス管理コンソール) 用の脆弱性対応をインストールできます。このアプリケーションには、インストール、関連する ServiceNow Store アプリケーション、プラグインが含まれます (まだインストールされていない場合)。

始める前に

- アプリケーションとその関連するすべての ServiceNow Store アプリケーションに有効な ServiceNow エンタイトルメントがあることを確認してください。詳細については、次を参照してください。 [のエンタイトルメントを取得する ServiceNow 製品またはアプリケーション](#)。
- 次のものをレビュー [脆弱性対応 for Microsoft Defender for IoT \(オンプレミス管理コンソール\)](#)。依存関係、ライセンスやサブスクリプションの要件、およびリリースの互換性については、ServiceNow Store のアプリケーションリスト。
- 脆弱性対応 for Microsoft Defender for IoT (オンプレミス管理コンソール) には次の ServiceNow Store アプリケーションが必要です。Microsoft Defender for IoT との脆弱性対応統合をインストールする前に、これらのアプリケーションがインストールされていることを確認してください。

CMDB CI クラスモデルストアアプリ

この統合では、オペレーショナルテクノロジー [拡張クラス](#) CMDB CI クラスモデルアプリケーションの一部です。詳細については、「[CMDB CI クラスモデル](#)」を参照してください。

サービスグラフ コネクタ Microsoft Defender for IoT (オンプレミス)

この統合では、オペレーショナルテクノロジー マネージャー アプリケーションを使用して、センサーアプライアンス、OT デバイス、およびネットワーク接続のインポートを自動化します。サービスグラフをインストールするには、「[サービスグラフ Connector for Microsoft Defender for IoT \(オンプレミス管理コンソール\)](#)」を参照してください。

必要なロール：admin

このタスクについて

次のアイテムは、脆弱性対応 for Microsoft Defender for IoT (オンプレミス管理コンソール) とともにインストールされます。

- 脆弱性対応プラグイン
- NVD の脆弱性対応統合

手順

1. 移動先 [すべて > システムアプリケーション > 利用可能なすべてのアプリケーション > すべて](#)。
2. フィルター基準と検索バーを使用して、Microsoft Defender for IoT (オンプレミス管理コンソール) の脆弱性対応を検索します。

名前または ID でアプリケーションを検索できます。アプリケーションが見つからない場合は、ServiceNow Store へのリクエストが必要になることがあります。

[インストール] ボタンの横のリストに、使用可能なバージョンが表示されます。

3. リストからバージョンを選択し、[インストール] を選択します。

表示される [インストールの詳細を確認] ダイアログボックスに、アプリケーションとともにインストールされている依存関係が一覧表示されます。

4. プロンプトが表示された場合は、ServiceNow Store へのリンクに従って、依存関係のエントリメントを取得します。

5. [Install (インストール)] を選択します。

Microsoft Defender for IoT (オンプレミス管理コンソール) ロールへの脆弱性対応のアサイン

ユーザーにロールをアサインして、脆弱性対応 for Microsoft Defender for IoT (オンプレミス管理コンソール) アプリケーションの機能、能力、データへのアクセスを制御できるようにします。

始める前に

必要なロール：admin

このタスクについて

次のテーブルに記載されているロールを持つユーザーは、Microsoft Defender for IoT 用 脆弱性対応 (オンプレミス管理コンソール) アプリケーションを使用できます。

必要に応じてアドミンユーザーまたはユーザーグループにロールをアサインします。

脆弱性対応 for Microsoft Defender for IoT (オンプレミス管理コンソール) ロール

ロール	説明
OT VR 統合ビューアー [sn_otvr.integration_viewer]	OT VR 統合レコードを表示できます。
OT VR 統合アドミン [sn_otvr.integration_admin]	OT VR 統合を構成して実行できます。
MID サーバー [mid_server]	MID サーバーを設定できます。

手順

ServiceNow AI Platform ユーザー管理機能を使用して、ユーザーとグループにロールをアサインします。

タスク	ユーザー管理機能
ユーザーへのロールのアサイン	ユーザーへのロールの割り当て を参照してください。
グループへのロールのアサイン	グループへのロールのアサイン を参照してください。

National Vulnerability Database 統合の実行

脆弱性情報データベース (NVD) 統合を実行して、米国国立標準技術研究所 (NIST) の NVD 製品からデータをインポートします。NVD 統合を実行すると、環境内で見つかった共通脆弱性識別子 (CVE) の重大度と詳細を判断する際に役立ちます。

始める前に

インスタンスで NIST NVD 統合を実行する前に、インストールと構成の手順を完了する必要があります。インストールと構成を完了すると、NVD 製品が オペレーショナルテクノロジー脆弱性対応アプリケーションと適切に統合されます。

NVD プラグインをインストールするには、「[脆弱性対応 Integration with the NIST National Vulnerability Database のインストール](#)」を参照してください。

必要なロール：admin

手順

1. 移動先 **すべて > 脆弱性対応 > アドミニストレーション > 統合**。
2. [NIST NVD integration - API (CVE only) (NIST NVD 統合- API (CVE のみ))] レコードを選択します。

Name	Active	Class	Updated	Source Instance
Claroty CTD Vulnerability Closure Integration	false	Claroty CTD Vulnerability Integration	2023-06-09 09:52:27	Claroty CTD
Claroty CTD Vulnerability Detection Integration - Delta Import	false	Claroty CTD Vulnerability Integration	2023-06-22 10:23:09	Claroty CTD
Claroty CTD Vulnerability Detections - Full Import	true	Claroty CTD Vulnerability Integration	2023-06-22 10:23:16	Claroty CTD
CWE Comprehensive 2000 Integration	true	Vulnerability Integration	2015-11-25 10:58:50	(empty)
Manual Ingestion CSV Integration	true	Vulnerability Integration	2022-05-22 20:50:20	Manual Ingestion
Manual Ingestion Excel Integration	true	Vulnerability Integration	2022-05-24 01:02:35	Manual Ingestion
Manual Ingestion JSON Integration	true	Vulnerability Integration	2022-05-22 21:07:45	Manual Ingestion
Manual Ingestion XML Integration	true	Vulnerability Integration	2022-05-24 01:02:56	Manual Ingestion
Microsoft D4IoT Auto-close Resolved Vulnerable Items	false	Microsoft D4IoT VR Integration	2022-03-02 21:22:20	Microsoft D4IoT Vulnerability Response L...
Microsoft D4IoT Devices CVE Integration (Delta Import)	false	Microsoft D4IoT VR Integration	2021-09-03 01:12:50	Microsoft D4IoT Vulnerability Response L...
Microsoft D4IoT Devices CVE Integration (Full Import)	false	Microsoft D4IoT VR Integration	2021-09-03 01:12:54	Microsoft D4IoT Vulnerability Response L...
Microsoft Security Response Center Solution Integration	false	Microsoft Security Response Center Solut...	2019-03-13 21:21:01	Microsoft Security Response Center Solut...
NIST National Vulnerability Database Integration - API (CVE and CPE)	false	REST Integration	2020-11-10 20:30:02	National Vulnerability Database
NIST National Vulnerability Database Integration - API (CVE only)	true	REST Integration	2023-07-11 07:13:28	National Vulnerability Database
Red Hat Solution Integration	false	Red Hat Solution Integration	2020-03-03 23:10:43	Red Hat Solution Integration

3. [インポート開始日時] フィールドで、値を **NULL** に設定します。

4. [Execute Now (今すぐ実行)] を選択します。

Microsoft Defender for IoTの脆弱性対応の構成 (オンプレミス管理コンソール)

脆弱性対応 for Microsoft Defender for IoT (オンプレミス管理コンソール) 統合のレコードを構成します。

始める前に

脆弱性対応 for Microsoft Defender for IoT (オンプレミス管理コンソール) ガイド付きセットアップを使用して、構成を完了します。ガイド付きセットアップにアクセスするには、次に移動します：**MSFT D4IoT 脆弱性統合 > アドミニストレーション > ガイド付きセットアップ**。

必要なロール:sn_otvr.integration_admin および mid_server

手順

1. 移動先 **すべて > MSFT D4IoT 脆弱性統合 > アドミニストレーション > 構成**。
2. [New] をクリックします。
3. フォームのフィールドに入力します。
フィールド値の説明については、「[Microsoft Defender for IoT VR 構成フォーム](#)」を参照してください。
4. [認証情報の保存と検証] をクリックします。

Microsoft Defender for IoT VR 構成フォーム

Microsoft Defender for IoT VR 構成フォームを使用して、Microsoft Defender for IoT (オンプレミス管理コンソール) アプリケーションの脆弱性対応を構成します。

Microsoft Defender for IoT VR 構成フォーム

フィールド	説明
名前	構成の名前。
統合インスタンス	構成のインスタンス。 利用可能なデフォルトの統合インスタンスは Microsoft Defender for IoT 脆弱性対応 インスタンスです。
エンドポイント URL	Microsoft Defender for IoT管理コンソールの URL。 例: https://10.10.0.222/external/v3/integration/devicecves
MID サーバー	統合に使用される MID サーバー。
API キー	Central Manager API にアクセスするために必要なトークン。 Microsoft Defender for IoT管理コンソールでの API キーの作成については、「 https://docs.microsoft.com/en-us/azure/defender-for-iot/organizations/references-work-with-defender-for-iot-apis 」を参照してください。
ページサイズ	Microsoft API 応答の 1 ページあたりのデバイス数。 デフォルトのページサイズは 50 です。
CVSS V2 スコア	設定された CVSS V2 スコア以上のスコアを持つ脆弱性は、CVE のインポートと脆弱性一致アイテム (VIT) レコードの作成で考慮されます。 デフォルト値は 0 に設定されています。
解決済み VIT の自動クローズ	VIT レコードが解決済みに設定されている場合、その OT デバイスの Microsoft Defender for IoT からの API 応答に CVE が表示されなくなれば、VIT レコードを自動的にクローズできます。
解決済み VIT を再オープンするまでの待機日数	VIT が解決されると、ネットワーク内での OT デバイスの通信に基づいて、Microsoft Defender for IoT が脆弱性が解決されたかどうかを確認するのにしばらく時間がかかることがあります。 解決済み VIT が NIDS によってクローズ済みとして確認できない場合に、解決済み VIT を再オープンするまでの日数を定義します。

インポートスケジュールの構成

Microsoft Defender for IoTレコードにアクセスするためのインポートスケジュールを構成します。

始める前に

Microsoft Defender for IoTレコードのインポートをスケジュールする前に、NVD 統合を実行して問題を修正します。詳細については、「[National Vulnerability Database 統合の実行](#)」を参照してください。

必要なロール：admin

手順

1. 移動先 すべて > **MSFT D4IoT** 脆弱性統合 > アドミニストレーション > 統合.
 2. レコードリストから、次のレコードを選択します。
 - 完全インポートスケジュールでは、すべての OT デバイスのすべての脆弱性がインポートされます。
 - ❗ 注: レコード数が増える可能性があるため、完全インポートスケジュールを頻繁に実行することはお勧めしません。
 - デルタインポートスケジュールは、デフォルトで Microsoft サービスグラフ Connections の統合後に実行されるように構成できます。「OT 脆弱性対応 統合のシステム ID の構成」を参照してください。
 - OT デバイスの脆弱性が解決された場合は、[解決済み VIT のインポート スケジュールの自動クローズ] を使用します。脆弱性一致アイテム (VIT) がスキャナーからの確認に基づいて自動的に閉じます。
- スコープが正しいアプリケーションにない場合は、「このレコードを編集するにはここをクリックしてください」というメッセージがページの上部に表示されます。
3. レコードを編集するには、ここをクリックしてください。
 4. [アクティブ] チェックボックスをオンにして、[アクティブ] を **true** に変更します。
 5. 必要に応じて、ドロップダウンリストから [スケジュール] を選択します。
 6. **[Execute Now (今すぐ実行する)]** をクリックします。

OT 脆弱性対応 統合のシステム ID の構成

Microsoft SGC 接続統合後に統合レコードを完全にインポートするようにシステム ID を構成します。

始める前に

必要なロール: admin

このタスクについて

脆弱性が報告されている可能性があるすべての OT デバイスを CMDB に含めるために、この構成を強くお勧めします。

手順

1. 移動先 すべて > サービスグラフコネクタ **Microsoft D4 IoT** > プロパティ.

スコープが間違ったアプリケーションに設定されている場合は、「このレコードを編集するにはここをクリックしてください」というメッセージがページの上部に表示されます。

① This record is in the [Service Graph Connector Integration with Microsoft Azure Defender for IoT application](#), but [Global](#) is the current application. To edit this record click [here](#).

Microsoft Defender for IoT Integration Properties

Integration Configurations

The following system properties are used to configure the Microsoft Defender for IoT integration.

Sensor API resource path. Default value is "/external/v3/integration/sensors". ②

/external/v3/integration/sensors

Device API resource path. Default value is "/external/v3/integration/devices". ②

/external/v3/integration/devices

Connection API resource path. Default value is "/external/v3/integration/connections". ②

/external/v3/integration/connections

(Optional) Override Connection Alias record sys_id used to connect the integration. Default value is empty. ②

The number of device records to fetch in a paginated REST call to the Microsoft Defender for IoT Management Console. Default value is 50. ②

50

The number of connection records to fetch in a paginated REST call to the Microsoft Defender for IoT Management Console. Default value is 50. ②

50

Get all devices. If not checked, then only devices created or updated since the last successful import will be imported. Default is No. ②

☐ Yes | No

Get all connections. If not checked, then only connections created or updated since the last successful import will be imported. Default is No. ②

☐ Yes | No

(Optional) Sys id of OT VR Integration (Scheduled Job) to execute after SG-OT Microsoft D4IoT Connections Import. ②

Save

2. レコードを編集するには、ここをクリックしてください。

3. システムプロパティ `sn_msftd4iotsgc.ot.vr.integration.id` を OT VR 統合の `sys_id` で構成します。

4. **[Save (保存)]** をクリックします。

古い検出の自動クローズの構成

[古い検出を自動クローズ] を有効にすると、サードパーティ統合によって最近検出されなかった古い脆弱性検出が自動的にクローズされます。

始める前に

必要なロール：admin

このタスクについて

古い検出は、ほとんどの場合、重大なリスク脆弱性一致アイテム (VIT) を対象とした修復に起因しており、この修正は、オープン ステータスの重要度の低い複数の VIT にも対処します。これらの VIT を [クローズ済み] に移動すると、ServiceNow AI Platform インスタンス内のアクティブな VIT と脆弱性グループの数が減ります。

手順

1. 移動先 **すべて > 脆弱性対応 > アドミニストレーション > 自動クローズ構成 > 古い検出**。

[古い構成を自動クローズ (Auto-Close Stale Configuration)] フォームが表示されます。

2. フィールドに入力します。

3. [古い検出を自動クローズする基準] フィールドで、[リストで 最後に発見された検出] を選択します。

このオプションは、スキャナーによって検出が再度見つかった最新の日付を検索します。

i 注: [前回スキャンされたデバイス] オプションは、OT スキャナーには適用されません。

脆弱性対応 v22.0 以降では、検索の追加オプションを設定できます。詳細については、「[自動クローズルールを作成する](#)」を参照してください。

4. モジュールを有効にするには、[アクティブ] チェックボックスをオンにします。

5. [最後に発見された検出(日前)] フィールドに、古くなった検出の経過日数を入力します。

デフォルトは 90 日です。日数には任意の正の値を入力できます。この値は、Microsoft Defender for IoT によって提供された前回検出された日付と照合するために使用されます。[90] と [最後に発見された検出] が表示されている場合、過去 90 日間に検出されなかった脆弱性一致アイテムは自動的にクローズされます。

6. オプション: 保留された VIT または現在保留のレビュー中の VIT にマッピングされている古い検出を無視するには、[保留された VI の古い検出を無視する] チェックボックスをオンにします。このオプションを無効のままにすると、保留された VIT または保留についてレビュー中の VIT にマッピングされた、基準に一致するすべての検出がクローズされます。これらの検出に対応する保留 VIT またはレビュー中の VIT も、ロールアップロジックに基づいて自動的にクローズされます。ロールアップロジックの詳細については、「[脆弱性対応での古い検出のクローズ](#)」を参照してください。

このオプションを有効にすると、保留された VIT または保留についてレビュー中の VIT にマッピングされる基準に一致する検出は、自動クローズ時にスキップされます。

7. オプション: [クローズされている VI の古い検出を無視する] チェックボックスをオフにします。デフォルトでは、このチェックボックスはオンになっており、このクローズされた VIT に対する新しい検出が特定されたときにクローズされた VIT が再オープンされないようにします。ロールアップロジックの詳細については、「[脆弱性対応での古い検出のクローズ](#)」を参照してください。

8. [Update (更新)] を選択します。

スケジュール済みジョブ [Auto-Close Stale Detections] を毎日実行します。このジョブでは、選択された日付が「最後に検出があった日付」と「最後に資産がスキャンされた日付」のどちらであるかを判断します。当該検出のステータスが [古い] に移行します。[古い検出を自動クローズ] 機能では、アクティブな統合インスタンスにおいて古い検出をクローズするだけであるということがポイントです。アクティブな統合インスタンスに関連付けられている脆弱性一致アイテムや検出はクローズされます。脆弱性対応の v21.1 以降、スケジュール済みジョブは共通テーブル [sn_vul_cm_n_auto_close_rule] を考慮するように変更されています。

検出が [古い] とマークされた後、スキャナーがその検出の発見を再度報告すると、検出の [ステータス] フィールドは [オープン] に移行します。検出の対応する脆弱性一致アイテムも再オープンされます。

また、検出が [古い] とマークされていて、スキャナーがそれを [修正済み] であると判断した場合、検出は [クローズ済み] に移行します。ステータスも VIT にロールアップされます。

オペレーショナルテクノロジー脆弱性対応の使用

サードパーティ統合からの脆弱性一致アイテムのインポートなど、必要なすべてのセットアップタスクを完了すると、産業用 ワークスペースからオペレーショナルテクノロジー脆弱性対応アプリケーションを使用できます。

産業用 ワークスペース

オペレーショナルテクノロジー脆弱性対応を使用するには、産業用 ワークスペースから次のランディングページとメニューにアクセスします。

産業用 ワークスペースの詳細については、「[産業用 ワークスペース](#)」を参照してください。

の OTVR (PA) ダッシュボード 産業用 ワークスペース

OTVR (PA) ダッシュボードを使用して、脆弱性一致アイテムの初期分析と検出から封じ込めや修復までのボリューム、パフォーマンス、および進捗状況を追跡します。アサイン先グループ、エクスポイト、リスク評価、またはステータスでレポートをフィルタリングして、脆弱性エクスポージャーと影響を受けるサービスに関するインサイトを得ることができます。

OTVR (PA) ダッシュボードの詳細については、次を参照してください。 [オペレーショナルテクノロジー脆弱性対応 \(PA\) ダッシュボード](#)

OT 脆弱性リスクロールアップダッシュボードの概要

オペレーショナルテクノロジー (OT) 脆弱性リスクロールアップダッシュボードには、脆弱性リスクスコアのテーブルが 2 つあります。

- 機器モデルエンティティの脆弱性リスクテーブル
- サイトがアサインされていない OT デバイスの脆弱性リスクテーブル

リストメニュー

[リスト] メニューを使用して、アクセスできるすべての OT 脆弱性一致アイテムレコードと、自分または自分がメンバーであるアサイン先グループにアサインされた修復タスクを表示します。

- OT 修復タスク
 - 自分にアサイン済み
 - 所属グループにアサイン済み
- OT 脆弱性一致アイテム
 - 自分にアサイン済み
 - 所属グループにアサイン済み
 - 自分の例外要求
 - すべての例外

 **注:** [すべての例外] リストには、[却下] ステータスの例外も表示されます。

[OT 修復タスク] または [OT 脆弱性一致アイテム] リストメニューの下のレコードに移動して、OT 関連のコンテキストをさらに取得します。レコードの履歴を表示するには、さまざまな作業メモ、コメント、およびレコードの更新がキャプチャされているレコードの [アクティビティ] ウィンドウを表示します。[作成 (**Compose**)] ウィンドウで新しいコメントまたは作業メモを追加することもできます。

修復タスクの詳細については、「[修復タスクの作成](#)」を参照してください。

オペレーショナルテクノロジー脆弱性対応産業用 ワークスペースのリストビューの使用法の詳細については、「[IT 修復ワークスペースでのリストビューの使用](#)」を参照してください。

設備モデルメニュー

機器モデルマネージャーを使用して、OT 脆弱性一致アイテムを表示し、機器モデルエンティティにマッピングされている OT デバイスに関連付けられた修復タスクを表示および作成します。

ハードウェア脆弱性アセスメント

[ハードウェア脆弱性アセスメント] メニューを使用して、インベントリ内の OT デバイスのファームウェアで実行された脆弱性アセスメントを表示および管理します。

[ハードウェア脆弱性アセスメント] メニューの次のタブを使用して、すべてのアセスメントレコードと自動的に作成された脆弱性一致アイテムを表示します。

- 完全に一致したアセスメント
- 部分的に一致したアセスメント
- 脆弱性一致アイテム
- 無視されたアセスメント
- 正規化待機中

関連トピック

[脆弱性対応のワークスペース](#)

での脆弱性一致アイテムとソリューションの表示 産業用ワークスペース

オペレーショナルテクノロジー (OT) 脆弱性一致アイテム (VIT) とそれぞれの優先ソリューション、または OT 脆弱性ソリューション管理によって提供されるすべての利用可能なソリューションを産業用ワークスペースで表示します。

始める前に

必要なロール：admin

手順

1. 移動先 **すべて** > 産業用ワークスペース > リスト  > **OT 脆弱性一致アイテム** > **すべて** > **すべての OT VIT** を表示します。
2. VIT のリストに移動します。
 - 移動先 **すべて** > 産業用ワークスペース > リスト  > **OT 脆弱性一致アイテム**。
 - 移動先 **すべて** > 産業用ワークスペース > 機器モデルビュー  > **脆弱性一致アイテム**。
 - a. 表示されたリストから VIT を選択します。
 - b. VIT の [修復] セクションで、VIT の優先ソリューションまたは利用可能なすべてのソリューションを表示できます。
 - c. VIT で利用可能なソリューションが複数ある場合は、[優先ソリューション] フィールドで [検索]  を選択して、VIT で利用可能なすべてのソリューションを検索して表示します。
3. 移動先 **すべて** > 産業用ワークスペース > リスト  > **ソリューション**。
 - a. [すべて] リストを選択して、利用可能な脆弱性ソリューションの完全なリストを表示します。
 - b. [脆弱性一致アイテムあり (**With vulnerable items**)] リストを選択して、それぞれの脆弱性一致アイテムの脆弱性ソリューションのリストを表示します。

関連トピック

[オペレーショナルテクノロジー 脆弱性ソリューション管理](#)

での脆弱性の例外の表示 産業用ワークスペース

オペレーショナルテクノロジー (OT) アドミンの要求を使用して、脆弱性一致アイテム (VIT) を例外として無視できます。

始める前に

必要なロール：admin

手順

1. 移動先 **すべて > 産業用ワークスペース > リスト**  **> OT 脆弱性一致アイテム**.
 - [自分の例外要求] リストを選択して、例外と見なすように要求した VIT を表示します。
 - [すべての例外要求] リストを選択して、OT 環境内のすべてのユーザーによって要求された VIT 例外を表示します。
 - [すべての例外] リストを選択して、OT 環境で承認されたすべての VIT 例外を表示します。
2. 移動先 **すべて > 産業用ワークスペース > リストメニュー** () **> OT 脆弱性例外の承認**.

[自分にアサイン済み (**Assigned to me**)] リストを選択すると、承認のために自分にアサインされた、または既に承認されたすべての VIT 例外要求が表示されます。

このメニューを使用して、承認のステータスの変化と、産業用ワークスペースからトリガーされた特定の例外に対して要求された承認の詳細を表示します。

修復タスクの作成

機器モデルエンティティにマッピングされている OT デバイスに関連付けられた修復タスクを作成します。

始める前に

必要なロール:sn_otvr.remediation_owner

手順

1. 移動先 **すべて > 産業用ワークスペース**.
2. [機器モデル] ページを開きます。
3. [機器モデルビュー対象] フィールドで、機器モデル情報を表示するサイトを選択します。
4. 適切な機器モデルエンティティを選択し、**[Vulnerable Items (脆弱性一致アイテム)]** 関連リストタブに移動します。
5. 修復タスクに追加する脆弱性一致アイテムレコードを選択し、[修復タスクの作成] を選択します。

Number	Summary	OT asset	Manufacturer	Risk score	Risk rating	State	Remediation task
☒ VIT0010001	[Claroty] Rockwell sending a CIP connection request to an affected device and upon successful connection enables sending a new IP configuration	90.73.88.104 @ e5:ec:fe:3a:ee:2e	BizLink	0	5 - None	Open	
☒ VIT0010232	[Claroty] Rockwell sending a CIP connection request to an affected device and upon successful connection enables sending a new IP configuration	90.73.88.104 @ e5:ec:fe:3a:ee:2e	BizLink	80	2 - High	Open	
☐ VIT0010235	[Claroty] Rockwell sending a CIP connection request to an affected device and upon successful connection enables sending a new IP configuration	90.73.88.104 @ e5:ec:fe:3a:ee:2e	BizLink	80	2 - High	Open	
☐ VIT0010236	[Claroty] Rockwell sending a CIP connection request to an affected device and upon successful connection enables sending a new IP configuration	90.73.88.104 @ e5:ec:fe:3a:ee:2e	BizLink	40	3 - Medium	Open	
☐ VIT0010237	[Claroty] Rockwell sending a CIP connection request to an affected device and upon successful connection enables sending a new IP configuration	90.73.88.104 @ e5:ec:fe:3a:ee:2e	BizLink	20	4 - Low	Open	
☐ VIT0010238	[Claroty] Rockwell sending a CIP connection request to an affected device and upon successful connection enables sending a new IP configuration	90.73.88.104 @ e5:ec:fe:3a:ee:2e	BizLink	80	2 - High	Open	

6. 修復タスクに必要なすべての詳細情報を入力します。

[Assignment group (アサイン先グループ)] フィールドは、サイトのアサイン先グループに基づいて自動的にアサインされます。

7. [Save (保存)] をクリックしてタスクレコードを作成します。

結果

修復タスクを作成すると、機器モデルエンティティのメンテナンススケジュールによって決定された次の定期メンテナンス中にタスクが取得されます。機器モデルエンティティスケジュールの詳細については、「[設備モデルの管理](#)」を参照してください。

修復タスクの開始時間を手動で選択することもできます。開始時間の選択の詳細については、「[修復タスクの開始時間の選択](#)」を参照してください。

修復タスクの開始時間の選択

機器モデルエンティティスケジュールのタイムスロットを使用して、オペレーショナルテクノロジー (OT) 修復タスクの予定開始時間を選択します。

始める前に

必要なロール: sn_otvr.remediation_owner

このタスクについて

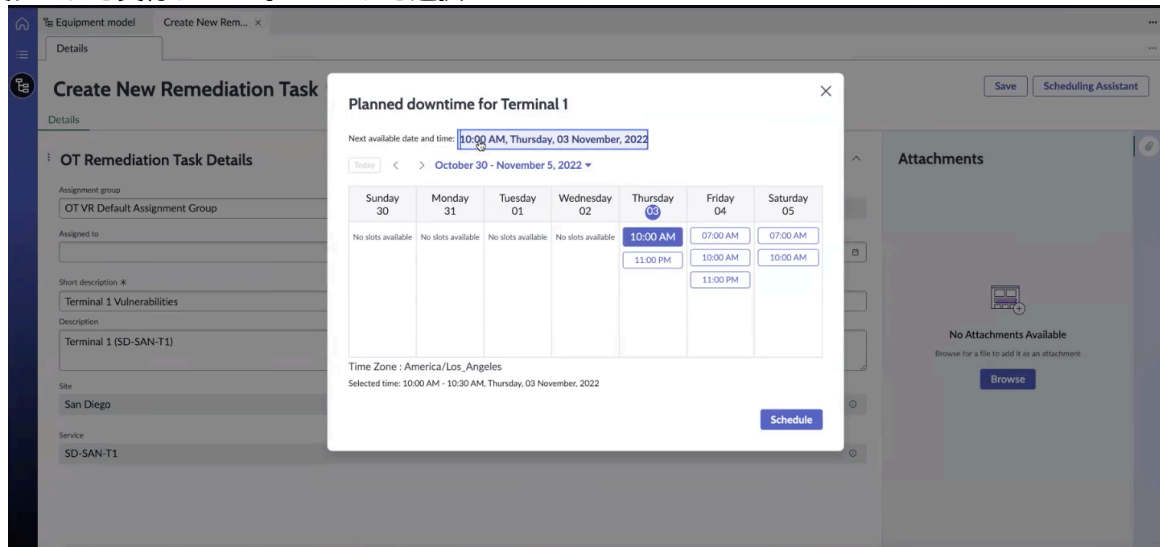
OT 修復タスクの開始時間を 手動で 選択する方法は 2 つあります。

- 修復タスクの作成時に開始時間を選択するには、[新しい修復タスクの作成 (Create New Remediation Task)] フォームで [スケジュールアシスタント] を選択します。
- 既存の修復タスクを開き、そこからスケジュールを設定できます。

スケジュールアシスタントは、機器モデルエンティティスケジュールのタイムスロットを使用します。詳細については、「[機器モデルエンティティスケジュールの管理](#)」を参照してください。

手順

1. 修復タスクの作成時に開始時間を選択する場合は、次のアクションを実行します。
 - a. **修復タスクの作成**を参照し、ステップ 1 ～ 6 を実行します。
 - b. [スケジュールアシスタント] を選択します。
 - c. 修復タスクを実行する日時スロットを選択しま



す。

- d. **[Schedule (スケジュール)]** を選択します。
2. 既存の修復タスクの開始時間を選択する場合は、次のアクションを実行します。
 - a. 移動先 **すべて > 産業用ワークスペース**。
 - b. リストビューで、次に移動します: **OT 修復タスク > 自分にアサイン済み**。
 - c. リストから、開始時間を設定する修復タスクを選択します。
 - d. [スケジュールアシスタント] を選択します。
 - e. 修復タスクを実行する日時スロットを選択します。
 - f. **[Schedule (スケジュール)]** を選択します。

結果

修復タスクは、設定された時間内に実行されます。

修復タスクを分割

ユーザーは、修復タスクレコードから脆弱性一致アイテム (VI) を分割して、修復タスクを作成できます。

始める前に

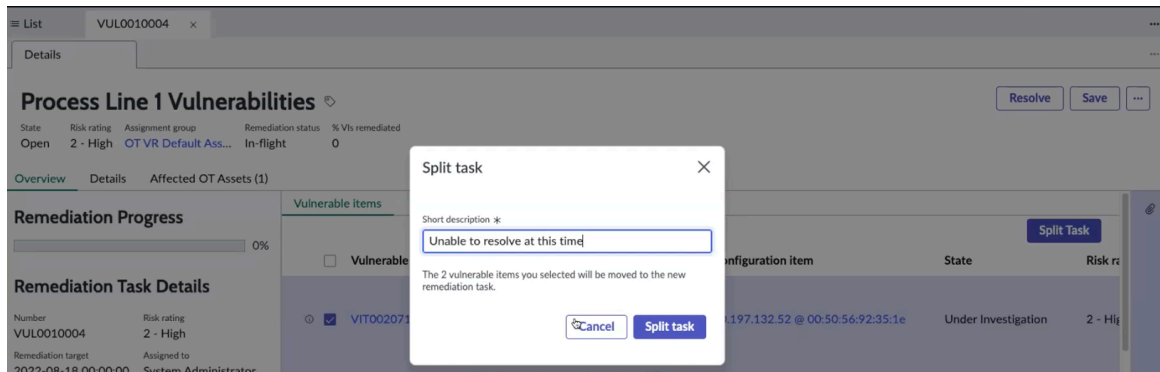
必要なロール: sn_otvr.remediation_owner

手順

1. 移動先 **すべて > 産業用ワークスペース > OT 修復タスク > 自分にアサイン済み**。
2. リストから、新しい修復タスクに移動する VI を選択します。
3. [タスクを分割] をクリックします。
4. 表示されるダイアログで、[簡単な説明] フィールドに入力します。

リストから選択した VI の数が表示されます。

タスク分割メッセージ



5. [タスクを分割] を再度クリックします。

での修復タスクの表示 産業用ワークスペース

その産業用ワークスペースの オペレーショナルテクノロジー (OT) 脆弱性一致アイテム (VIT) に対して作成された修復タスクを表示します。

始める前に

必要なロール：admin

手順

1. 移動先 **すべて** > 産業用ワークスペース > リストメニュー (☰) > **OT 修復タスク**.
2. [自分にアサイン済み] リストを選択して、自分にアサインされたすべての修復タスクを表示します。
3. [所属グループにアサイン済み (**Assigned to My Groups**)] リストを選択して、ユーザーとしてアサインされているユーザーグループにアサインされたすべての修復タスクを表示します。
4. [自分の例外要求] リストを選択して、例外と見なすように要求した修復タスクを表示します。
5. [すべての例外] リストを選択して、例外として承認された OT 環境内のすべての修復タスクを表示します。
6. [すべて] リストを選択すると、OT 環境で作成されたすべての修復タスクが表示されます。

関連トピック

[修復タスクの作成](#)

[修復タスクを分割](#)

修復タスクの保留

修復タスクを保留して、後で解決できる例外要求を作成します。

始める前に

必要なロール：admin

手順

1. 移動先 **すべて** > 産業用ワークスペース.
2. 産業用 ワークスペースリストビューを開くには、リスト (☰) アイコンを選択します。
3. [**OT 修復タスク**] モジュールで、利用可能なリストのいずれかを選択します。

4. 保留する修復タスクを選択します。
5. [例外の要求] ボタンを選択します。
6. フォームで、フィールドに入力します。

フィールド	説明
期限	保留ステータスが期限切れになり、修復タスクが再アクティブ化される日付を選択します。
理由	問題を保留する理由を入力します。次の選択肢があります。 ○ メンテナンス期間待ち ○ 誤検出 ○ 修正が利用不可 ○ リスクの受容 ○ コントロールの緩和を実施 ○ その他
追加情報	その他の関連情報を入力します。

7. [Save (保存)] を選択します。

結果

例外要求が作成されます。例外要求は、[OT 修復タスク] モジュールの [自分の例外要求] リストで確認できます。[OT 修復タスク] モジュールの [すべての例外] リストで、既存のすべての例外要求を表示することもできます。

の補完コントロールについて オペレーショナルテクノロジー

OT 環境での補完コントロールは、脆弱性によってもたらされるリスクにすぐにパッチを適用できない場合の代替セキュリティ対策です。

OT 環境では、インフラストラクチャおよび本番プロセスにおける重要な役割のため、更新のためにシステムをオフラインにできないことがよくあります。補完コントロールは OT 環境を保護し、パッチやハードウェアの交換などの永続的なソリューションを使用して脆弱性が完全に修正されるまでリスクを軽減します。

次の表は、補完コントロールがリスクの軽減に役立つ特定のシナリオを示しています。

補完コントロールのユースケースシナリオ

ユースケースシナリオ	補完コントロール
プログラマブルロジックコントローラー (PLC) への不正アクセス。	- ネットワークデバイスにアクセス制御リスト (ACL) を実装します。 - PLC の未使用のポートとサービスを無効にします。 - 強力なパスワードと認証メカニズムを実装します。
ヒューマンマシンインターフェイス (HMI) パネルでのバッファオーバーフロー	- HMIパネルの製造元からリリースされたファームウェアアップデートを適用します。 - フェイルセーフ操作のハードウェアウォッチドッグタイマーを有効にします。 - アプリケーションコードに境界チェックを実装します。
PROFINET に対する中間者攻撃	- VPNまたはIPsecを介した暗号化された通信を使用します。 - 安全な証明書を使用して PROFINET を構成します。 - ファイアウォールを使用してネットワークセグメンテーションを実装します。
SCADA システムでのサービス拒否 (DoS)	- 重要な OT ネットワークコンポーネントのレート制限を有効にします。 - 冗長性と負荷分散のために SCADA システムを構成します。 - シーメンスが提供するセキュリティパッチを適用します。
エンジニアリングワークステーションでのマルウェア感染	- メーカーが推奨するマルウェア対策ソフトウェアをインストールし、定期的に更新します。 - アプリケーションの許可リストを適用して、不正なソフトウェアの実行を防止します。 - 安全なリムーバブルメディアポリシーを使用します。

の補完コントロールの使用 オペレーショナルテクノロジー

補完コントロール オペレーショナルテクノロジー (OT) を構成します。

このタスクについて

補完コントロールは、エクスプロイトが成功する可能性や影響を軽減するのに役立ちます。補完コントロールの詳細については、「[リスク削減の補完コントロールについて](#)」を参照してください。

始める前に

必要なロール:sn_vul.vulnerability_admin または sn_vul.vulnerability_analyst

手順

1. 移動先 **すべて** > 産業用ワークスペース.
2. [リスト]  アイコンを選択します。
3. [**Libraries** (ライブラリ)] モジュールの下で、[**Compensating Controls** (補完コントロール)] リストを選択します。
4. [**New** (新規)] を選択します。
5. フォームで次のフィールドに入力します。

補完コントロールフォーム

フィールド	説明
名前	追加する補正コントロールの名前。
説明	追加する補完コントロールの説明。
アクティブ	選択すると、補正コントロールが有効になります。

6. [**Save** (保存)] を選択します。

での一般的な脆弱性エントリの表示 産業用 ワークスペース

産業用 ワークスペース内の共通脆弱性エントリ (CVE) を表示して、コントロールの補完に必要な情報にアクセスします。

始める前に

必要なロール : sn_vul.vulnerability_admin

手順

1. 移動先 **すべて** > 産業用ワークスペース.
2. [リスト]  アイコンを選択します。
3. [ライブラリ] モジュールで [**CVE**] リストを選択します。

オペレーショナルテクノロジー脆弱性対応の参照

参照トピックには、オペレーショナルテクノロジー脆弱性対応 アプリケーションに関する追加情報が記載されています。

オペレーショナルテクノロジー脆弱性対応とともにインストールされるコンポーネント

いくつかのタイプのコンポーネント (ユーザーロール、ビジネスルールなど) が、オペレーショナルテクノロジー脆弱性対応 (com.sn_otvr) プラグインのアクティブ化とともにインストールされます。

- i** 注: アプリケーションファイルテーブルには、このアプリケーションとともにインストールされたコンポーネントがリストされています。このテーブルへのアクセス手順については、「[アプリケーションとともにインストールされているコンポーネントの検索](#)」を参照してください。

この機能ではデモデータを利用できます。

インストールされるロール

ロール タイトル [名前]	説明	含まれるロール
OT 脆弱性修正オーナー [sn_otvr.remediation_owner]	修復タスクを作成できます。脆弱性一致アイテムの既存の修復タスクをスケジュールすることもできます。	• cmdb_ot_isa_viewer • cmdb_ot_viewer • sn_vul.close_vi_vg • sn_vul.remediation_owner
OT VR 統合ビューアー [sn_otvr.integration_viewer]	オペレーショナルテクノロジー脆弱性対応統合レコードを表示できます。	なし
OT VR 統合アドミン [sn_otvr.integration_admin]	オペレーショナルテクノロジー脆弱性対応統合レコードを表示および編集できます。	• sn_sec_cmn.admin • sn_otvr.integration_viewer • sn_vul.read_all

インストールされるビジネスルール

ビジネスルール	テーブル	説明
OT VIT の修復タスクへの関連付け	修復タスク [sn_vul.vulnerability]	OT 修復タスクが作成されると、タスク > フィルターのグループ化構成で指定されたフィルター条件に従って、関連付けられた脆弱性一致アイテムがタスクにグループ化されます。

オペレーショナルテクノロジー脆弱性対応 脆弱性一致アイテムフォームフィールド
OT デバイス用に作成された脆弱性一致アイテムに表示されるフィールドのリスト。

脆弱性一致アイテムフィールド

フィールド	説明
概要	
番号	このレコードに対して自動的に生成された脆弱性一致アイテム番号。

フィールド	説明
状況	このフィールドのデフォルトは [オープン] ですが、脆弱性をすぐに修正する準備ができている場合は [調査中] に変更できます。
リスク評価	脆弱性一致アイテムを [重大]、[高]、[中]、[低]、および [なし] に分類する数値化された [リスクスコア]。リスク評価の詳細については、「 脆弱性対応の算出と脆弱性算出ルール 」を参照してください。 i 注: この基本リスク評価は、ソリューションレコードのリスク評価と同じではありません。
リスクスコア	脆弱性一致アイテムが環境にもたらすリスク量を算出したもの。 i 注: この基本リスクスコアは、ソリューションレコードのリスクスコアと同じではありません。 詳細については、「 脆弱性対応の算出と脆弱性算出ルール 」を参照してください。
脆弱性	この脆弱性一致アイテムに関連付けられた脆弱性の ID。
ソース	この脆弱性一致アイテムを検出したスキャナー。
構成アイテム	この脆弱性一致アイテムに関連付けられた OT 資産の ID。
アサイン先グループ	この修復タスクで作業するように選択されたグループ。
アサイン先	この脆弱性に対して作業する、選択されたアサイン先グループの個人。
作成済み	この脆弱性一致アイテムがインスタンスに作成された日付。
最終オープン日時	この脆弱性一致アイテムが最後にインスタンスでオープンされた日付。初期状態では脆弱性一致アイテムの作成日と同じですが、クローズされた後に再オープンされると、最終オープン日には再オープン日時が含まれます。
更新日時	前回のスキャンの日付。
サマリー	脆弱性の説明。
重大度	この脆弱性の重大度を正規化したもの。重大度マップは、NVD および ServiceNow サードパーティ統合に提供されます。重大度マップの作成または調整の詳細については、「 脆弱性対応 重大度マップの作成 」を参照してください。

フィールド	説明
脆弱性スコア (v3)	CVSS v3 スコア。
脆弱性スコア (v2)	CVSS v2 スコア。
エクスプロイト有無	この脆弱性一致アイテムに関連付けられた脆弱性に少なくとも 1 つのエクスプロイトが関連付けられている場合は、有り。
エクスプロイト攻撃ベクトル	この脆弱性一致アイテムに関連付けられた脆弱性のエクスプロイトの最も脆弱な攻撃ベクトル。
エクスプロイトスキルレベル	この脆弱性一致アイテムに関連付けられた脆弱性のエクスプロイトに必要な最低スキルレベル。
公開日	この脆弱性が公開された日付。
最終変更日	この脆弱性が前回変更された日付。
脅威	脅威に関する関連情報。脆弱性エントリーレコードから取得されます。  注: ここで変更を加えると、脆弱性エントリーレコードが更新されます。
修復メモ	脆弱性エントリーレコードから取得された、脅威に対する関連ソリューション。
追加コメント / 作業メモ	関連情報。その他のコメントを追加するには、このチェックボックスをオンにします。 脆弱性対応 v20.0 以降では、保留された脆弱性一致アイテムの [メモ (Notes)] セクションに作業メモを追加できます。
アクティビティ	作業メモが作成された場合にのみ表示されます。
関連リンク	
リスクスコアを計算	[脆弱性重大度] または [リスクスコア] 算出のいずれかが有効になっている場合、[リスクスコア] フィールドが更新されます。

関連情報

ネットワーク侵入検知システム (NIDS) 拡張クラス、OT 拡張クラス、および関連アプリケーションの詳細を確認してください。

拡張クラスの概要

拡張クラスは、オペレーショナルテクノロジー管理が構成管理データベース (CMDB)でどのように機能するかを理解するのに役立ちます。

ネットワーク侵入検知システム (NIDS) CI 拡張クラス

ネットワーク侵入検知システム (NIDS) [cmdb_ci_nids] クラスは、パッシブネットワークモニタリングアプライアンスと、それが検出するネットワーク上のデバイスとの間の関係をビルドします。

オペレーショナルテクノロジー (OT) 拡張クラス

構成管理データベース (CMDB) は OT のクラスを更新します。

関連アプリケーション

脆弱性対応

オペレーショナルテクノロジー脆弱性対応 と統合すると、ServiceNow 脆弱性対応 アプリケーションはプロセスの重要度に基づいて OT の脆弱性を優先順位付けして解決するのに役立ちます。

CMDB CI クラスモデル

CMDB CI Class Models ストアアプリは、クラスの説明、識別ルール、識別子エントリ、および依存関係を含む、CMDB クラス階層を拡張するクラスモデルを追加します。

製造業プロセスマネージャー

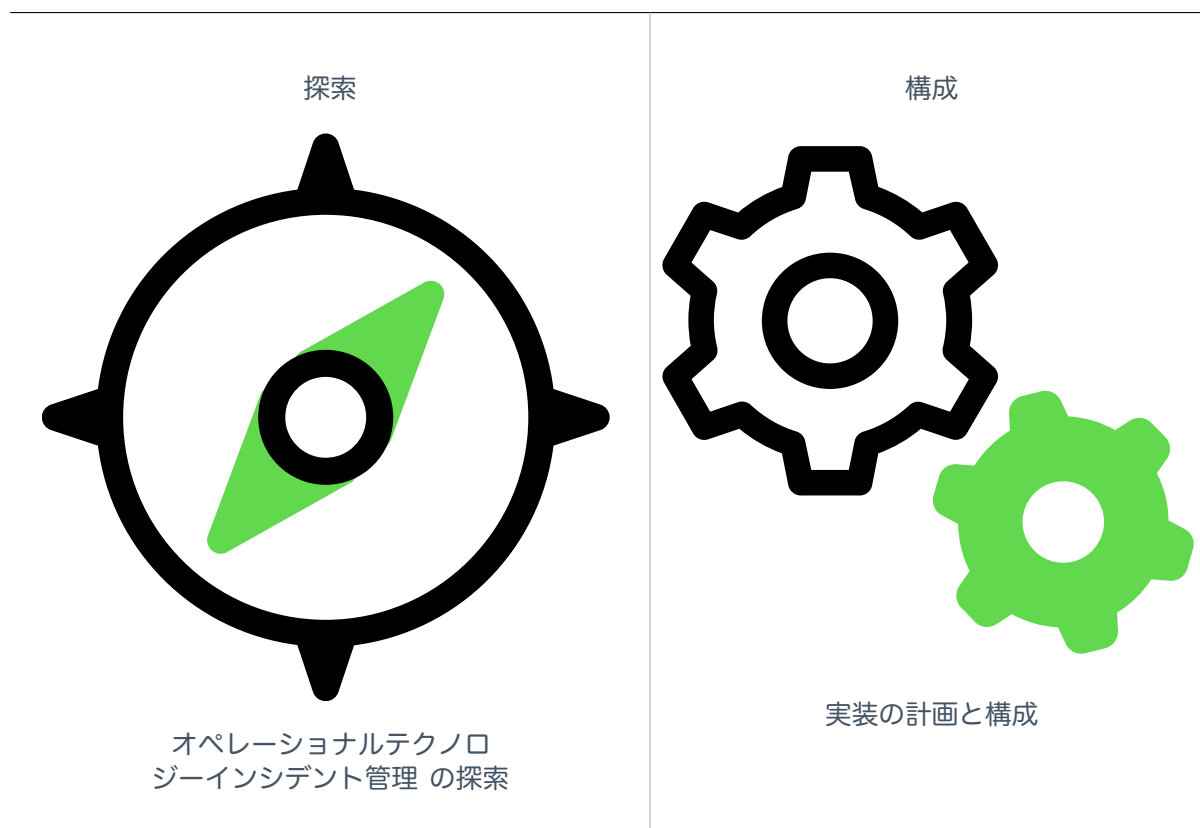
製造業プロセスマネージャー アプリケーションを使用して、ServiceNow 産業用 ソリューションに必要な ISA-95 設備モデルのデータ基盤を作成します。これにより、各産業サイトで独自のバージョンの設備モデルを作成できます。

オペレーショナルテクノロジーマネージャー

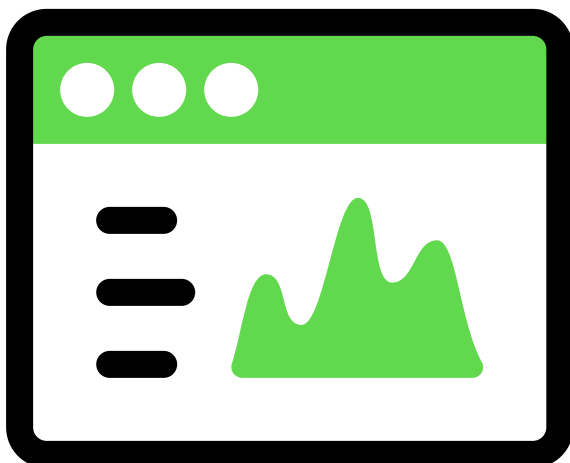
オペレーショナルテクノロジーマネージャー アプリケーションを使用すると、複数のソースから OT デバイスデータを集計できるため、産業用 ソリューションで使用される基本的なデータ関係をビルドできます。

オペレーショナルテクノロジーインシデント管理

オペレーショナルテクノロジーインシデント管理 を使用すると、メーカーは OT デバイスインシデントをオープンからクローズまで管理できます。

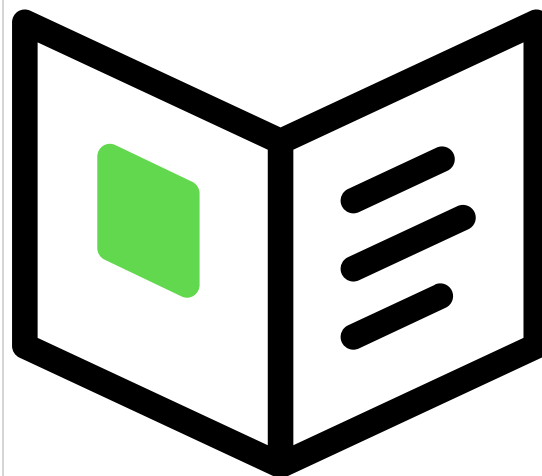


使用方法



オペレーショナルテクノロジー
インシデント管理 の使用

参照



関連情報とアプリケーションの詳細を取得

オペレーショナルテクノロジーインシデント管理 の探索

オペレーショナルテクノロジーインシデント管理アプリケーションの詳細を確認してください。

オペレーショナルテクノロジーインシデント管理の概要

オペレーショナルテクノロジーインシデント管理アプリケーションの詳細については、Operational Technology Service Management製品スイートの概要をご覧ください。

https://player.vimeo.com/video/1019801515?badge=0&autoplay=0&player_id=0&app_id=58479

主な機能

オペレーショナルテクノロジーインシデント管理では、次の主要な機能を使用できます。

- OT インシデントを作成してワークフローを推進し、OT デバイスの影響を受ける本番プロセスを迅速に復元します。
- OT インシデントが本番プロセスに及ぼすコンテキストと影響を理解します。
- OT インシデントを IT インシデントと別にして監視し管理します。
- OT インシデント履行者に別のロールをアサインします。
- OT ユーザーエクスペリエンスの向上。
- オペレーショナルテクノロジーのナレッジ管理のサポート。詳細については、「[オペレーショナルテクノロジーのナレッジ管理](#)」を参照してください。

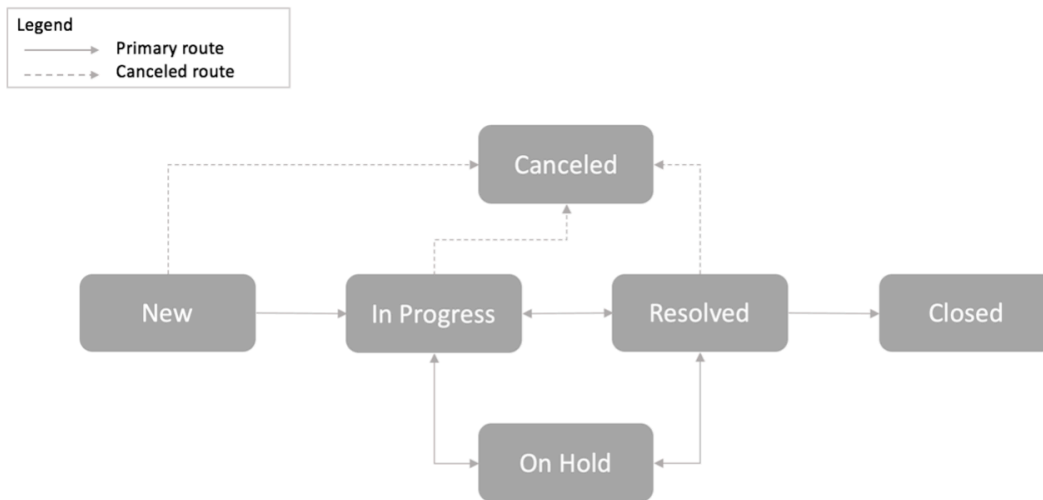
オペレーショナルテクノロジーインシデント管理

オペレーショナルテクノロジーインシデント管理 を使用すると、エンジニアはオペレーショナルテクノロジー (OT) デバイスと本番プロセスの問題を迅速に解決できます。

オペレーショナルテクノロジーインシデント管理を使用すると、OT インシデントを IT インシデントとは別に管理できます。OT インシデントは、OT ネットワーク上の OT デバイスによって提供されるサービスが中断されると発生します。ときとして、インシデントが最初に作成されたときの OT デバイスが不明な場合があります。OT デバイスが不明な場合は、問題が発生した機器モデルエンティティに対してインシデントが発生する可能性があります。

OT インシデントマネージャーは、作成からクローズまで、インシデントのデフォルトライフサイクルを管理する責任があります。OT インシデント管理プロセスには多くのステータスがあり、それぞれがプロセスの成功と提供されるサービスの品質にとって重要です。さまざまな状況を次の図に示します。

オペレーショナルテクノロジーインシデント管理 プロセスステータス



インシデント状況は次のとおりです。

状況	説明
新規	インシデントはログに記録されていますが、調査はまだです。
進行中	インシデントはアサインされていて、調査中です。
保留	詳しい情報、証拠、または解決策を提供するために、インシデントが一時的に別のエンティティに移行します。[保留中] オプションを選択すると、次の [保留理由] リストが表示されます。これらのリストオプションは、追加情報の取得元を示します。 • 問い合わせユーザー待ち • 変更待ち • 問題待ち • ベンダー待ち 保留理由が 問い合わせユーザー待ちの場合、[追加コメント] セクションは必須です。

状況	説明
	i 注: 問い合わせユーザーがインシデントを更新した場合、[保留理由] フィールドはクリアされ、インシデントのステータスが[処理中]に変更されます。[アサイン先] フィールドに名前が記載されているユーザーとウォッチリストのユーザーにメール通知が送信されます。インシデントをクローズする前に、インシデントを 1 回以上保留にすることができます。
解決済み	インシデントが再発しないように、適切な修正が提供されます。
クローズ済み	インシデントは所定の期間 [Resolved (解決済み)] の状況で経過すると、 [Closed (クローズ済み)] のマークが付けられ、問題なく解決したことが確定します。
キャンセル済み	インシデントはトリアーじされましたが、重複するインシデント、不要なインシデント、またはインシデントではないと判断されました。

製造業プロセスマネージャー との統合

オペレーショナルテクノロジーインシデント管理 製造業プロセスマネージャーと統合して、機器モデルエンティティのインシデントを報告します。

製造業プロセスマネージャー は、ServiceNow オペレーショナルテクノロジー ソリューションに必要な ISA-95 機器モデルデータ基盤を作成します。オペレーショナルテクノロジーインシデント管理と統合すると、本番プロセスに対するインシデントの影響度を表示できます。

製造業プロセスマネージャー とともにインストールされる ISA 設備階層モデルプラグイン (sn_isa_model) は、指定されたロールのビューを有効にします。詳細については、「[ISA-95 機器モデル](#)」を参照してください。

OT デバイスレコードから OT インシデントが作成されると、次のことが起こります。

- OT インシデントフォームの **[OT device (OT デバイス)]** フィールドに、OT デバイスの値が入力されます。
- OT デバイスに関連付けられた機器モデルエンティティがある場合、その機器モデルエンティティは OT インシデントフォームの **[Equipment model entity (機器モデルエンティティ)]** フィールドに追加されます。
- OT インシデントフォームの **[Site (サイト)]** フィールドに、OT デバイスの値が入力されます。

機器モデルエンティティレコードから OT インシデントが作成されると、次のことが起こります。

- OT インシデントフォームの **[機器モデルエンティティ]** フィールドには、機器モデルエンティティの値が入力されます。
- OT インシデントフォームの **[サイト]** フィールドには、機器モデルエンティティのサイトが入力されます。

機器モデルエンティティレコードの **OT** インシデント関連リストには、そのエンティティで報告されたすべての OT インシデントが表示されます。フォーム上の **[Equipment model entity (機器モデルエンティティ)]** フィールドには、選択したサイトのエンティティのみを含めることができます。

オペレーショナルテクノロジーインシデント管理の構成

ServiceNow オペレーショナルテクノロジー ソリューションのデータ基盤を作成できるように、オペレーショナルテクノロジーインシデント管理 アプリケーションを構成します。

オペレーショナルテクノロジーインシデント管理 v2 は Tokyo P5 以降に依存しています。

注:

admin ロールを持っている場合は、ガイド付きセットアップを使用して、オペレーショナルテクノロジーインシデント管理 アプリケーションのセットアップ手順を実行できます。ガイド付きセットアップにアクセスするには、次に移動します: 産業用ワークスペースアドミン > ガイド付きセットアップ。

タスク	目的
1. ServiceNow Storeからオペレーショナルテクノロジーインシデント管理アプリケーションをインストールします。	オペレーショナルテクノロジーインシデント管理 アプリケーションとサポートプラグインをインストールします。
2. オペレーショナルテクノロジーインシデント管理 ロールを割り当てます。	ロールを割り当てて、各ユーザーが使用できるアクションをコントロールします。
3. OT インシデントを移行します。	OT インシデントをインシデントテーブルから OT インシデントテーブルに移行します。  注: この手順は、Paris、San Diego、または Tokyo から Utah にアップグレードする場合にのみ適用されます。
4. OT インシデントのカテゴリとサブカテゴリを構成します。	必要に応じて、OT インシデントのカテゴリとサブカテゴリを構成します。
5. 状況モデルを構成します。	OT インシデントサイトの状況モデルを構成します。
6. (オプション) アサインルールを作成します。	OT インシデントを適切なグループまたはユーザーに自動的にアサインするアサインルールを作成します。

オペレーショナルテクノロジーインシデント管理 をインストール

admin ロールをお持ちであれば、オペレーショナルテクノロジーインシデント管理 アプリケーション (sn_ot_inc_mgmt) をインストールできます。このアプリケーションは、関連する ServiceNow Store アプリケーションとプラグインをインストールします (まだインストールされていない場合)。

始める前に

- アプリケーションとその関連するすべての ServiceNow Store アプリケーションに有効な ServiceNow エンタイトルメントがあることを確認してください。詳細については、次を参照してください。 [のエンタイトルメントを取得する ServiceNow 製品またはアプリケーション](#)。
- オペレーショナルテクノロジーインシデント管理 には次のプラグインが必要です。オペレーショナルテクノロジーインシデント管理 をインストールする前に、これらのプラグインがアクティブ化されていることを確認してください。

必須の ServiceNow プラグイン

CMDB CI クラスモデル (sn_cmdb_ci_class)

CMDB CI Class Models (CMDB CI クラスモデル) ストアアプリは、クラスの説明、識別ルール、識別子エントリ、および依存関係を含む、CMDB クラス階層を拡張するクラスモデルを追加します。詳細については、「[CMDB CI クラスモデルストアアプリ](#)」を参照してください。

ISA Equipment Model (ISA 設備階層モデル) (sn_isa_model)

ISA-95 機器モデルエンティティおよびテンプレートのデータモデル詳細については、「[ISA-95 機器モデル](#)」を参照してください。

- オペレーショナルテクノロジーインシデント管理 には、次の ServiceNow Store アプリケーションのいずれかまたは両方が必要です。オペレーショナルテクノロジーインシデント管理をインストールする前に、これらのアプリケーションが少なくとも 1 つインストールされていることを確認します。

必要な ServiceNow Store アプリケーション

オペレーショナルテクノロジーマネージャー

オペレーショナルテクノロジーマネージャー アプリケーションは、企業が ServiceNow オペレーショナルテクノロジーソリューションを使用できるようにする基盤データと関係を作成します。オペレーショナルテクノロジーマネージャー は、ServiceNow AI Platformでの構成管理データベース (CMDB)、サービスグラフコネクタ、およびディスカバリーアプリケーションの使用をサポートしています。詳細については、「[オペレーショナルテクノロジーマネージャーの構成](#)」を参照してください。

製造業プロセスマネージャー

製造業プロセスマネージャー アプリケーションは、ServiceNow 産業用ソリューションに必要な ISA-95 機器モデルデータ基盤を作成し、各産業サイトで独自のバージョンの機器モデルを作成できるようにします。詳細については、「[製造業プロセスマネージャーの構成](#)」を参照してください。

- 必要なロール：admin

このタスクについて

オペレーショナルテクノロジーインシデント管理 とともに次のアイテムがインストールされます。

- プラグイン
- ストアアプリケーション
- ロールと ACL

インストールされているロールと ACL の詳細については、「[オペレーショナルテクノロジーインシデント管理とともにインストールされるコンポーネント](#)」を参照してください。

- ❗ **注：** オペレーショナルテクノロジー ヴィジビリティのライセンスを持たないOperational Technology Service Managementユーザーの場合は、次の点に注意してください。

- 最新バージョンの オペレーショナルテクノロジーインシデント管理 をインストールすると、製造業プロセスマネージャー もインストールされます。
- 最新バージョンの オペレーショナルテクノロジー変更管理 をインストールすると、製造業プロセスマネージャー もインストールされます。

Operational Technology Service Management エクスペリエンスにアクセスできるように、最新バージョンにアップグレードする必要があります。

手順

1. 移動先 **すべて > システムアプリケーション > 利用可能なすべてのアプリケーション > すべて**.
2. フィルター基準と検索バーを使用して、**オペレーショナルテクノロジーインシデント管理 アプリケーション (sn_ot_inc_mgmt)** を検索します。

名前または ID でアプリケーションを検索できます。アプリケーションが見つからない場合は、ServiceNow Store へのリクエストが必要になることがあります。

ServiceNow Store Web サイトにアクセスして利用可能なすべてのアプリを表示し、ストアにリクエストを送信する方法について確認してください。リリースされたすべてのアプリのリリースノート情報については、「[ServiceNow Storeバージョン履歴のリリースノート](#)」を参照してください。

3. アプリケーションのインストールダイアログボックスで、アプリケーションの依存関係を確認します。

依存するプラグインとアプリケーションがインストールされている場合、現在インストールされている場合、またはインストールする必要がある場合は、リストに表示されます。インストールする必要があるプラグインまたはアプリケーションがある場合は、**オペレーショナルテクノロジーインシデント管理** をインストールする前にインストールする必要があります。

4. **[Install (インストール)]** を選択します。

インシデントを新しいインシデントテーブルに移行する

古いインシデントテーブルから新しいインシデントテーブルに **オペレーショナルテクノロジー インシデント** を移行します。インシデントを移行すると、古いテーブルが適用されなくなったことが **オペレーショナルテクノロジーインシデント管理 アプリケーション** に通知されます。

始める前に

- **Operational Technology Incident Management** (オペレーショナルテクノロジーインシデント管理) にアプリケーションスコープを設定します。
- 必要なロール：admin

手順

1. 移動先 **産業用ワークスペースアドミン > ガイド付きセットアップ**.
2. **[オペレーショナルテクノロジーインシデント管理]** カテゴリで、**[開始]** を選択します。
3. **[OT インシデントを移行]** セクションの横にある **[構成]** を選択します。
4. **[今すぐ実行]** を選択して移行を開始します。
5. オプション: このスケジュール済みジョブのアクティビティログを表示するには、次に移動します: **すべて > システムログ > システムログ > すべて**.

結果

オペレーショナルテクノロジーインシデント は新しいインシデントテーブルに移行され、**オペレーショナルテクノロジーインシデント管理アプリケーション** は古いテーブルを使用しなくなります。

ユーザーへのロールのアサイン

オペレーショナルテクノロジーインシデント管理 アプリケーションでユーザーにロールをアサインして、機能やデータへのアクセス権を制御できるようにします。

始める前に

必要なロール：admin

このタスクについて

次のテーブルにリストされているロールを持つユーザーは、オペレーショナルテクノロジーインシデント管理 アプリケーションを使用できます。

- i** 注: OT インシデントユーザー [ot_incident_user] ロールは複製される。このロールがアサインされているユーザーについて、スケジュール済みジョブ「新しい OT インシデントロールのアサイン」を実行して、新しい オペレーショナルテクノロジーインシデント管理 ロールをアサインできます。詳細については、「[ユーザーに新しいロールをアサインする](#)」を参照してください。

ロール	説明
OT インシデントアドミン [sn_ot_incident_admin]	あらゆる機器モデルエンティティの OT インシデントレコードの作成、表示、削除、編集ができます。このロールを持つユーザーは、優先度 ルックアップルール と OT インシデントシステムプロパティを設定できます。
OT インシデントリーダー [sn_ot_incident_read]	OT インシデントレコードの表示のみできます。
OT インシデント履行者 [sn_ot_incident_write]	OT インシデントレコードを作成、表示、編集できます。

手順

ServiceNow AI Platformユーザー管理機能を使用して、ユーザーまたはグループにロールを割り当てます。

タスク	ユーザー管理機能
ユーザーへのロールのアサイン	ユーザーへのロールの割り当て を参照してください。
グループへのロールのアサイン	グループへのロールのアサイン を参照してください。

ユーザーに新しいロールをアサインする

オペレーショナルテクノロジーインシデント管理 アプリケーションのスケジュール済みジョブを通じて、OT インシデントユーザー [ot_incident_user] ロールを持つユーザーに新しいロールをアサインします。

始める前に

- **Operational Technology Incident Management** (オペレーショナルテクノロジーインシデント管理) にアプリケーションスコープを設定します。
- 必要なロール：admin

このタスクについて

OT インシデントユーザーロール [ot_incident_user] は廃止されました。スクリプトの実行をスケジュールすることで、ot_incident_userロールを持っていたユーザーに新しいロールを割り当てることができます。

手順

1. 移動先 **すべて > システム定義 > スケジュール済みジョブ**。
2. 検索バーで、[新しい **OT** インシデントロールの割り当て (**Assign New OT Incident Roles**)] スケジュール済みジョブを検索します。
3. [**今すぐ実行**] を選択して、スケジュール済みジョブを開始します。
4. オプション: このスケジュール済みジョブのアクティビティログを表示するには、次に移動します: **すべて > システムログ > システムログ > すべて**。

結果

スケジュール済みジョブが実行され、ユーザーに新しい オペレーショナルテクノロジーインシデント管理 ロールがアサインされます。

アサイン先グループの作成

OT インシデントレコードにアサインする オペレーショナルテクノロジー (OT) 固有のアサイン先グループを作成します。

始める前に

必要なロール：admin

このタスクについて

OT インシデントレコードの [アサイン先グループ] フィールドには、OT タイプのアサイン先グループのみが表示されます。これは、オペレーショナルテクノロジー (OT) インシデントと情報技術 (IT) インシデントを分離するのに役立ちます。

OT インシデントレコードに表示する OT 固有のアサイン先グループを作成できます。

手順

1. 移動先 **すべて > ユーザー管理 > グループ**。
2. [**New (新規)**] を選択します。
3. フォームで、フィールドに入力します。

アサイン先グループフォーム

フィールド	説明
名前	アサイン先グループの名前
マネージャー	グループマネージャーまたはリード
タイプ	このグループのカテゴリです。[ターゲットレコードを選択] フィールドで、「 OT 」を検索して [タイプ] フィールドに追加します。

フィールド	説明
グループ メール	グループのメール配布リストまたは連絡先メールアドレス。
親	グループがメンバーである他のグループ。
説明	アサイン先グループの説明

4. [Submit (送信)] を選択します。

結果

これで、OT 固有のアサイン先グループがインシデントレコードに表示されます。

インシデントカテゴリとサブカテゴリ

オペレーショナルテクノロジー (OT) インシデントを分類することで、特定の OT インシデントをグループ化して検索を絞り込むことができます。

OT インシデントを作成できる場合は、次の表に示すカテゴリとサブカテゴリから選択できます。

インシデントカテゴリ

カテゴリ	サブカテゴリ
データベース	• DB2 • MS SQL Server • Oracle
ハードウェア	• OT の問題 • CPU • ディスク • キーボード • メモリー • 監視 • マウス
問い合わせ/ヘルプ	• ウィルス対策 • メール • 内部アプリケーション
ネットワーク	• DHCP • DNS • IP アドレス

インシデントカテゴリ (続く)

カテゴリ	サブカテゴリ
	• VPN • ワイヤレス
生産性	• マイナーストップ • 低速走行 • セットアップと調整 • ブレークダウン
品質	• 入荷する素材 • スタートアップの拒否 • プロセスの欠陥 - 定性的 • プロセスの欠陥 - 定量的
安全	• ニアミス • 危険 • 安全性に関する懸念 • 事故
ソフトウェア	• メール • オペレーティングシステム

カテゴリまたはサブカテゴリの編集

既存の オペレーショナルテクノロジー インシデントカテゴリおよびサブカテゴリを編集して、インシデントを分類します。

始める前に

- **Operational Technology Incident Management** (オペレーショナルテクノロジーインシデント管理) にアプリケーションスコープを設定します。
- 必要なロール：admin

手順

1. 移動先 **すべて > システム定義 > 選択リスト**。
2. 条件フィルターを [テーブル] [次の値に等しい] **[sn_ot_incident]** および [要素] [次の値に等しい] [カテゴリ] または [要素] [次の値に等しい] [サブカテゴリ] に設定します。
3. カテゴリまたはサブカテゴリレコードを選択します。

4. 必要に応じてフォームを編集します。

5. **[Save (保存)]** を選択します。

結果

これで、既存のカテゴリまたはサブカテゴリへの変更がレコードに表示されます。

カテゴリまたはサブカテゴリの作成

インシデントの分類に使用する オペレーショナルテクノロジー インシデントカテゴリまたはサブカテゴリを作成します。

始める前に

- **Operational Technology Incident Management** (オペレーショナルテクノロジーインシデント管理) にアプリケーションスコープを設定します。
- 必要なロール：admin

手順

1. 移動先 **すべて > システム定義 > 選択リスト**.
2. カテゴリを作成するには、次のアクションを実行します。
 - a. **[New (新規)]** を選択します。
 - b. [要素] フィールドに「category」という語を入力します。
 - c. **[Label (ラベル)]** フィールドに、カテゴリ名を入力します。
 - d. **[Value (値)]** フィールドに、カテゴリ値を入力します。
 - e. **[Sequence (シーケンス)]** フィールドに、シーケンス番号を入力します。
 - f. **[Submit (送信)]** を選択します。
3. 新しいサブカテゴリを追加するには、次のアクションを実行します。
 - a. **[New (新規)]** を選択します。
 - b. [要素] フィールドに、「サブカテゴリ」という語を入力します。
 - c. [ラベル] フィールドにサブカテゴリ名を入力します。
 - d. [値] フィールドにサブカテゴリ値を入力します。
 - e. **[Sequence (シーケンス)]** フィールドに、シーケンス番号を入力します。
 - f. サブカテゴリが既存のカテゴリに属している場合は、カテゴリ値を [依存値] フィールドに追加します。
 - g. **[Submit (送信)]** を選択します。

結果

新しいカテゴリまたはサブカテゴリは、オペレーショナルテクノロジー インシデントレコードで選択できます。

カテゴリまたはサブカテゴリを削除する

オペレーショナルテクノロジーインシデントカテゴリまたはサブカテゴリを組織で使用しなくなった場合は、そのカテゴリまたはサブカテゴリを削除します。

始める前に

- **Operational Technology Incident Management** (オペレーショナルテクノロジーインシデント管理) にアプリケーションスコープを設定します。
- 必要なロール：admin

手順

1. 移動先 **すべて > システム定義 > 選択リスト**。
2. 条件フィルターを [テーブル] [次の値に等しい] **[sn_ot_incident]** および [要素] [次の値に等しい] [カテゴリ] または [要素] [次の値に等しい] [サブカテゴリ] に設定します。
3. 削除するカテゴリまたはサブカテゴリレコードをポイントし、チェックボックスをオンにします。
4. [選択した行のアクション] メニューで、[削除] を選択します。

結果

削除されたカテゴリまたはサブカテゴリは、オペレーショナルテクノロジー インシデントレコードで使用できなくなります。

インシデント状況モデルの作成

サイトの オペレーショナルテクノロジー (OT) インシデント状況モデルを作成します。インシデント状況モデルを使用すると、関連するインシデントのライフサイクルを管理できます。

始める前に

- **Operational Technology Incident Management** (オペレーショナルテクノロジーインシデント管理) にアプリケーションスコープを設定します。
- 必要なロール：admin

このタスクについて

状況管理を使用すると、OT インシデントサイトとそのインシデントライフサイクルの状況モデルを構成できます。サイトごとに 1 つのモデルを作成できます。

状況管理と状況モデルの詳細については、「[状況管理](#)」を参照してください。

インシデントのライフサイクルの詳細については、「[オペレーショナルテクノロジーインシデント管理](#)」を参照してください。

手順

1. 移動先 **すべて > 状況管理 > ステータスモデル**。
2. **[OT インシデント:デフォルト]** フローモデルを選択します。
3. 条件を設定します。
4. 必要に応じて、State Transitions (状況移行) コンテキストメニューで、状況遷移レコードを構成します。
たとえば、[処理中] ステータスレコードの [入力条件] フィールドを編集する場合は、ステータスレコードを選択し、変更を追加して [更新] を選択します。
5. **[Update (更新)]** を選択します。

結果

これで、状況モデルは、インシデントレコードのライフサイクルを通じて予想されるレコードワークフローを正確に記述します。

インシデントの優先度ルックアップルールの定義

オペレーショナルテクノロジーインシデントの影響度と緊急度を定義して、その優先度を計算します。その後、優先度の計算を使用して作業に優先順位を付け、組織内でサービスレベルアグリーメント (SLA) を推進することができます。

始める前に

必要なロール:ot_incident_admin

手順

1. 移動先 **すべて > 産業用ワークスペースアドミン > オペレーショナルテクノロジーインシデント管理 > 優先度ルックアップルール**。
2. **[New (新規)]** を選択します。
3. フォームで、フィールドに入力します。

[優先度ルックアップルール] フォーム

フィールド	説明
影響	ビジネスプロセスに対するインシデントの影響度の測定値。
緊急度	インシデントがビジネスに重大な影響を与える前に解決にかけられる時間を測定します。
優先度	影響度と緊急度に基づくオプション。優先度は、OT エンジニアがタスクにどの程度迅速に対処すべきかを示します。
アプリケーション	ルールのスコープ。スコープは、すべてのアプリケーションとスコープ対象アプリケーションのどちらでルールを使用できるかを定義します。
アクティブ	ルールがアクティブかどうかを定義するオプション。
順番	ルールが [優先度] ルックアップリストに表示される順番。このフィールドは、最初に行われるルールを示します。

i 注:

優先度は、次の表のサンプルデータルックアップルールに従って計算されます。

優先度のデータルックアップルール

影響 ^{***} にそれぞれ変更します。	緊急度	優先度
1 - 高	1 - 高	1 - 重大
1 - 高	2 - 中	2 - 高
1 - 高	3 - 低	3 - 中
2 - 中	1 - 高	2 - 高
2 - 中	2 - 中	3 - 中
2 - 中	3 - 低	4 - 低
3 - 低	1 - 高	3 - 中
3 - 低	2 - 中	4 - 低
3 - 低	3 - 低	5 - 計画中

デフォルトでは、[優先度] フィールドは読み取り専用で、[影響度] と [緊急度] の値を選択して設定する必要があります。優先度の計算方法を変更するには、優先度ルックアップルールを変更するか、**[Priority is managed by Data Lookup - set as read-only]** (優先度はデータルックアップで管理される - 読み取り専用として設定) UI ポリシーを無効にして独自のビジネスロジックを作成します。

4. [Submit (送信)] を選択します。

システムプロパティの設定

必要に応じてインシデントのプロパティを有効にできるように、オペレーショナルテクノロジーインシデント管理 アプリケーションのシステムプロパティを設定します。

始める前に

- ナビゲーションバーの地球儀アイコン (🌐) を選択して、アプリケーションスコープを **Operational Technology** インシデント管理 に設定します。
- 必要なロール:sn_ot_incident_admin

手順

- 移動先 **すべて > 産業用ワークスペースアドミン > オペレーショナルテクノロジーインシデント管理 > システムプロパティ**.
- 組織の必要に応じて、次のプロパティを有効にします。

プロパティ	説明
com.sn_ot_inc_mgmt.sn_ot_incident_task.closure	Related Incidents (関連インシデント) を閉じたかキャンセルしたときに、開いている OT インシデントタスクを閉じるプロパティ。 関連するインシデントがクローズまたはキャンセルされたときにオープンインシデントタスク

プロパティ	説明
	をクローズする場合は、このフィールドを [はい] に設定します。
com.snc.sn_ot_incident.create.child.enable	OT インシデントレコードの子インシデント機能を作成するプロパティ。 インシデントレコードの子インシデントを作成する場合は、このフィールドを [はい] に設定します。
com.snc.sn_ot_incident.copy.attributes	親インシデントから子インシデントにコピーする属性をリストするプロパティ。 必要な属性をカンマ区切りリストに追加します。
glide.ui.sn_ot_incident_activity.fields	アクティビティフォーマッターに表示されるフィールド。 カンマ区切りリストに必要なフィールドを追加します。

3. [Save (保存)] を選択して変更を保存します。

アサインルールの作成

アサインルールの 1 つ以上の条件に従って、オペレーショナルテクノロジー (OT) インシデントをグループまたはユーザーに自動的にアサインするアサインルールを作成します。アサインルールを使用して、OT インシデントを開いたときに実行します。

始める前に

必要なロール：admin

手順

1. 移動先 **すべて** > システムポリシー > ルール > アサイン。
2. **[New (新規)]** を選択します。
3. フォームのフィールドに入力します。
フィールド値の説明については、「[\[アサインルール\] フォーム](#)」を参照してください。
4. **[Submit (送信)]** を選択します。

次のタスク

アサインルールについては、「[アサインルールの定義](#)」を参照してください。

オペレーショナルテクノロジーインシデント管理の使用

オペレーショナルテクノロジーインシデント管理 アプリケーションに必要なすべてのセットアップタスクを完了すると、OT インシデントの管理を開始できます。

OT インシデントの管理

アサインされたユーザーロールに応じて、産業用 ワークスペース で OT インシデントを管理できます。

産業用 ワークスペースでは、OT インシデントライターは次の場所から OT インシデントフォームを作成および更新できます。

- OT デバイスフォーム
- 機器モデルエンティティフォーム
- リストモジュール

産業用 ワークスペースでは、OT インシデントビューアーは次の場所で OT インシデントを表示できます。

- OT デバイスレコードの [関連レコード] タブにある [OT インシデント] 関連リスト
- 機器モデルエンティティレコードの **[OT インシデント]** タブ
- **OT** インシデントリストモジュールの下の次のリスト:
 - 自分にアサイン済み
 - 自分のサイトに所属
 - すべて

OT インシデントアドミニストレーターは、産業用 ワークスペース 内の任意の OT インシデントレコードに移動して削除できます。

インシデントのアクセス制御

オペレーショナルテクノロジー (OT) データと情報技術 (IT) データを分離するために、OT ユーザーのみが OT インシデントを表示できます。

次の表では、オペレーショナルテクノロジーインシデント管理 ロールを持つユーザーのロールと権限について説明します。

ロール	権限
sn_ot_incident_write	OT インシデントを作成、編集、および読み取ることができます。
sn_ot_incident_read	OT インシデントの読み取りのみできます。
sn_ot_incident_admin	任意の機器モデルエンティティのインシデントレコードを作成、表示、編集、および削除できます。

アクセス制御ルールについて詳しくは、[アプリケーション管理アプリのアクセス制御ルール](#) を参照してください。

インシデントを報告

オペレーショナルテクノロジー (OT) インシデントレコードを作成して、想定される標準的な運用からの逸脱を報告します。

始める前に

必要なロール:sn_ot_incident_write

手順

1. 移動先 **すべて** > 産業用ワークスペース.
2. デバイスレコードまたは機器モデルエンティティレコードを選択します。

i 注: OT インシデントリストモジュールで OT インシデントを発生させることもできます。

3. [OT インシデント] タブを選択します。

4. [New (新規)] を選択します。

5. フォームで、フィールドに入力します。

デバイスレコードを選択した場合、[サイト] フィールドと [OT デバイス] フィールドは自動的に入力されます。機器モデルエンティティレコードを選択した場合、[サイト] フィールドと [機器モデルエンティティ] フィールドは自動的に入力されます。OT インシデントが [OT インシデント] リストモジュールから発生した場合、これらのフィールドは自動的に入力されません。

i 注: 組織で、インシデント管理プロセスに準拠するようにインシデントフォームとそのフィールドを設定している。次の表に、一般的な OT インシデントフォームのフィールドを示します。

オペレーショナルテクノロジー インシデントフォーム

フィールド	説明
簡単な説明	インシデントの簡単な説明
説明	インシデントの詳細な説明
番号	Operational Technology Incident (OTINC) にプリフィックスされている、システムが生成した一意のインシデント番号。
問い合わせユーザー	問題について OT エンジニアに連絡したユーザー。
影響	インシデントが産業プロセスに及ぼす影響の測定値。
緊急度	インシデントがビジネスに重大な影響を及ぼすまでに、解決を遅らせることができる時間の指標。
状況	OT インシデントの状況。ステータスは、いくつかの解決の段階を通じてインシデントを移動させ、インシデントを追跡します。
カテゴリ	問題の種類。カテゴリを選択し、該当する場合は次にサブカテゴリを選択します。
サブカテゴリ	選択したカテゴリ内の問題の種類。
ウォッチリスト	コメントが追加されたときにこのインシデントに関する通知を受け取るユーザー。
作業メモリスト	作業メモが追加されたときにこのインシデントに関する通知を受け取るユーザー。
サイト	問題が発生したサイト。
OT デバイス	サイトで影響を受ける OT デバイス。
設備モデルのエンティティ	サイトで影響を受ける機器モデルの機器モデルエンティティ。
ビジネスへの影響度	OT インシデントのビジネスインパクトに関する詳細情報。

フィールド	説明
アサイン先グループ	インシデントで動作するアサイン先グループ。タイプが OT のあらゆるグループがアサイン先グループになれます。
アサイン先	このインシデントを担当するユーザー。アサイン先グループが変更されると、[アサイン先] フィールドはクリアされます。 選択できるのは、[アサイン先グループ] フィールドに含まれ、 sn_ot_incident_write ロールを持つユーザーのみです。[アサイン先グループ] フィールドが空の場合、sn_ot_incident_write ロールを持つ任意のサイトユーザーを選択できます。
親インシデント	このインシデントレコードの親インシデントの一意の番号。
追加コメント	必要に応じて追加する、問題に関する詳細情報。追加のコメントは、インシデントを表示できるすべてのユーザーに表示されます。
作業メモ	インシデントの解決方法に関する情報、またはインシデントの解決手順 (該当する場合)。

6. [Save (保存)] を選択します。

結果

これで、アサイン先グループとアサイニーは、対処が必要な OT インシデントがあることを認識しました。

オペレーショナルテクノロジー変更要求からのオペレーショナルテクノロジーインシデントの作成

産業用ワークスペース の OT 変更レコードから直接、OT 変更要求に関連する オペレーショナルテクノロジー (OT) インシデントを作成します。

始める前に

必要なロール:sn_ot_change_writeおよびsn_ot_incident_write

このタスクについて

次の関連リストは、産業用ワークスペース の OT 変更レコードで使用できるため、OT インシデントを作成したり、変更要求に関連する既存の OT インシデントを追加したりできます。

変更により修正されたインシデント

選択した変更レコードによって修正される OT インシデント。

変更起因するインシデント

選択した変更レコードによって発生した OT インシデント。

手順

1. 移動先 **すべて > 産業用ワークスペース**.
2. 産業用ワークスペースリストビューを開きます。
3. [OT 変更要求] リストモジュールで、利用可能なリストのいずれかを選択します。

4. いずれかのサイトで、インシデントの作成元とする変更レコードを選択します。
5. OT インシデントを作成するには、次のアクションを完了します。
 - a. [変更により修正されたインシデント] 関連リストまたは [変更に起因するインシデント] 関連リストで、[新規] を選択します。
 - b. フォームで次のフィールドに入力します。

OT インシデントフォーム

フィールド	説明
番号	Operational Technology Incident (OTINC) にプリフィックスされている、システムが生成した一意のインシデント番号。
開始日時	インシデントが送信された日付。
簡単な説明	インシデントの簡単な説明
サイト	問題が発生したサイト。
設備モデルのエンティティ	サイトで影響を受ける機器モデルの機器モデルエンティティ。
OT デバイス	サイトで影響を受ける OT デバイス。

- c. [Save (保存)] を選択します。
6. 既存の OT インシデントを変更要求レコードに追加するには、次のアクションを実行します。

i 注: OT インシデントは、最大 1 つの OT 変更要求で修正でき、最大 1 つの OT 変更要求によって発生します。別の OT 変更要求に既に関連付けられている OT インシデントを追加できますが、そうすると既存の関係が上書きされます。

 - a. [変更により修正されたインシデント] 関連リストまたは [変更に起因するインシデント] 関連リストで、[追加] を選択します。
 - b. 追加する OT インシデントを選択します。
 - c. [Add (追加)] を選択します。

結果

変更要求からインシデントを作成した後、関連リストでインシデントレコードを表示するか、産業用ワークスペース リストビューに戻ることができます。次に、[**OT インシデント**] リストモジュールで利用可能なリストのいずれかを選択します。

インシデントを履行するタスクの作成

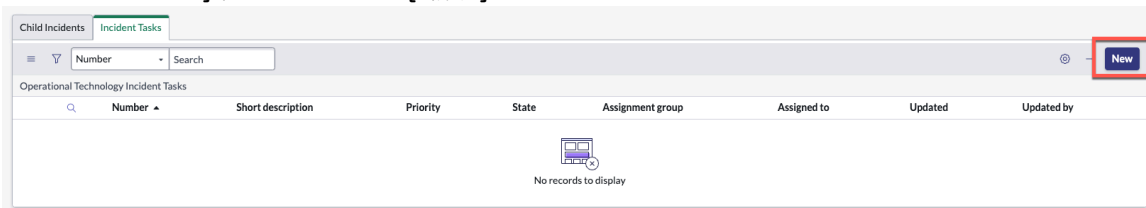
オペレーショナルテクノロジー (OT) インシデントを履行するための一連のインシデントタスクを作成します。インシデントタスクは、インシデントの解決に必要な作業を分割し分類するのに役立ちます。

始める前に

必要なロール:sn_ot_incident_write

手順

1. 移動先 すべて > インシデント > オープン。
2. タスクを作成する OT インシデントレコードを開きます。
3. [インシデントタスク] 関連リストで、[新規] を選択しま



す。

[インシデントタスク] 関連リストが表示されない場合は、追加する必要があります。

4. フォームで、フィールドに入力しま

す。

インシデントタスクフォーム

フィールド	説明
番号	一意のシステム生成インシデントタスク番号。
インシデント	タスクが関連するインシデント。
サイト	影響を受けるインシデントサイト。 <i>i</i> 注: このフィールドは読み取り専用で、該当する場合は関連インシデントサイトが自動的に入力されます。
機器モデルエンティティ	影響を受ける機器モデルエンティティ。 <i>i</i> 注: このフィールドは読み取り専用であり、該当する場合は関連する機器モデルエンティティが自動的に入力されます。
OT デバイス	影響を受ける OT デバイス。

フィールド	説明
	i 注: このフィールドは読み取り専用であり、該当する場合は関連する OT デバイスが自動的に入力されます。
状況	インシデントの解決のいくつかのステージを通じてインシデントタスクを追跡するためのステータス。
優先度	インシデントタスクの優先度。
アサイン先グループ	インシデントタスクを担当するグループ。このフィールドを空のままにすると、インシデントが自動的にアサインされます。
アサイン先	インシデントタスクがアサインされて作業するユーザー。 i 注: [アサイン先グループ] が変更された場合、[アサイン先] フィールドはクリアされます。
簡単な説明	インシデントタスクの簡単な説明。
説明	インシデントタスクの詳細な説明。
メモ	
作業メモリスト	作業メモが追加されたときにこのインシデントタスクに関する通知を受け取るユーザー。 i 注: [自分を追加] アイコン [] を選択して、自分を作業メモリストに追加できます。
作業メモ	インシデントタスクの解決方法に関する情報、またはインシデントタスクの解決に必要な手順 (該当する場合)。

5. [Submit (送信)] を選択します。

結果

これで、ServiceNow AI Platform または 産業用ワークスペース の [インシデントタスク] タブで、関連する OT インシデントレコードのインシデントタスクを表示および編集できます。

次の場所の 産業用ワークスペース リストビューでインシデントタスクを表示することもできます。

- 自分にアサインされたインシデントタスク: **OT** タスク > 自分にアサイン済み
- グループにアサインされたインシデントタスク: **OT** タスク > 自分のグループにアサイン済み
- 未アサインのインシデントタスク: **OT** タスク > 未アサイン

子インシデントを作成する

子 オペレーショナルテクノロジー (OT) インシデントレコードを作成して、報告された逸脱の一部をキャプチャし、個別に処理できるようにします。子インシデントを作成すると、同じ親に関連する複数のインシデントを整理するのに役立ちます。

始める前に

- [子インシデントを作成] 機能 (`com.snc.incident.create.child.enable`) プロパティを有効にします。詳細については、「[システムプロパティの設定](#)」を参照してください。
- 必要なロール: `sn_ot_incident_write`

このタスクについて

子インシデントにコピーされるフィールドは、`com.snc.sn_ot_incident.copy.attributes` システムプロパティを使用して構成されます。

手順

1. 産業用 ワークスペースの **[OT インシデント]** リストモジュールに移動します。
または、OT デバイスレコードまたは機器モデルエンティティレコードに移動し、**[OT インシデント]** タブを選択することもできます。
2. 子インシデントを作成する OT インシデントを開きます。
3. [子インシデント] 関連リストを選択します。
4. **[New (新規)]** を選択します。
5. 子インシデントの詳細を入力します。
6. **[Save (保存)]** を選択します。

結果

これで、親インシデントレコードで子インシデントを表示および編集できます。

サイト全体のインシデントの可視化

オペレーショナルテクノロジー (OT) インシデント履行者ロール (`sn_ot_incident_write`) を使用すると、サイトに属するインシデントを表示、作成、または編集できます。他のサイトに属するインシデントを表示して、サイトで同様のインシデントを解決することもできます。

OT インシデントの可視化の概要

OT インシデント履行者ロール (`sn_ot_incident_write`) を持つユーザーは、次のタスクを実行できます。

- 自分にアサインされた OT インシデントレコードまたはサイトに属するインシデントを表示および編集します。
- OT インシデントを作成します。
- 他のサイトに属する OT インシデントを表示します。

OT インシデント履行者ロールのメリット

OT インシデント履行者であることの主な利点は、サイト全体のインシデントを読み取り専用で可視化できることです。サイトをまたいで他のインシデントを表示すると、サイトでの同様のインシデントの解決に役立ちます。

- ❗ **注:** 他のサイトの OT インシデントを編集することはできません。サイトに属するインシデントのみを編集できます。

インシデントを表示または編集する場所

次の OT インシデントリストは、産業用 ワークスペース のリストモジュールで利用できます。

- 自分にアサイン済み:次に移動して、アサイン済みインシデントレコードを表示および編集します:
OT インシデント > 自分にアサイン済み.
- 自分のサイトに所属:サイトに属するインシデントレコードを表示および編集するには、次の場所に移動します。 **OT インシデント** > 自分のサイトに所属.
- に移動して、さまざまなサイトの既存のインシデントレコードを表示します。 **OT インシデント** > すべて.

インシデントとインシデントタスク間の同期

オペレーショナルテクノロジー (OT) インシデントタスクを使用して、他のステークホルダーとコラボレーションし、他のステークホルダーからの作業を要求できます。OT インシデントとそのタスクは同期されるため、インシデントタスクのステータスはインシデントのステータスに応じて変化します。

`com.snc.incident.ot_incident_task.closure`プロパティは、関連するインシデントがクローズまたはキャンセルされたときに、オープンインシデントタスクをクローズします。このプロパティは、OT インシデントのステータスに基づいて OT インシデントタスクで実行されるさまざまなアクションを担当します。

OT インシデントとそのオープン OT インシデントタスク間の同期は次のようになります。

- OT インシデントがクローズされると、オープンな OT インシデントタスクのステータスが [未完了でクローズ] に設定されます。
- OT インシデントがキャンセルされると、オープンな OT インシデントタスクのステータスが [スキップしてクローズ] に設定されます。

インシデントメール通知

オペレーショナルテクノロジー (OT) インシデントメール通知を使用して、インシデントに変更が加えられたときにユーザーにアラートを送信します。

通知を次の表に示します。

OT インシデントメール通知

通知の名称	送信時	[Who receives it]	内容
コメントされたインシデント	余分のコメントが追加された場合	アサイン先、ウォッチリスト	件名:<インシデント #> - コメントが追加されました 本文:コメントが追加されました インシデントへの URL
オープン済みで未アサインのインシデント	[アサイン先] フィールドが空に変わり、[アクティブ] が true になったとき	インシデントをオープンしたユーザー	件名:<インシデント #> - 未アサイン 本文: このインシデントを担当する人を指定してください

OT インシデントメール通知 (続く)

通知の名称	送信時	[Who receives it]	内容
			インシデントへの URL
クローズ済みインシデント	インシデントがクローズされている場合	アサイン先グループ	件名:<インシデント #> - クローズ済み 本文:解決コードと解決メモ
変更されたインシデントの優先度	トリガーされた場合	アサイン先、アサイン先グループ、ウォッチリスト	件名:<インシデント #> - 優先度が変更されました 本文:新しい優先度:<優先度>
解決済みインシデント	インシデントのステータスが [解決済み] に変更されたとき	発信者、ウォッチリスト	件名:<インシデント #> - 解決済み 本文:解決コードと解決メモ
自分のグループに割り当てられたインシデント	[アサイン先グループ] フィールドが変更されたとき	アサイン先グループ、ウォッチリスト	件名:<インシデント #> - アサイン先グループ<にアサインされます> 本文:優先度、簡単な説明、説明 インシデントへの URL
自分に割り当てられたインシデント	[アサイン先] フィールドが変更されたとき	アサイン先、ウォッチリスト	件名:<インシデント #> があなたにアサインされました 本文:優先度、簡単な説明、説明 インシデントへの URL
自分のためにオープンされたインシデント	新規インシデントが作成させる場合	問い合わせユーザー	件名:<インシデント #> - 要求に応じてオープンされました 本文:優先度、簡単な説明、説明 インシデントへの URL

OT インシデントメール通知 (続く)

通知の名称	送信時	[Who receives it]	内容
変更されたインシデントの状況	インシデントの状況が変わったとき	アサイン先、ウォッチリスト	件名:<インシデント #> - ステータス変更済み 本文:簡単な説明、古いステータス、新しいステータス インシデントへの URL

OT インシデントレコードからのメールの作成

OT インシデントレコードで直接メールを作成して、チームや他のユーザーがインシデントについて簡単に更新できるようにします。

始める前に

必要なロール:sn_ot_incident_write

手順

1. 移動先 すべて > 産業用ワークスペース.
2. 産業用 ワークスペースリストビューを開きます。
3. [OT インシデント] リストモジュールで、利用可能なリストのいずれかを選択します。
4. メールを送信するインシデントレコードを選択します。
5. インシデントヘッダーで、[その他のアクション] ... を選択してメニューを開きます。 ボタンをクリックします。
6. **[Compose Email (メールの作成)]** を選択します。
7. メールテンプレートで、フォームに入力します。

メールテンプレートフォーム

フィールド	説明
移動先	メールの送信先のユーザー (複数可)。 このフィールドでは、OT インシデントレコードの [アサイン先] フィールドにユーザーが自動的に入力されます。
件名	メールの件名。 このフィールドには、OT インシデントレコードの番号とその簡単な説明が自動的に入力されます。
本文	OT インシデントに関連するユーザーに送信する更新。

8. オプション: メールが応答の場合は、[応答テンプレート] フィールドで応答テンプレートを使用してメール本文に入力できます。

9. オプション: メールを下書きとして保存するには、**下書きとして保存** を選択します。

10. **[メール送信]** を選択します。

結果

メールテンプレートで指定した 1 つまたは複数のユーザーにメールが送信されます。

インシデントを解決してクローズする

問題が修正されたら、オペレーショナルテクノロジー (OT) インシデント状況を **[解決済み]** に設定できます。解決策に問題がなければ、インシデントをクローズできます。インシデントは、インシデントの自動クローズプロパティに基づいて、一定時間後に自動的にクローズされます。

始める前に

必要なロール:sn_ot_incident_write

手順

1. 移動先 **すべて > インシデント > オープン**.
2. 解決してクローズする進行中の OT インシデントを開きます。
3. **[解決情報]** 関連リストで、次のフィールドに入力します。

のフィールド

フィールド	説明
解決コード	解決済みケースを分類するための情報。 複製 インシデントは既存のインシデントの複製であり、クローズする必要があります。 既知のエラー インシデントは既知のエラーのソリューションによって解決されました。 問い合わせユーザーによって解決済み 問題について OT エンジニアに連絡したユーザーによってインシデントが解決されました。 変更により解決済み インシデントは OT 変更要求で解決されました。 OT 変更要求の詳細については、「変更要求を作成」を参照してください。 問題により解決済み インシデントは、インシデントの原因を特定する問題で解決されました。 問題の詳細については、「問題の管理」を参照してください。

フィールド	説明
	要求により解決済み インシデントは OT 要求によって解決されました。 OT 要求の詳細については、「でオペレーショナルテクノロジー要求を作成する 産業用 ワークスペース」を参照してください。 Solution provided (提供されたソリューション) 他の解決コードに適合しないインシデントのソリューションが提供されました。
解決メモ	インシデントがどのように解決されたかを説明します。

4. [状態] フィールドで、[解決済み] を選択します。

5. **[Update (更新)]** をクリックします。

インシデントレコードの関連デバイスと機器モデルエンティティを編集する

関連する オペレーショナルテクノロジー (OT) デバイスと機器モデルエンティティを OT インシデントレコードから直接追加または削除します。インシデントと影響を受けるアイテムの関係を追跡できます。

始める前に

必要なロール:sn_ot_incident_write または sn_ot_incident_admin

手順

1. 移動先 **すべて > 産業用ワークスペース**.
2. 産業用 ワークスペースリストビューを開きます。
3. [OT インシデント] リストモジュールで、利用可能なリストのいずれかを選択します。
4. 編集するインシデントレコードを選択します。
5. 関連する OT デバイスを追加または削除します。

アクション	説明
インシデントレコードから関連する OT デバイスを追加する	a. [影響を受ける OT デバイス] 関連リストを選択します。 b. [Add (追加)] を選択します。 c. [OT デバイスの追加 (Add OT Devices)] ウィンドウで、追加するデバイスの横にあるチェックボックスをオンにします。 d. [Add (追加)] を選択します。

アクション	説明
インシデントレコードから関連する OT デバイスを削除する	a. [影響を受ける OT デバイス] 関連リストを選択します。 b. 削除するデバイスの横にあるチェックボックスをオンにします。 c. [削除] ボタンを選択します。 d. 表示される確認ウィンドウで、[削除] を選択します。

これで、OT デバイスが [影響を受ける OT デバイス] 関連リストの変更レコードに追加または削除されました。

6. インシデントレコードに対して機器モデルエンティティを追加または削除するには、ステップ 4 と 5 を繰り返しますが、[影響を受ける機器モデルエンティティ] 関連リストで行います。

オペレーショナルテクノロジーインシデント管理の参照

参照トピックには、オペレーショナルテクノロジーインシデント管理 アプリケーションに関する追加情報が記載されています。

[アサインルール] フォーム

アサインルールは、アサインルールの 1 つ以上の条件に従って、オペレーショナルテクノロジー (OT) インシデントをグループまたはユーザーに自動的にアサインします。

次の表に、アサインルールフォームのフィールド値を示します。

[アサインルール] フォーム

フィールド	説明
名前	アサインルールの説明的な名前です。
アクティブ	アサインルールをアクティブ化するオプション。
適用先	
テーブル	アサインルールを適用するレコードを格納したテーブルです。 i 注: OT インシデントに固有のアサインルールの場合は、[テーブル] フィールドを オペレーショナルテクノロジーインシデント [sn_ot_incident] に設定します。 リストには、アサインルールと同じスコープ内にあるテーブルビューとデータベースビューのみが表示されます。タスクテーブルを拡張するカスタムテーブルを選択し、アサインルールが正しく機能するようにするには、<a href="https://<instance_name>.service-now.com/cache.do">https://<instance_name>.service-now.com/cache.do に移動してインスタンスキャッシュをクリアする必要があります。 i 重要: システムキャッシュをクリアすると、全体的なパフォーマンスに影響が及ぶ可能性があります。システムの応答時間が低下する可能性があります。キャッシュのフラッシュを営業時間中に実行したり、キャッシュのフラッシュを自動的に実行するようにトリガーしたりしないでください。

[アサインルール] フォーム (続く)

フィールド	説明
条件	アサインルールが適用される条件。
アサイン先	
ユーザー	イベントがアサインされているユーザー。
グループ	イベントがアサインされているグループ。
スクリプト	
スクリプト	高度なアサインルール機能を指定するスクリプト。current.variable_pool 変数セットを使用できます。 i 注: スクリプトの入力が正しいこと、および入力タイプがアサインルールスクリプトのフィールドタイプと一致していることを確認してください。たとえば、アサインルールスクリプトが整数フィールドの値を設定し、スクリプトの値が文字列に設定されている場合、アサインルールによって予期しない結果が生じる可能性があります。
オプションのフィールド	
一致条件	任意 いずれかの条件が満たされると、アサインルールが適用されます。 すべて すべての条件が満たされると、アサインルールが適用されます。
実行順序	アサインルールが処理される順番。アサインルールが競合する場合、順序値が小さいルールが大きい値のルールよりも優先されます。順序値が同じ数値に設定されている場合、最初に一致した条件を持つアサインルールが、最初に一致しない他のルールよりも優先されます。一致条件を備えた最初のアサインルールのみがレコードに対して実行されます。

オペレーショナルテクノロジーインシデント管理とともにインストールされるコンポーネント

ユーザーロールなど、いくつかのタイプのコンポーネントを、オペレーショナルテクノロジーインシデント管理 (sn_ot_inc_mgmt) プラグインのアクティブ化とともにインストールできます。

i 注: アプリケーションファイルテーブルには、このアプリケーションとともにインストールされたコンポーネントがリストされています。このテーブルへのアクセス手順については、「[アプリケーションとともにインストールされているコンポーネントの検索](#)」を参照してください。

インストールされているロール

ロール	説明	含まれるロール
OT インシデントアドミン [sn_ot_incident_admin]	任意の機器モデルエンティティの OT インシデントレコードを作成、表示、削除、編集できます。優先度ルックアップルールと	- cmdb_ot_isa_viewer_all - sn_ot_incident_write

ロール	説明	含まれるロール
	OT インシデントシステムプロパティ を設定できます。	
OT インシデントリーダー [sn_ot_incident_read]	OT インシデントレコードの表示のみできます。	• cmdb_ot_viewer • cmdb_ot_isa_viewer
OT インシデント履行者 [sn_ot_incident_write]	OT インシデントレコードを表示、作成、編集できます。	sn_ot_incident_read

- i** 注: OT インシデントユーザー [ot_incident_user] ロールは複製される。このロールがアサインされているユーザーは、スケジュール済みジョブを実行して新しい オペレーショナルテクノロジーインシデント管理 ロールを割り当てることができます。詳細については、「[ユーザーに新しいロールをアサインする](#)」を参照してください。

インストールされるテーブル

テーブル	説明
OT インシデント [sn_ot_incident]	サイト全体で報告された OT インシデントのリスト。
OT インシデントタスク [sn_ot_incident_task]	さまざまな OT インシデントで作成された OT インシデントタスクのリスト。
OT インシデント優先度ルールルックアップ [dl_ot_inc_priority]	OT インシデントの優先度を計算するためのルールのリスト。

関連情報

OT 拡張クラスと関連アプリケーションの詳細を確認してください。

拡張クラスの概要

拡張クラスは、オペレーショナルテクノロジー管理 が 構成管理データベース (CMDB)でどのように機能するかを理解するのに役立ちます。

オペレーショナルテクノロジー (OT) 拡張クラス

構成管理データベース (CMDB) は OT のクラスを更新します。

関連アプリケーション

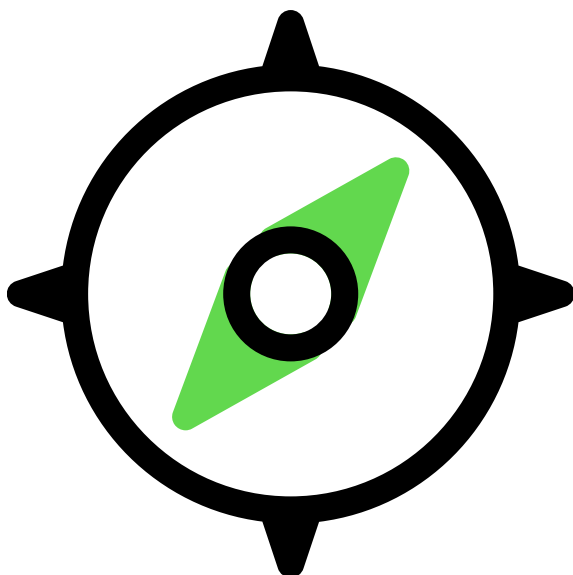
IT Service Management

ServiceNow IT Service Management アプリケーションを オペレーショナルテクノロジーインシデント管理 と統合すると、エンジニアは OT デバイスと本番プロセスの問題を迅速に解決できます。

オペレーショナルテクノロジー変更管理

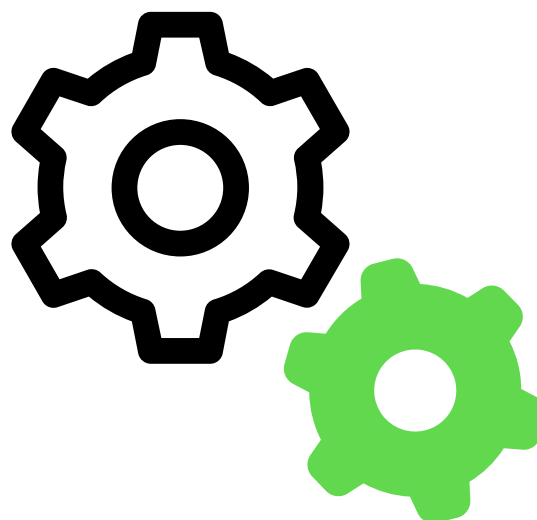
ServiceNow[®] オペレーショナルテクノロジー変更管理アプリケーションを使用すると、組織はオペレーショナルテクノロジー (OT) デバイスと本番プロセスに変更を実装できます。

探索



オペレーショナルテクノロジー変更管理 の探索

構成



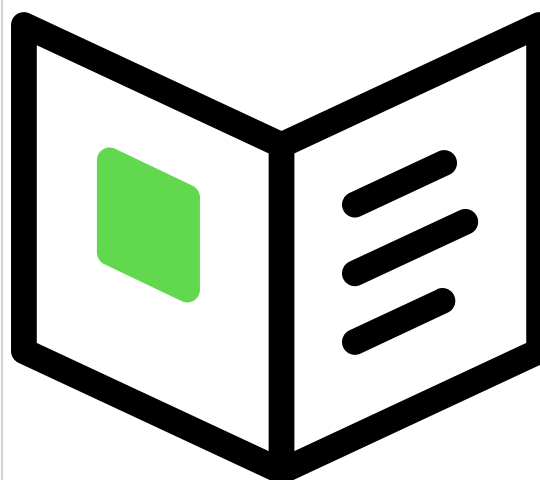
実装の計画と構成

使用方法



オペレーショナルテクノロジー変更管理 の使用

参照



関連情報とアプリケーションの詳細を取得

自動翻訳

オペレーショナルテクノロジー変更管理の探索

オペレーショナルテクノロジー変更管理アプリケーションの詳細を確認してください。

オペレーショナルテクノロジー変更管理の概要

オペレーショナルテクノロジー変更管理アプリケーションの詳細については、Operational Technology Service Management製品スイートの概要をご覧ください。

[https://player.vimeo.com/video/1019801515?](https://player.vimeo.com/video/1019801515?badge=0&autoplay=0&player_id=0&app_id=58479)

[badge=0&autoplay=0&player_id=0&app_id=58479](https://player.vimeo.com/video/1019801515?badge=0&autoplay=0&player_id=0&app_id=58479)

主な機能

オペレーショナルテクノロジー変更管理 アプリケーションでは、次の主要な機能を使用できます。

- すべてのステークホルダーを結び付ける、デジタル化変更ワークフロー。
- さまざまな変更管理プロセス (ワークフロー) を持つサイト。
- IT Change Management と オペレーショナルテクノロジー変更管理 は分離されていますが、必要に応じて組み合わせることができます。
- オペレーショナルテクノロジーインシデント管理およびオペレーショナルテクノロジー脆弱性対応アプリケーションと統合されたオペレーショナルテクノロジー変更管理ワークフロー。
- ダウンタイムスケジュールに合わせて調整された、設備モデルエンティティの工場フロアの変更。

オペレーショナルテクノロジー変更管理を使用して生産プロセスを最適化する

オペレーショナルテクノロジー変更管理 アプリケーションを使用すると、チームメンバーは、オペレーショナルテクノロジー (OT) デバイスや産業機器の構成の変更と共に取り組むことができます。たとえば、最適化、生産プロセスの改変、脆弱性の修正などです。

オペレーショナルテクノロジー変更管理の概要

オペレーショナルテクノロジー変更管理 アプリケーションを使用すると、OT 変更要求を情報技術 (IT) 変更要求とは別に管理できます。OT 変更要求をネットワークタイプ別に IT 変更要求から分離でき、サイトごとに OT 変更要求を管理できます。

次の例は、組織に オペレーショナルテクノロジー変更管理 を適用する方法を示しています。

- OT デバイスの脆弱性の修正を担当する OT 修復オーナーが、一連の脆弱性を修正するための変更を開始する。
- OT 構成とプラントエンジニアリングアクティビティを担当する OT 技術者が、作業現場で故障したロボットアームを修理するための変更を実行したいと考えています。
- 全体的な生産アクティビティを担当するプラント長が、エンジニアリングチームによって要求された変更をレビューして承認したいと考えています。

OT 変更要求

OT 変更要求は、OT ネットワーク上の OT デバイスからサービスが中断されたときに発生します。場合によっては、変更要求の作成時に OT デバイスがわからないことがあります。産業用 ワークスペース から OT 変更要求を作成すると、変更要求には **OT** のネットワークタイプが自動的にアサインされます。この属性は、OT 変更要求と IT 変更要求を区別するために使用されます。このフィールドは、デフォルトでは表示されません。OT デバイスの詳細については、「[OT デバイスの関連アイテムと関連リスト](#)」を参照してください。

OT 変更要求の作成方法の詳細については、「[変更要求を作成](#)」を参照してください。

IT と OT の変更の分離

オペレーショナルテクノロジー変更管理 アプリケーションがインスタンスにインストールされている場合は、[ネットワークタイプ] で **[IT]**、**[OT]**、または [なし] を選択できます。新しい変更要求には、デフォルトで「なし」のネットワークタイプが割り当てられます。

オペレーショナルテクノロジー変更管理 モデルステータス移行

次の表に、基本的な OT 変更モデルと高度な OT 変更モデルの両方の オペレーショナルテクノロジー変更管理 モデル状況移行を示します。OT 変更モデルの詳細については、「[変更要求を満たす変更モデルを選択](#)」を参照してください。

基本的な OT 変更モデルの状況

状況	説明
新規	OT 変更要求が開始されます。
計画	OT 変更要求は、次の基準で分析されます。 - 理由 - Implementation plan (実装計画) - Risk and impact analysis (リスクと影響度の分析) - バックアウトプラン - テスト計画 - 変更のスケジュール設定
実装	変更はターゲット OT デバイスで実行されます。
クローズ済み	変更完了後、変更レコードがクローズされます。
キャンセル済み	変更レコードはキャンセルされ、変更は OT デバイスに適用されません。

高度な OT 変更モデルの状況

状況	説明
新規	OT 変更要求が開始されます。
計画	OT 変更要求は、次の基準で分析されます。 - 理由 - Implementation plan (実装計画) - Risk and impact analysis (リスクと影響度の分析) - バックアウトプラン - テスト計画 - 変更のスケジュール設定

高度な OT 変更モデルの状況 (続く)

状況	説明
承認	レビュー担当者は、OT 変更要求を承認または拒否します。
実装	変更はターゲット OT デバイスで実行されます。
実装後のレビュー	必要に応じて OT 変更タスクを追加し、次のチェックを実行します。 • 電氣的チェック • ネットワークチェック • 品質チェック • 安全性チェック
クローズ	変更完了後、変更レコードがクローズされます。
キャンセル済み	変更レコードはキャンセルされ、変更は OT デバイスに適用されません。

オペレーショナルテクノロジー変更管理の構成

ServiceNow オペレーショナルテクノロジー (OT) ソリューションのデータ基盤を作成できるように、オペレーショナルテクノロジー変更管理 アプリケーションを構成します。

admin ロールを持っている場合は、ガイド付きセットアップを使用して オペレーショナルテクノロジー変更管理 アプリケーションのセットアップをガイドできます。ガイド付きセットアップは、アプリケーションの構成を支援するツールです。構成アクティビティをカテゴリに整理します。これらのカテゴリには、セットアップタスクに関する情報、各タスクを完了するための手順、および構成を実行するインスタンス内のページへのリンクが含まれています。役立つヘルプコンテンツへのリンクも提供されます。

i 注:

オペレーショナルテクノロジー変更管理 は Utah P4 以降のリリースに依存しています。

ガイド付きセットアップにアクセスするには、産業用ワークスペースアドミン > ガイド付きセットアップ。

次の表では、オペレーショナルテクノロジー変更管理 アプリケーションのガイド付きセットアップタスクとその目的について説明します。

タスク	目的
1. ServiceNow Storeからオペレーショナルテクノロジー変更管理アプリケーションをインストールします。	オペレーショナルテクノロジー変更管理 アプリケーションとサポートプラグインをインストールします。
2. オペレーショナルテクノロジー変更管理 ロールを割り当てます。	各ユーザーが使用できるアクションを制御するルールを割り当てます。

タスク	目的
3. オペレーショナルテクノロジー変更管理 カテゴリを設定します。	組織に必要な OT 変更のカテゴリを構成します。
4. オペレーショナルテクノロジー変更管理 モデルを選択します。	組織の変更モデルを選択します。

オペレーショナルテクノロジー変更管理 をインストール

admin ロールをお持ちであれば、オペレーショナルテクノロジー変更管理 アプリケーション (sn_ot_chg_mgmt) をインストールできます。

始める前に

- アプリケーションとその関連するすべての ServiceNow Store アプリケーションに有効な ServiceNow エンタイトルメントがあることを確認してください。詳細については、次を参照してください。 [のエンタイトルメントを取得する ServiceNow 製品またはアプリケーション](#)。
- オペレーショナルテクノロジー変更管理アプリケーションには次のプラグインが必要です。オペレーショナルテクノロジー変更管理 アプリケーションをインストールする前に、これらのプラグインがアクティブ化されていることを確認してください。

必須の ServiceNow プラグイン

CMDB CI クラスモデル (sn_cmdb_ci_class)

構成管理データベース (CMDB) CI クラスモデルストアアプリは、クラスの説明、識別ルール、識別子エントリ、依存関係など、CMDB クラス階層を拡張するクラスモデルを追加します。詳細については、「[CMDB CI クラスモデルストアアプリ](#)」を参照してください。

ISA Equipment Model (ISA 設備階層モデル) (sn_isa_model)

ISA-95 機器モデルエンティティおよびテンプレートのデータモデル詳細については、「[ISA-95 機器モデル](#)」を参照してください。

- オペレーショナルテクノロジー変更管理アプリケーションには、次のServiceNow Storeアプリケーションの一方または両方が必要です。オペレーショナルテクノロジー変更管理アプリケーションをインストールする前に、これらのアプリケーションが少なくとも 1 つインストールされていることを確認します。

必要な ServiceNow Store アプリケーション

オペレーショナルテクノロジーマネージャー

オペレーショナルテクノロジーマネージャーアプリケーションは、組織がオペレーショナルテクノロジーソリューションを使用できるようにする基盤データと関係を作成します。オペレーショナルテクノロジーマネージャー アプリケーションは、ServiceNow AI Platform の 構成管理データベース (CMDB)、サービスグラフ コネクタ、および ディスカバリー アプリケーションの使用をサポートしています。詳細については、「[オペレーショナルテクノロジーマネージャーの構成](#)」を参照してください。

製造業プロセスマネージャー

製造業プロセスマネージャー アプリケーションは、ServiceNow 産業用 ソリューションに必要な ISA-95 機器モデルデータ基盤を作成し、各産業サイトで独自のバージョンの機器モデルを作成できるようにします。詳細については、「[製造業プロセスマネージャー の構成](#)」を参照してください。

必要なロール：admin

このタスクについて

次のアイテムは、オペレーショナルテクノロジー変更管理 アプリケーションとともにインストールされます。

- プラグイン
- ストアアプリケーション
- ロールと ACL

インストールされているロールと ACL の詳細については、「[オペレーショナルテクノロジー変更管理とともにインストールされるコンポーネント](#)」を参照してください。

- i 注：** オペレーショナルテクノロジー ヴィジビリティのライセンスを持たないOperational Technology Service Managementユーザーの場合は、次の点に注意してください。
- 最新バージョンの オペレーショナルテクノロジーインシデント管理 をインストールすると、製造業プロセスマネージャー もインストールされます。
 - 最新バージョンの オペレーショナルテクノロジー変更管理 をインストールすると、製造業プロセスマネージャー もインストールされます。

Operational Technology Service Managementエクスペリエンスにアクセスできるように、最新バージョンにアップグレードする必要があります。

手順

1. 移動先 **すべて > システムアプリケーション > 利用可能なすべてのアプリケーション > すべて**。
2. フィルター基準と検索バーを使用して **オペレーショナルテクノロジー変更管理 アプリケーション** を検索します。

名前または ID でアプリケーションを検索できます。アプリケーションが見つからない場合は、ServiceNow Store に要求する必要がある場合があります。

ServiceNow Store Web サイトにアクセスして利用可能なすべてのアプリを表示し、ストアにリクエストを送信する方法について確認してください。リリースされたすべてのアプリのリリースノート情報については、「[ServiceNow Storeバージョン履歴のリリースノート](#)」を参照してください。

3. アプリケーションのインストールダイアログボックスで、アプリケーションの依存関係を確認します。

リストに表示されるのは、インストール予定である依存プラグインおよびアプリケーション、現在インストールされている依存プラグインおよびアプリケーション、またはインストールする必要がある依存プラグインおよびアプリケーションです。インストールする必要があるプラグインまたはアプリケーションがある場合は、オペレーショナルテクノロジー変更管理 アプリケーションをインストールする前にインストールする必要があります。

4. **[Install (インストール)]** を選択します。

オペレーショナルテクノロジー変更管理 ロールの割り当て

ユーザーにロールをアサインして、オペレーショナルテクノロジー変更管理 アプリケーションの機能やデータへのアクセスを制御できるようにします。

始める前に

必要なロール：admin

このタスクについて

次の表にリストされているロールを持つユーザーは、アプリケーションを使用できます。

ロール	説明
変更マネージャー [sn_ot_change_manager]	OT 変更モデルレコードを管理できます。
変更アドミン [sn_ot_change_admin]	OT 変更レコードを作成、表示、削除、編集できます。カテゴリとシステムプロパティを設定できます。
変更書き込みユーザー [sn_ot_change_write]	OT 変更レコードを作成、表示、編集できます。 IT 変更タスクをアサインし、アサインされた IT 変更タスクを編集してクローズすることもできます。 詳細については、「 サイト間での変更要求の管理 」を参照してください。
変更読み取りユーザー [sn_ot_change_read]	OT 変更レコードの表示のみできます。

手順

ServiceNow AI Platform ユーザー管理機能を使用して、ユーザーとグループにロールをアサインします。

タスク	ユーザー管理機能
ユーザーへのロールのアサイン	ユーザーへのロールの割り当て を参照してください。
グループへのロールのアサイン	グループへのロールのアサイン を参照してください。

変更要求を満たす変更モデルを選択

組織のニーズに応じて、変更要求の実行を開始する オペレーショナルテクノロジー (OT) 変更モデルを選択します。

始める前に

必要なロール:sn_ot_change_admin または admin

このタスクについて

次の 2 つの OT 変更モデルを使用できます。

- 基本的な OT 変更
- 高度な OT 変更

基本的な OT 変更モデルでは、承認なしの変更プロセスが使用されます。

OT 変更ベーシックモデルの詳細については、「[基本的な OT 変更モデルプレイブック](#)」を参照してください。

高度な OT 変更モデルでは、承認付きの変更プロセスが使用されます。変更承認ポリシーを作成し、変更要求をレビューする承認グループをアサインすることができます。変更承認の詳細については、「[オペレーショナルテクノロジー 変更承認](#)」を参照してください。

高度な OT 変更モデルの詳細については、「[高度な OT 変更モデルプレイブック](#)」を参照してください。

手順

1. 移動先 産業用ワークスペースアドミン > ガイド付きセットアップ.
2. Operational Technology Change Management (オペレーショナルテクノロジー変更管理) カテゴリで、**[Get Started (開始)]** を選択します。
3. [変更モデル] セクションの横にある [構成] を選択します。
4. 組織のニーズに合った変更モデルを選択します。
5. 必要に応じてレコードを編集します。

結果

変更モデルがシステムに適用され、OT 変更要求の作成を開始できます。

基本的な OT 変更モデルプレイブック

承認のない OT 変更が完了するまで通過する必要がある基本的なオペレーショナルテクノロジー (OT) 変更モデルプレイブックステージについて説明します。

開始

OT 変更要求の開始ステージでは、要求された変更の詳細をキャプチャし、必要に応じて変更をアサインできます。このステージには 3 つのタスクがあります。

変更の説明

フィールド	説明
簡単な説明	変更の簡単な説明
説明	変更の詳細。
カテゴリ	変更のタイプです。
サイト	変更が行われるサイト。
ウォッチリスト	コメントが追加されたときにこの変更に関する通知を受け取るユーザー。
作業メモリスト	作業メモが追加されたときにこの変更に関する通知を受け取るユーザー。

リスクをキャプチャ

フィールド	説明
優先度	変更にとどの程度迅速に対処すべきかを判断するための影響度と緊急性。
リスク	変更によってもたらされるリスクの量。
影響	変更が産業プロセスに及ぼす影響の尺度。

変更をアサイン

フィールド	説明
要求者	変更を要求するユーザー。
アサイン先グループ	変更に取り組むアサイン先グループ。タイプが OT のあらゆるグループがアサイン先グループになれます。
アサイン先	この変更を担当するユーザー。アサイン先グループが変更されると、[アサイン先] フィールドはクリアされます。

計画

OT 変更要求の計画ステージでは、変更の理由、実装計画、リスクと影響の計画、バックアウト計画、テスト計画、および変更をスケジュールする時間を追加できます。このステージには 6 つのタスクがあります。

理由を追加

フィールド	説明
理由	変更を行う必要がある理由。

実施計画を追加

フィールド	説明
実装計画	要求された変更の実装方法の詳細。

リスクと影響の分析を追加

フィールド	説明
Risk and impact analysis (リスクと影響度の分析)	この変更に関連するリスクと影響要因の詳細。

バックアウト計画を追加

フィールド	説明
バックアウトプラン	必要に応じて変更を元に戻す方法の詳細。

テスト計画を追加

フィールド	説明
テスト計画	実装された変更をテストする方法の詳細。

変更のスケジュール設定

フィールド	説明
開始予定日	変更が行われる日付。

変更のスケジュール設定 (続く)

フィールド	説明
	i 注: [スケジュールアシスタント] ボタンを選択して開始予定日フィールドを自動的に入力することで、カレンダーで利用可能なダウンタイムスロットを選択することもできます。
終了予定日	変更が終了する日付。 i 注: [スケジュールアシスタント] ボタンを選択して、カレンダーで利用可能なダウンタイムスロットを選択し、終了予定日フィールドを自動的に入力することもできます。

実装

OT 変更要求の実装ステージでは、次のタスクの詳細が提供されます。完了したら、このステージを完了としてマークできます。

変更を実行

ターゲットの OT デバイスで変更が実行され、完了したときに完了としてマークします。

クローズ

クローズステージでは、変更が完了した後に変更レコードをクローズできます。

変更レコードを閉じる

フィールド	説明
クローズコード	変更レコードがクローズされた理由。
クローズメモ	変更レコードのクローズに関するその他の詳細。

高度な OT 変更モデルプレイブック

承認のある OT 変更が完了するまでに通過する必要がある Advanced Operational Technology (OT) 変更モデルプレイブックステージについて説明します。

開始

OT 変更要求の開始ステージでは、要求された変更の詳細をキャプチャし、必要に応じて変更をアサインできます。このステージには 3 つのタスクがあります。

変更の説明

フィールド	説明
簡単な説明	変更の簡単な説明

変更の説明 (続く)

フィールド	説明
説明	変更の詳細。
カテゴリ	変更のタイプです。
サイト	変更が行われるサイト。
ウォッチリスト	コメントが追加されたときにこの変更に関する通知を受け取るユーザー。
作業メモリスト	作業メモが追加されたときにこの変更に関する通知を受け取るユーザー。

リスクをキャプチャ

フィールド	説明
優先度	変更にとどの程度迅速に対処すべきかを判断するための影響度と緊急性。
リスク	変更によってもたらされるリスクの量。
影響	変更が産業プロセスに及ぼす影響の尺度。

変更をアサイン

フィールド	説明
要求者	変更を要求するユーザー。
アサイン先グループ	変更に取り組むアサイン先グループ。タイプが OT のあらゆるグループがアサイン先グループになれます。
アサイン先	この変更を担当するユーザー。アサイン先グループが変更されると、[アサイン先] フィールドはクリアされます。

計画

OT 変更要求の計画ステージでは、変更の理由、実装計画、リスクと影響の計画、バックアウト計画、テスト計画、および変更をスケジュールする時間を追加できます。このステージには 6 つのタスクがあります。

理由を追加

フィールド	説明
理由	変更を行う必要がある理由。

実施計画を追加

フィールド	説明
実装計画	要求された変更の実装方法の詳細。

リスクと影響の分析を追加

フィールド	説明
Risk and impact analysis (リスクと影響度の分析)	この変更に関連するリスクと影響要因の詳細。

バックアウト計画を追加

フィールド	説明
バックアウトプラン	必要に応じて変更を元に戻す方法の詳細。

テスト計画を追加

フィールド	説明
テスト計画	実装された変更をテストする方法の詳細。

変更のスケジュール設定

フィールド	説明
開始予定日	変更が行われる日付。 i 注: [スケジュールアシスタント] ボタンを選択して開始予定日フィールドを自動的に入力することで、カレンダーで利用可能なダウンタイムスロットを選択することもできます。
終了予定日	変更が終了する日付。 i 注: [スケジュールアシスタント] ボタンを選択して、カレンダーで利用可能なダウンタイムスロットを選択し、終了予定日フィールドを自動的に入力することもできます。

承認

OT 変更要求の承認ステージでは、レビュー担当者が OT 変更を承認または拒否できます。このステージには 1 つのタスクのみが含まれます。

レビューしてアクションを実行

フィールド	説明
[承認] ボタン	タスクフォームのテーブルに表示されるレビュー担当者の場合は、[承認] を選択して変更を承認します。
[拒否] ボタン	タスクフォームのテーブルに表示されるレビュー担当者の場合は、[拒否] を選択して変更を却下します。

レビューしてアクションを実行 (続く)

フィールド	説明
コメント	変更の承認または拒否に関する追加情報。

変更承認の詳細については、「[オペレーショナルテクノロジー 変更承認](#)」を参照してください。

実装

OT 変更要求の実装ステージでは、次のタスクの詳細が提供されます。完了したら、このステージを完了としてマークできます。

機能を停止

必要に応じて、ターゲット OT デバイスの機能を停止した後に完了としてマークします。

LOTO を確認

ロックアウト/ターゲット (LOTO) は、メンテナンス中またはサービス中の機械の偶発的または意図しない起動を防ぐための安全手順です。LOTO の完了時に完了としてマークします。

変更を実行

ターゲットの OT デバイスで変更が実行され、完了したときに完了としてマークします。

実施後のレビュー

OT 変更要求の実装後レビューステージでは、実行されたタスクをチェックし、レビュー中に特定された残存作業に対して追加の OT 変更タスクを作成して、LOTO 取り消しプロセスを完了としてマークできます。

チェックを実行

フィールド	説明
電気チェックを実行	電気チェックが完了した後に選択するチェックボックス。
ネットワークのチェックを実行	ネットワークのチェックが完了した後に選択するチェックボックス。
品質チェックを実行	品質チェックが完了した後に選択するチェックボックス。
安全チェックを実行	安全チェックが完了した後に選択するチェックボックス。

スピノフタスクを推奨

フィールド	説明
OT 変更タスク	OT 変更に関連する変更タスクのリスト。
状況	OT 変更のステータス。ステータスは、いくつかの解決の段階を通じて変化を移動させ、変更を追跡します。

スピノフタスクを推奨 (続く)

フィールド	説明
アサイン先	この変更を担当するユーザー。アサイン先グループが変更されると、[アサイン先] フィールドはクリアされます。
簡単な説明	変更タスクの簡単な説明。

LOTO の取り消し

変更が実装されてレビューされた後、ロックアウトターゲットが取り消されたときに完了としてマークします。

スピノフタスク

[スピノフタスク] ステージには、実施後のレビューで完了する必要があるすべての変更タスクが一覧表示されます。

クローズ

クローズステージでは、変更が完了した後に変更レコードをクローズできます。

変更レコードを閉じる

フィールド	説明
クローズコード	変更レコードがクローズされた理由。
クローズメモ	変更レコードのクローズに関するその他の詳細。

オペレーショナルテクノロジー変更管理の使用

オペレーショナルテクノロジー変更管理 アプリケーションに必要なすべてのセットアップタスクを完了すると、オペレーショナルテクノロジー (OT) 変更要求の管理を開始できます。

変更要求を作成

サイトの変更を報告する オペレーショナルテクノロジー (OT) 変更要求を作成します。

始める前に

必要なロール:sn_ot_change_write

手順

1. 移動先 **すべて > 産業用ワークスペース**.
2. **[OT 変更要求]** リストビューで、開くリストを選択します。
3. **[New (新規)]** を選択します。
4. 組織に適用する OT 変更モデルを選択します。
5. **[OT 変更レコードの作成]** を選択します。
6. チームが変更要求に取り組むように、必要に応じてプレイブックを完成させます。

基本的な OT 変更モデルプレイブックの詳細については、「[基本的な OT 変更モデルプレイブック](#)」を参照してください。高度な OT 変更モデルプレイブックの詳細については、「[高度な OT 変更モデルプレイブック](#)」を参照してください。

- i** 注: プレイブックを有効にしていない場合は、OT 変更要求レコードの [詳細] タブと [関連レコード] タブのみを表示できます。

変更要求を履行するための変更タスクの作成

オペレーショナルテクノロジー (OT) 変更要求を履行するための変更タスクを作成します。変更タスクは、変更要求中に実行する必要があるすべてのタスクをキャプチャするのに役立ちます。

始める前に

必要なロール:sn_ot_change_write

このタスクについて

変更タスクは、変更要求を実行して完了するために実行する必要がある個々のステップです。

手順

1. 移動先 **すべて > 産業用ワークスペース**.
2. タスクを作成する変更レコードを選択します。
3. [変更タスク] 関連リストで、[新規] を選択します。
[変更タスク] 関連リストが表示されない場合は、追加する必要があります。
4. フォームで、フィールドに入力します。

インシデントタスクフォーム

フィールド	説明
OT 変更タスク	
簡単な説明	変更タスクの簡単な説明。
説明	変更タスクの詳細。
OT デバイス	影響を受ける OT デバイス。
OT 変更要求	関連する OT 変更要求のレコード番号。
状況	変更実装のいくつかのステージを通じて変更タスクを追跡するためのステータス。
タイプ	変更のタイプです。
アサイン	
アサイン先グループ	変更タスクを担当するグループ。このフィールドを空のままにすると、変更タスクが自動的にアサインされます。
アサイン先	変更タスクがアサインされて作業するユーザー。 i 注: [アサイン先グループ] が変更された場合、[アサイン先] フィールドはクリアされます。
メモ	

フィールド	説明
OT 変更タスク	
ウォッチリスト	コメントが追加されたときにこの変更に関する通知を受け取るユーザー。
作業メモリスト	作業メモが追加されたときにこの変更に関する通知を受け取るユーザー。
作業メモ (プライベート)	顧客が利用できない作業メモ。

5. [Save (保存)] を選択します。

結果

関連する OT 変更レコードで変更タスクを表示および編集できます。

次の場所の 産業用 ワークスペース リストビューで変更タスクを表示できます。

- 自分にアサインされたタスクの変更: **OT** タスク > 自分にアサイン済み
- グループにアサインされたタスクを変更: **OT** タスク > 自分のグループにアサイン済み
- 未アサインの変更タスク: **OT** タスク > 未アサイン

OT デバイスの詳細から変更要求を作成する

OT デバイスレコードから オペレーショナルテクノロジー (OT) 変更要求を作成します。デバイスレコードから変更要求を作成すると、サイトやビジネスサービス、[OT デバイス] フィールドなどの変更要求レコードの情報が自動的に入力されます。

始める前に

必要なロール:sn_ot_change_write

手順

1. 移動先 **すべて** > 産業用ワークスペース。
2. [すべての OT デバイス] リストで、OT デバイスレコードを選択します。
3. [関連レコード] タブで、[OT 変更要求] 関連リストを選択します。
4. **[New (新規)]** を選択します。
5. 組織に適用する OT 変更モデルを選択します。
6. [**OT** 変更レコードの作成] を選択します。
7. チームが変更要求に取り組むように、必要に応じてプレイブックを完成させます。

基本的な OT 変更モデルプレイブックの詳細については、「[基本的な OT 変更モデルプレイブック](#)」を参照してください。高度な OT 変更モデルプレイブックの詳細については、「[高度な OT 変更モデルプレイブック](#)」を参照してください。

設定した条件に応じて、次のフィールドが自動的に入力されます。

- [**OT** デバイス] フィールドは、製造業プロセスマネージャー アプリケーションが有効になっている場合にのみ自動入力されます。
- 製造業プロセスマネージャーがインストールされている場合、OT デバイスに割り当てられたサイトが [サイト] フィールドに表示されます。

- 製造業プロセスマネージャーが有効になっていて、OT デバイスに関連付けられているエンティティが 1 つしかない場合は、[機器モデルエンティティ] フィールドが自動的に入力されます。

注: 複数のエンティティがデバイスに関連付けられている場合、機器モデルエンティティフィールドは空のままになります。

結果

変更要求が作成され、[アサイン先グループ]、[アサイン先]、および [ウォッチリスト] フィールドのユーザーに通知されます。

修復タスクからの変更要求の作成

OT 修復タスクから オペレーショナルテクノロジー (OT) 変更要求を作成します。修復タスクから変更要求を作成すると、[サイト] フィールドや [OT デバイス] フィールドなどの変更要求レコードの情報が自動的に入力されます。

始める前に

必要なロール:sn_ot_change_write または sn_otvr.remediation_owner

手順

- 移動先 すべて > 産業用ワークスペース。
- 変更要求を作成する修復タスクレコードを開きます。
- 次の例に示すように、[**OT 変更を作成**] ボタンを選択しま

The screenshot displays the ServiceNow interface for a record titled 'California Vulnerabilities'. At the top right, there are buttons for 'Assign to me', 'Resolve task', 'Create OT Change' (highlighted), 'Save', and a menu icon. Below this, a table shows the record's status: State: Open, Risk rating: 3 - Medium, Assignment group: OT VR Default Ass..., Remediation status: In-flight, % VIs remediated: 0. The main content area is divided into two sections: 'Remediation Progress' on the left, showing a 0% progress bar, and 'Vulnerable Items' on the right, which contains a table with one item: VIT0010002. This item has a summary describing a remote code execution vulnerability in Microsoft Office components, a configuration item of PLC001, and a state of Open with a risk rating of 3 - Medium. The right sidebar, titled 'Attachments', indicates 'No Attachments Available' and provides a 'Browse' button. The bottom of the interface shows 'Showing 1-1 of 1' and '20 rows per page'.

す。

注: アクティブな変更モデルがない場合は、次のエラーが表示されま

す。

Error creating Change Request: No active change model available. Please contact your OT Change admin

- 組織に適用する OT 変更モデルを選択します。
- [Next (次へ)] をクリックします。
- チームが変更要求に取り組むように、必要に応じてプレイブックを完成させます。

基本的な OT 変更モデルプレイブックの詳細については、「[基本的な OT 変更モデルプレイブック](#)」を参照してください。高度な OT 変更モデルプレイブックの詳細については、「[高度な OT 変更モデルプレイブック](#)」を参照してください。

設定した条件に応じて、次のフィールドが自動的に入力されます。

- [**OT デバイス**] フィールドは、製造業プロセスマネージャー アプリケーションが有効になっている場合にのみ自動入力されます。
- 製造業プロセスマネージャーがインストールされている場合、OT デバイスに割り当てられたサイトが [**サイト**] フィールドに表示されます。
- 製造業プロセスマネージャーが有効になっていて、OT デバイスに関連付けられているエンティティが 1 つしかない場合は、[**機器モデルエンティティ**] フィールドが自動的に入力されます。

i 注: 複数のエンティティがデバイスに関連付けられている場合、機器モデルエンティティ フィールドは空のままになります。

インシデントレコードからの変更要求の作成

OT インシデントレコードから オペレーショナルテクノロジー (OT) 変更要求を作成します。インシデントレコードから直接変更要求を作成すると、データがインシデントレコードからの新しい変更要求に自動的にマッピングされます。

始める前に

必要なロール:sn_ot_incident_write、sn_ot_incident_admin、または sn_ot_change_write

手順

1. 移動先 **すべて > 産業用ワークスペース**.
2. [**OT インシデント**] リストモジュールで、利用可能なリストのいずれかを選択します。
3. OT 変更要求を作成するインシデントレコードを選択します。
4. [**OT 変更を作成**] ボタンを選択します。
[**OT 変更を選択 (Select OT change)**] フォームが開きます。
5. 組織に適用可能な変更モデルを選択します。
詳細については、「[変更要求を満たす変更モデルを選択](#)」を参照してください。
6. [**OT 変更レコードの作成**] を選択します。
7. 必要に応じて、プレイブックと関連フォームに入力します。

プレイブックと関連フォームの詳細については、「選択した OT 変更モデルに応じて [基本的な OT 変更モデルプレイブック](#) と [高度な OT 変更モデルプレイブック](#)」を参照してください。

i 注: 新しい変更要求の [詳細] 関連リストの次のフィールドと関連リストに、関連する OT インシデントレコードの値が自動的に入力されます。

- サイト
- 機器モデルエンティティ
- OT デバイス (CI)
- 簡単な説明
- 説明
- 優先度

i 注: 1 ~ 4 の [優先度] フィールドの値は、新しい変更レコードで同じです。ただし、インシデントレコードの [優先度] フィールドの値 5 は、新しい変更レコードでは 4 に変更されます。

変更レコードの関連デバイスと機器モデルエンティティを編集する

関連する オペレーショナルテクノロジー (OT) デバイスと機器モデルエンティティを OT 変更レコードから直接追加または削除します。変更要求とその影響を受けるアイテムとの関係を追跡できます。

始める前に

必要なロール:sn_ot_change_write または sn_ot_change_admin

手順

1. 移動先 **すべて > 産業用ワークスペース**.
2. 産業用 ワークスペースリストビューを開きます。
3. [OT 変更要求] リストモジュールで、利用可能なリストのいずれかを選択します。
4. 編集する変更レコードを選択します。
5. 関連する OT デバイスを追加または削除します。

アクション	説明
変更レコードから関連する OT デバイスを追加する	a. [影響を受ける OT デバイス] 関連リストを選択します。 b. [Add (追加)] を選択します。 c. [OT デバイスの追加 (Add OT Devices)] ウィンドウで、追加するデバイスの横にあるチェックボックスをオンにします。 d. [Add (追加)] を選択します。
変更レコードから関連する OT デバイスを削除する	a. [影響を受ける OT デバイス] 関連リストを選択します。 b. 削除するデバイスの横にあるチェックボックスをオンにします。

アクション	説明
	c. [削除] ボタンを選択します。 d. 表示される確認ウィンドウで、[削除] を選択します。

これで、OT デバイスが [影響を受ける OT デバイス] 関連リストの変更レコードに追加または削除されました。

6. [影響を受ける機器モデルエンティティ] 関連リストでステップ 4 と 5 を繰り返して、変更レコードに対して機器モデルエンティティを追加または削除します。

オペレーショナルテクノロジー 変更承認

オペレーショナルテクノロジー (OT) 変更承認を使用すると、レビュー担当者は要求された変更を承認し、必要に応じて改善を提案できます。

変更承認の概要

高度な OT 変更モデルを使用した OT 変更承認により、承認者は変更要求をレビューし、必要に応じて要求を編集して、変更要求を承認できます。

- i** 注: 変更承認は、高度な OT 変更モデルにのみ適用されます。基本 OT 変更モデルに変更承認ポリシーが適用されていません。

変更承認要件

要件	説明
サイトレベル	変更が行われるサイトまたはエリア。
サイト承認グループ	変更要求をレビューおよび承認できる承認グループにアサインされたメンバー。
必要なロール	承認者には sn_ot_change_read ロールが必要です。
承認率	承認グループの 51% が、先に進むために変更を承認する必要があります。

OT 変更承認フロー

OT 変更承認フローは次のとおりです。

1. 変更要求を作成します。
2. フローは変更モデルに基づいて呼び出されます。
3. フローにより、変更承認ポリシーが適用されます。
4. さまざまな意思決定レコードが評価されます。
5. 一致する承認定義が実行されます。
6. サイトレベルの承認者のリストを変更レコードに追加します。

高度な OT 変更モデルには、変更承認ポリシーが含まれています。独自の承認ポリシーを作成することもできます。承認ポリシーの作成方法の詳細については、「[変更承認ポリシーの作成](#)」を参照してください。

変更要求をレビューする承認者を追加する

グループメンバーまたは承認者を承認グループに手動で追加して、オペレーショナルテクノロジー (OT) 変更要求をレビューします。

始める前に

必要なロール：admin

手順

1. 移動先 **すべて > ユーザー管理 > グループ**.
2. [グループ] リストから、[**OT 変更のデフォルト承認者**] グループを選択します。
3. [グループメンバー] 関連リストを選択します。
4. [Edit (編集)] を選択します。
5. [コレクション] リストで、承認グループに追加するメンバーを選択します。
6. 中央矢印を使用して、選択したメンバーを [OT 変更のデフォルト承認者] リストに移動します。
7. [Save (保存)] を選択します。

結果

承認グループに新しいメンバーが追加されました。これで、承認グループが変更要求をレビューできるようになります。

高度な OT 変更モデルプレイブックで OT 変更要求の開始ステージと計画ステージを完了したら、承認ステージで承認を要求できます。承認グループのメンバーは、次のいずれかの方法を使用して、変更要求レコードを開いて 産業用ワークスペース で承認する必要があります。

- 変更要求レコードで、[承認者] タブを選択し、[ステータス] フィールドを [要求済み] から適切なオプションに変更します。
- [プレイブック] タブで、[承認] ステージを選択し、[ステータス] フィールドを [要求済み] から適切なオプションに変更します。

サイト間での変更要求の管理

オペレーショナルテクノロジー変更管理アプリケーションを使用して、自分のサイトまたは他のサイトに属する変更要求を表示、作成、または編集できます。他のサイトからの変更要求を表示することで、自分のサイトで同様の変更を実装できます。

サイト間の変更要求の概要

sn_ot_change_write ロールを持っている場合は、次のタスクを実行できます。

- 自分にアサインされた オペレーショナルテクノロジー (OT) 変更要求またはサイトに属する変更要求を表示および編集します。
- OT 変更要求を作成します。
- 他のサイトに属する OT 変更要求を表示します。

sn_ot_change_write ロールの主な利点は、サイト全体の変更を読み取り専用で表示できることです。サイトをまたいで他の変更を表示すると、サイトで同様の変更を実装するのに役立ちます。

- i** 注：編集できるのは、アクセス可能なサイトに属する OT 変更要求のみです。クロスサイト OT 変更要求の管理に必要な追加のロールの詳細については、次のセクションを参照してください。

sn_ot_change_write ロールに必要なその他の OT ロールと権限

次の表では、sn_ot_change_write ロールを持つユーザーが、サイトまたは任意のサイトの変更要求にアクセスするために必要な追加のロールについて説明します。

sn_ot_change_write ロールに必要なその他のロール

ロール	権限
cmdb_ot_isa_editorロールを持つ sn_ot_change_write	サイトの変更要求を作成および編集します。
cmdb_ot_isa_viewerロールを持つ sn_ot_change_write	サイトの変更要求を作成および編集します。
sn_ot_change_writeと cmdb_ot_isa_viewer_all	任意のサイトの変更要求を作成および編集します。
サイトロールのないsn_ot_change_write	任意のサイトの変更要求を表示します。

sn_ot_change_read ロールに必要なその他の OT ロールと権限

次の表では、sn_ot_change_read ロールを持つユーザーとして、サイトまたは任意のサイトの変更要求を表示するために必要な追加のロールと権限について説明します。

sn_ot_change_read ユーザーロールに必要なその他のロール

ロール	権限
cmdb_ot_isa_editorロールを持つ sn_ot_change_read	サイトの変更要求を表示します。
cmdb_ot_isa_viewerロールを持つ sn_ot_change_read	サイトの変更要求を表示します。
sn_ot_change_readとcmdb_ot_isa_viewer_all	任意のサイトの変更要求を表示します。
サイトロールのないsn_ot_change_read	任意のサイトの変更要求を表示します。

変更要求を表示または編集する場所

次の OT 変更要求リストは、産業用 ワークスペースのリストモジュールで利用できます。

- 自分にアサイン済み:次に移動して、アサインされた変更レコードを表示および編集します。 **OT** 変更要求 > 自分にアサイン済み.
- 自分のサイトに所属:サイトに属する変更レコードを表示および編集するには、次の場所に移動します。 **OT** 変更要求 > 自分のサイトに所属.
- に移動して、さまざまなサイトの既存の変更レコードを表示します。 **OT** 変更要求 > すべて.

サイト間での変更モデルレコードの可視化

オペレーショナルテクノロジー (OT) 変更ロールとサイトロールに応じて、自分のサイトまたは他のサイトの変更モデルレコードを表示、作成、または編集できます。

OT 変更モデルレコードへのロールとヴィジビリティの変更

次の表では、さまざまな OT 変更ユーザーが変更モデルレコードにアクセスするためのロールと権限について説明します。

sn_ot_change_writeルールを持つユーザーの権限

ルール	権限
cmdb_ot_isa_editor サイトルールを持つ sn_ot_change_write	レコードに変更モデルを使用します。
cmdb_ot_isa_viewer サイトルールを持つ sn_ot_change_write	レコードに変更モデルを使用します。
cmdb_ot_isa_viewer_all サイトルールを持つ sn_ot_change_write	レコードに変更モデルを使用します。
サイトルールのない sn_ot_change_write	変更モデルへのアクセス権がありません。

sn_ot_change_readルールを持つユーザーの権限

ルール	権限
cmdb_ot_isa_editor サイトルールを持つ sn_ot_change_read	変更モデルへのアクセス権がありません。
cmdb_ot_isa_viewer サイトルールを持つ sn_ot_change_read	変更モデルへのアクセス権がありません。
サイトルールのない sn_ot_change_read	変更モデルへのアクセス権がありません。
cmdb_ot_isa_viewer_all サイトルールを持つ sn_ot_change_read	変更モデルへのアクセス権がありません。

sn_ot_change_managerルールを持つユーザーの権限

ルール	権限
cmdb_ot_isa_editor サイトルールを持つ sn_ot_change_manager	- 任意のサイトの変更モデルを作成、編集、削除します。 - 変更モデルを任意のサイトにアサインします。 - サイトから変更モデルを削除します。
cmdb_ot_isa_viewer サイトルールを持つ sn_ot_change_manager	- 任意のサイトの変更モデルを作成、編集、削除します。 - 変更モデルを任意のサイトにアサインします。 - サイトから変更モデルを削除します。
サイトルールのない sn_ot_change_manager	サイトの変更モデルを表示または編集することはできません。どのサイトにも関連付けられていないベースシステムの変更モデルのみを表示できます。

sn_ot_change_adminルールを持っている場合は、変更モデルを使用して任意のサイトの変更要求を作成できます。

メール通知の変更

メール通知を使用して、オペレーショナルテクノロジー (OT) 変更要求または変更タスクが更新されたときにユーザーにアラートを送信します。

OT 変更要求と変更タスクの通知を次の表に示します。

OT 変更要求メール通知

名前	送信時	[Who receives it]	内容
自分に割り当てられた変更	[アサイン先] フィールドが変更され、空でない場合	変更をアサインしたユーザー	件名:<変更要求 #> 通知 Body (本文) : 簡単な説明:<簡単な説明> 変更要求を表示するには、ここをクリックしてください<変更要求の URL> サイト:<サイト名> OT デバイス:<OT デバイス> 機器モデルエンティティ:<機器モデルエンティティ> 説明:<説明>
自分のグループに割り当てられた変更	[アサイン先グループ] フィールドが変更され、空でない場合	アサイン先グループ	件名:<変更要求 #> がグループ <アサイン先グループ> にアサインされました。 Body (本文) : 簡単な説明:<簡単な説明> 変更要求を表示するには、ここをクリックしてください<変更要求の URL> サイト:<サイト名> OT デバイス:<OT デバイス> 機器モデルエンティティ:<機器モデルエンティティ>

OT 変更要求メール通知 (続く)

名前	送信時	[Who receives it]	内容
			説明:<説明>
コメントされた変更	変更要求にコメントが追加されたとき	• 要求者 • ウォッチリスト	件名:<変更要求 #> コメントが追加されました Body (本文): 簡単な説明:<簡単な説明> 変更要求を表示するには、ここをクリックしてください<変更要求の URL> コメント:<変更要求に追加されたコメント>
作業メモされた変更	変更要求に作業メモが追加されたとき。	• 作業メモリスト • アサイン先 • アサイン先グループ	件名:<変更要求 #> 作業メモが追加されました Body (本文): 簡単な説明:<簡単な説明> 変更要求を表示するには、ここをクリックしてください:<変更要求の URL> 作業メモ:<変更要求に追加された作業メモ>
承認された変更	変更要求が承認されたとき	• アサイン先 • アサイン先グループ	件名:<変更要求 #> が承認されました Body (本文): 簡単な説明:<簡単な説明> <変更要求の URL>を表示するには、ここをクリックしてください 説明:<説明>
却下された変更	変更要求が却下されたとき	• アサイン先 • アサイン先グループ	件名:<変更要求 #> は却下されました Body (本文):

OT 変更要求メール通知 (続く)

名前	送信時	[Who receives it]	内容
			簡単な説明:<簡単な説明> <変更要求の URL>を表示するには、ここをクリックしてください 説明:<説明>
保留中の変更	変更要求が保留になっているとき	要求者	件名:<変更要求 #> が保留になりました Body (本文): こんにちは <変更要求を作成したユーザー>、 要求した<変更要求 #> は保留中です。要求が保留される理由:<変更要求が保留される理由> 変更要求を表示するには、ここをクリックしてください:<変更要求のURL>
保留解除の変更	変更要求が保留になったとき	要求者	件名:<変更要求 #> が保留解除されました Body (本文): こんにちは <変更要求を作成したユーザー>、 要求した <変更要求 #> は保留解除され、<更新済みステータスフィールド>ステータスになっています。 変更要求を表示するには、ここをクリックしてください:<変更要求のURL>

自動翻訳

OT 変更タスクのメール通知

名前	送信時	[Who receives it]	内容
自分にアサインされた変更タスク	[アサイン先] フィールドが変更され、空でない場合	変更タスクにアサインされた人物	件名:<変更タスク #> 通知 -- <簡単な説明> Body (本文):

OT 変更タスクのメール通知 (続く)

名前	送信時	[Who receives it]	内容
			簡単な説明:<簡単な説明> 変更タスクを表示するには、ここをクリックしてください:<変更タスクへの URL> サイト:<サイト名> OT デバイス:<OT デバイス> 機器モデルエンティティ:<機器モデルエンティティ> 説明:<説明>
自分のグループにアサインされた変更タスク	[アサイン先グループ] フィールドが変更され、空でない場合	アサイン先グループ	件名: 件名: <変更タスク #> 通知 -- <簡単な説明> Body (本文): 簡単な説明:<簡単な説明> 変更タスクを表示するには、ここをクリックしてください:<変更タスクへの URL> サイト:<サイト名> OT デバイス:<OT デバイス> 機器モデルエンティティ:<機器モデルエンティティ> 説明:<説明>
作業メモされた変更タスク	変更タスクに作業メモが追加されたとき	- 作業メモリスト - アサイン先 - アサイン先グループ	件名:<変更タスク #> 作業メモが追加されました -- <簡単な説明> Body (本文): 簡単な説明:<簡単な説明> 変更タスクを表示するには、ここをクリック

OT 変更タスクのメール通知 (続く)

名前	送信時	[Who receives it]	内容
			してください:<変更タスクへの URL> 作業メモ:<変更タスクに追加された作業メモ>

オペレーショナルテクノロジー変更管理の参照

参照トピックには、オペレーショナルテクノロジー変更管理 アプリケーションに関する追加情報が記載されています。

変更カテゴリ

オペレーショナルテクノロジー (OT) 変更要求を分類することで、特定の OT 変更要求をグループ化して検索を絞り込むことができます。カテゴリは、ステークホルダーが変更の内容を把握するためにも役立ちます。

OT 変更要求を作成できる場合は、次の表に示すカテゴリから選択できます。

OT 変更要求カテゴリ

カテゴリ	説明
ハードウェア	OT デバイスを追加、削除、または設定するための変更。
ソフトウェア	OT ソフトウェアを追加、削除、または構成するための変更。
サービス	OT サービスへの変更。
システムソフトウェア	OT システムソフトウェアへの変更。
アプリケーションソフトウェア	OT アプリケーションソフトウェアへの変更。
ネットワーク	サブネット、IP アドレス、および MAC アドレスに対する変更。
通信事業	OT システムで使用される電気通信の変更。
ドキュメント	OT ドキュメントの変更。
ファームウェア	OT ファームウェアの変更。
その他	その他の変更は、上記のカテゴリには含まれていません。

オペレーショナルテクノロジー変更管理とともにインストールされるコンポーネント

いくつかのタイプのコンポーネント (ユーザーロールなど) を、オペレーショナルテクノロジー変更管理 (sn_ot_chg_mgmt) アプリケーションのアクティブ化とともにインストールできます。

- i** 注: アプリケーションファイルテーブルには、このアプリケーションとともにインストールされたコンポーネントがリストされています。このテーブルへのアクセス手順については、「[アプリケーションとともにインストールされているコンポーネントの検索](#)」を参照してください。

インストールされるロール

ロール	説明	含まれるロール
変更マネージャー [sn_ot_change_manager]	OT 変更モデルレコードを管理できます。	- sn_ot_change_write - sn_sttrm_condition_read
変更アドミン [sn_ot_change_admin]	OT 変更レコードを作成、表示、削除、編集できます。カテゴリとシステムプロパティを設定できます。	- cmdb_ot_isa_viewer_all - sn_ot_change_write
変更書き込みユーザー [sn_ot_change_write]	OT 変更レコードを作成、表示、編集できます。 IT 変更タスクをアサインし、アサインされた IT 変更タスクを編集してクローズすることもできます。 詳細については、「サイト間での変更要求の管理」を参照してください。	- cmdb_ot_viewer - cmdb_ot_isa_viewer - sn_ot_change_read
変更読み取りユーザー [sn_ot_change_read]	OT 変更レコードの表示のみできます。	- cmdb_ot_viewer - cmdb_ot_isa_viewer

関連情報

OT 拡張クラスと関連アプリケーションの詳細を確認してください。

拡張クラスの概要

拡張クラスは、オペレーショナルテクノロジー管理が構成管理データベース (CMDB) でどのように機能するかを理解するのに役立ちます。

オペレーショナルテクノロジー (OT) 拡張クラス

構成管理データベース (CMDB) は OT のクラスを更新します。

関連アプリケーション

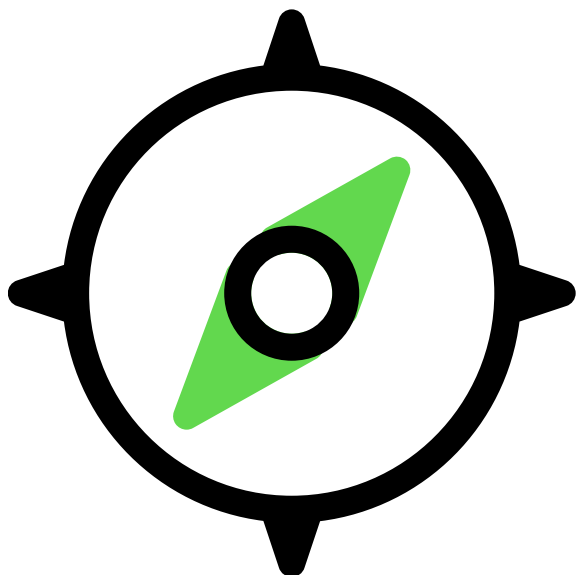
IT Service Management

ServiceNow IT Service Management アプリケーションをオペレーショナルテクノロジー変更管理と統合すると、エンジニアは OT デバイスと本番プロセスの問題を迅速に解決できます。

オペレーショナルテクノロジーのナレッジ管理

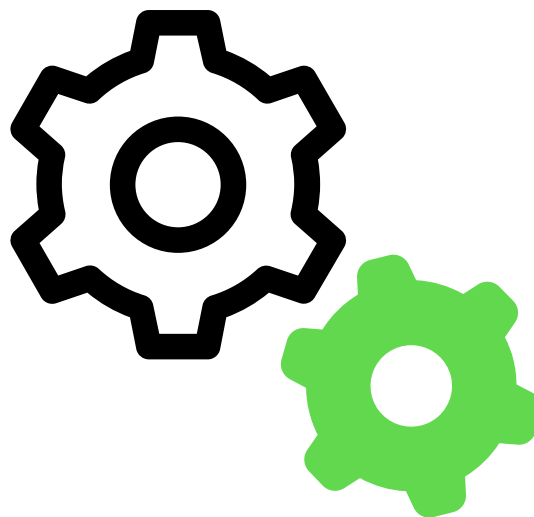
ServiceNow[®] オペレーショナルテクノロジーのナレッジ管理 は、オペレーショナルテクノロジー (OT) システム、そのデバイス、および組織内の解決済みインシデントに関するナレッジを収集、整理、および共有するのに役立ちます。

探索



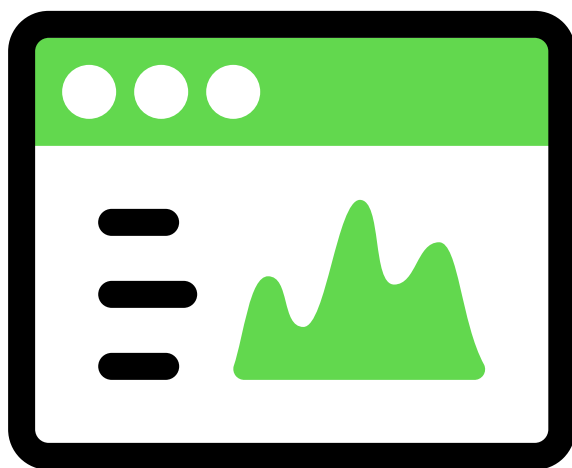
オペレーショナルテクノロジーのナレッジ管理 の探索

構成



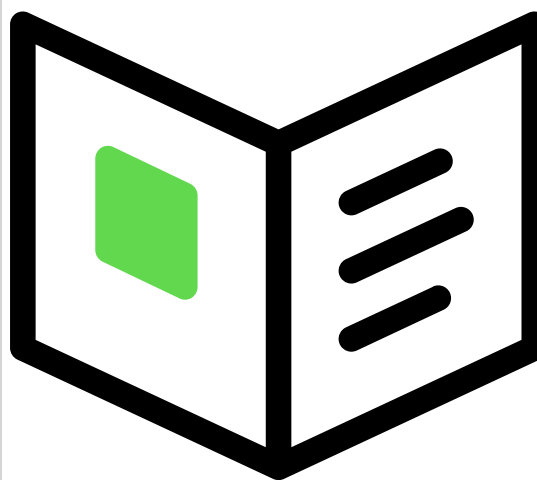
実装の計画と構成

使用方法



オペレーショナルテクノロジーのナレッジ管理 の使用

参照



関連情報とアプリケーションの詳細を取得

自動翻訳

オペレーショナルテクノロジーのナレッジ管理の探索

オペレーショナルテクノロジーのナレッジ管理 は、OT インシデントに関連するナレッジ記事で オペレーショナルテクノロジー (OT) システムに関する情報をキャプチャするのに役立ちます。組織は、これらのナレッジ記事を使用して、ユーザーが適切な情報にアクセスできるようにし、ユーザーとの誤解を防ぐことができます。

オペレーショナルテクノロジーのナレッジ管理の概要

オペレーショナルテクノロジーのナレッジ管理の詳細については、Operational Technology Service Management製品スイートの概要をご覧ください。

[https://player.vimeo.com/video/1019801515?](https://player.vimeo.com/video/1019801515?badge=0&autoplay=0&player_id=0&app_id=58479)

[badge=0&autoplay=0&player_id=0&app_id=58479](https://player.vimeo.com/video/1019801515?badge=0&autoplay=0&player_id=0&app_id=58479)

オペレーショナルテクノロジーのナレッジ管理のメリット

オペレーショナルテクノロジーのナレッジ管理では、次の主要な機能を使用できます。

- オペレーショナルテクノロジー管理ソリューションで既存のナレッジ管理 ServiceNow AI Platform 機能を使用する機能。
- OT インシデントに関連するすべてのナレッジベース記事を参照し、インシデントレコードから直接ナレッジ記事を作成する機能。
- ナレッジマネージャーとナレッジユーザーの OT ナレッジベースを構成する機能。
- 産業用 ワークスペースでナレッジ記事を作成する機能。
- ナレッジ記事の公開、編集、廃止、または削除の承認を要求する機能。
- 更新された情報を使用して既存のナレッジ記事を編集する機能。

オペレーショナルテクノロジーのナレッジ管理の構成

オペレーショナルテクノロジー (OT) ソリューションのデータ基盤を作成できるようにオペレーショナルテクノロジーのナレッジ管理を構成します。

admin ロールを持っている場合は、ガイド付きセットアップを使用して オペレーショナルテクノロジーのナレッジ管理のセットアップをガイドできます。ガイド付きセットアップ は、アプリケーションの構成を支援するツールです。構成アクティビティをカテゴリに整理します。これらのカテゴリには、セットアップタスクに関する情報、各タスクを完了するための手順、および構成を実行するインスタンス内のページへのリンクが含まれています。役立つヘルプコンテンツへのリンクも提供されます。

ガイド付きセットアップにアクセスするには、に移動します 産業用ワークスペースアドミン > ガイド付きセットアップ。

次の表に、ガイド付きセットアップ タスクとその オペレーショナルテクノロジーのナレッジ管理の目的を示します。

- i 注:** オペレーショナルテクノロジーのナレッジ管理はオペレーショナルテクノロジーインシデント管理アプリケーションに入っています。オペレーショナルテクノロジーインシデント管理アプリケーション (バージョン 2.0.2) をインストールして構成していれば、オペレーショナルテクノロジーのナレッジ管理を構成できます。追加で必要なロールはありません。

次の表は、セットアップと構成を正しく行うためにユーザーが完了する必要があるタスクを示しています。

オペレーショナルテクノロジーのナレッジ管理セットアップタスク

タスク	目的
ナレッジ管理ロールをオペレーショナルテクノロジーのナレッジ管理に割り当てます。	各ユーザーが使用できるアクションを制御するロールを割り当てます。
OT ナレッジベースを作成します。	OT ナレッジベースを構成して、マネージャーを追加し、アクセスを設定します。
OT ナレッジベースに適用するユーザー基準を作成します。	ユーザー基準レコードを作成して、OT ナレッジベースを閲覧または寄稿できるユーザーを決定します。
OT ナレッジベースにユーザー基準をアサインします。	ユーザー基準レコードを OT ナレッジベースにアサインし、ナレッジベース内のナレッジ記事を作成、読み取り、書き込み、廃止できるユーザーを制御します。
非認証ユーザーの OT ナレッジベースへのアクセスを構成します。	非認証ユーザーがアクセスできる OT ナレッジベースを確認します。アクセス権は、ユーザー基準と glide.knowman.block_access_with_no_user_criteria プロパティ設定に基づきます。
ナレッジワークフローを OT ナレッジベースに割り当てます。	公開および廃止プロセス用に、さまざまなナレッジワークフローを各 OT ナレッジベースにアサインします。
[オペレーショナルテクノロジーのナレッジ管理] に使用されるナレッジ管理プロパティを確認します。	該当する ナレッジ管理 プロパティを使用して、OT ナレッジベースの外観と機能を構成します。

オペレーショナルテクノロジーのナレッジ管理ユーザーへのロールのアサイン

ナレッジ管理ロールをユーザーにアサインして、オペレーショナルテクノロジーのナレッジ管理の機能とデータへのアクセス権を制御できるようにします。

始める前に

必要なロール：admin

このタスクについて

ナレッジ管理ロールがアサインされている場合は、オペレーショナルテクノロジーのナレッジ管理機能を使用できます。

- i** 注：ユーザー基準によってナレッジ記事へのアクセスが決定されます。詳細については、「[ナレッジベースとナレッジ記事へのアクセスの管理](#)」を参照してください。

オペレーショナルテクノロジーのナレッジ管理に適用できるナレッジ管理ロールの詳細については、「[オペレーショナルテクノロジーのナレッジ管理 ロール](#)」を参照してください。

手順

ServiceNow AI Platform ユーザー管理機能を使用して、ユーザーとグループにロールをアサインします。

タスク	ユーザー管理機能
ユーザーへのロールのアサイン	ユーザーへのロールの割り当て を参照してください。
グループへのロールのアサイン	グループへのロールのアサイン を参照してください。

OT ナレッジベースの作成

オペレーショナルテクノロジー (OT) ナレッジベースを作成し、OT ナレッジユーザーが OT インシデントに関連するコンテンツを保存、共有、および管理するためのセルフサービスプラットフォームを提供します。

始める前に

必要なロール：admin

手順

1. 移動先 ナレッジ > アドミニストレーション > ナレッジベース。
2. **[New (新規)]** を選択します。
3. ナレッジベースフォームのフィールドに入力します。
フィールド値の説明については、「[ナレッジベース フォーム](#)」を参照してください。
4. フォームヘッダーを右クリックし、**[保存]** を選択します。
5. 関連リストセクションで、OT ナレッジベースに関連する次の表のアイテムを表示または設定します。

名前	説明
ナレッジ	このナレッジベースに保存されているナレッジ記事のリスト。
読み込み可能	読み取りアクセス権を付与し、基準に一致するユーザーが OT ナレッジベースの記事を読めるようにするユーザー基準のリスト。
寄稿可能	貢献者アクセス権を付与し、基準に一致するユーザーが OT ナレッジベースの記事を作成および変更できるようにするユーザー基準のリスト。
記事テンプレート	ナレッジ管理 Advanced (com.snc.knowledge_advanced) プラグインを有効にしている場合は、[記事テンプレート] 関連リストが表示されます。 記事テンプレートが関連リストにある場合、そのナレッジベースの記事は、リストされている記事テンプレートの 1 つを使用してのみ作成できます。 [記事テンプレート] 関連リストが空の場合、任意の記事テンプレートを使用して記事を作成できます。 [編集] を選択して、記事テンプレートをナレッジベースにマッピングします。

名前	説明
	i 注: アドミン、ナレッジアドミニストレーター、およびナレッジマネージャーは、ナレッジベースの記事テンプレートを編集できます。
ナレッジ カテゴリ	OT ナレッジベースに関連付けられているナレッジカテゴリのリスト。 i 注: カテゴリが非アクティブとしてマークされている場合、記事をカテゴリに関連付けることはできません。ただし、そのカテゴリの既存の記事には影響しません。

6. [Submit (送信)] を選択します。

OT ナレッジベースのユーザー基準の作成

ユーザー基準レコードを作成して、オペレーショナルテクノロジー (OT) ナレッジベースを閲覧または寄稿できるユーザーを決定します。

始める前に

必要なロール: user_criteria_admin

- i** 注: ナレッジモジュールからユーザー基準レコードを作成するには、knowledge ロールに加えて user_criteria_admin ロールが必要です。アクセスの詳細については、「[ナレッジベースとナレッジ記事へのアクセスの管理](#)」を参照してください。

このタスクについて

ナレッジ管理のユーザー基準を使用して、特定のユーザーが OT ナレッジベースとナレッジ記事にアクセスできるかどうかを判断します。ユーザー基準レコードを作成したら、それを OT ナレッジベースにアサインして、ナレッジベースとその記事を読んだり寄稿したりできるユーザーを制御できます。さらに、記事レベルでユーザー基準をアサインして、それを読むことができるユーザーを制御できます。

手順

1. 移動先 **すべて > ナレッジ > アドミニストレーション > ユーザー基準**.
2. **[New (新規)]** を選択します。
3. フォームで、フィールドに入力します。

[ユーザー基準] フォーム

フィールド	説明
名前	ユーザー基準の一意の名前。
ユーザー	ユーザー基準に一致する必要があるユーザー。
グループ	ユーザー基準に一致する必要があるグループ。

フィールド	説明
ルール	ユーザー基準に一致するルール。 i 注: - ルールの評価はセッションでキャッシュされるため、ルールを変更すると再度ログインする必要があります。 - ユーザー基準は、昇格された特権ルールに適用できません。
詳細	ユーザー基準フォームの [スクリプト] フィールドを含む詳細オプションを表示または非表示にするオプション。
スクリプト	true または false を返す追加のユーザー基準を定義するスクリプト。このフィールドは、[ユーザー基準] フォームで [詳細] オプションが選択されている場合に使用できます。 i 注: - スクリプトは、ユーザー基準が作成された範囲内で評価されます。 - スクリプトの評価はセッションにキャッシュされるため、評価を変更するには、再ログインする必要があります。スクリプト化されたユーザー基準がナレッジベースに対して定義されている場合、ナレッジベースへのユーザーアクセスは各セッションの後に評価されます。セッションキャッシュのビルド後にスクリプトによって変更が生じた場合、その変更は次のセッションで有効になります。 <code>gs.getUser()</code> またはその他のセッション API は診断ツールで使用する競合が発生するため、使用しないでください。スクリプトで利用可能な事前定義済みの <code>user_id</code> 変数を使用して、スクリプトを評価するために使用されているユーザーのユーザー ID を取得します。 - スクリプトは動的に評価されます。したがって、ユーザー基準にスクリプトを含めると、システムのパフォーマンスに影響を与える可能性があります。
アクティブ	ユーザー基準をアクティブ化/非アクティブ化するオプション。
会社	ユーザーレコードが一致する必要がある会社。
ロケーション	ユーザーレコードが一致する必要がある場所。
部門	ユーザーレコードが一致する必要がある部門。
すべて一致	入力された各ユーザー基準フィールドのすべての要素が一致する必要があるかどうかを判断するためのオプション。選択した場合、すべてのユーザー基準に一致するユーザーのみにアクセス権が付与されます。オフにした場合、ユーザーは、アクセス権が付与される 1 つ以上のユーザー基準のセットを満たす必要があります。 デフォルトでは、このチェックボックスはオフになっているため、いずれかの条件を満たせばアクセスできます。 たとえば、次の条件のユーザー基準レコードを考えてみましょう。 - 場所 A または B - 会社 C または D

フィールド	説明
	[すべて一致] を選択すると、次の条件をすべて満たすユーザーのみが照合されます。たとえば、場所 A および会社 C に所属するユーザーです。 [すべて一致] が選択されていない場合、これらの条件のいずれかを満たすユーザーが一致します。たとえば、場所 B のユーザー。 i 注: [すべて一致] を選択する場合は、決して満たされない矛盾した条件を作成しないようにしてください。たとえば、場所 A のすべてのユーザーが会社 G に対して作業している場合、この例の条件は決して満たせません。

4. [Submit (送信)] を選択します。

次のタスク

これで、ユーザー基準を OT ナレッジベースにアサインできます。詳細については、「[OT ナレッジベースへのユーザー基準のアサイン](#)」を参照してください。

OT ナレッジベースへのユーザー基準のアサイン

ユーザー基準レコードを オペレーショナルテクノロジー (OT) ナレッジベースにアサインし、ナレッジベース内のナレッジ記事を作成、読み取り、書き込み、および廃止できるユーザーを制御します。

始める前に

必要なロール: knowledge_manager、knowledge_admin、または admin

このタスクについて

ユーザー基準を OT ナレッジベースにアサインして、読み取りアクセスまたは寄稿アクセスを制御できます。

手順

1. 移動先 [すべて > ナレッジ > アドミニストレーション > ナレッジベース](#)。
2. 管理する OT ナレッジベースレコードを選択します。
3. OT ナレッジベースにユーザー基準を追加します。
 - a. 設定するユーザー基準に応じて、1 つ以上の関連リストを選択します。

関連リスト	説明
読込可能	ユーザーはナレッジベースにあるナレッジ記事を読むことができます。
読込不可	ユーザーはナレッジベースにあるナレッジ記事を読むことができません。
寄稿可能	ユーザーはナレッジベースにあるナレッジ記事を作成、変更、廃止できます。ナレッジベースへの寄稿アクセス権は、ナレッジベースのすべての記事への読み取りアクセス権も提供します。
寄稿不可	ユーザーはナレッジベースにあるナレッジ記事を作成、変更、廃止または読み取りできません。

b. 選択した関連リストで、必要なユーザー基準を追加します。

- admin ロールを持つユーザーとして、[新規] を選択し、必須フィールドを指定して [送信] を選択し、新しいユーザー基準レコードを追加します。
- knowledge_manager、knowledge_admin、または admin ロールを持つユーザーは、編集を選択し、必要なユーザー基準を コレクション 列から ナレッジ 列に移動して 保存 を選択し、既存のユーザー基準レコードを追加します。

4. ナレッジベースフォームで、[更新] を選択します。

非認証ユーザーの OT ナレッジベースへのアクセスを確認します

ユーザー基準と `glide.knowman.block_access_with_no_user_criteria` プロパティ設定を使用して、非認証ユーザーがアクセスできるオペレーショナルテクノロジー (OT) ナレッジベースを確認します。

始める前に

必要なロール: knowledge_admin または admin

このタスクについて

ナレッジベースの非認証ユーザーを制限する場合は、ユーザー基準または `glide.knowman.block_access_with_no_user_criteria` プロパティ設定を使用できます。

手順

1. 移動先 **すべて > ナレッジ > アドミニストレーション > ナレッジベース**。
2. 非認証ユーザーがアクセスできる OT ナレッジベースを確認します。
3. オプション: ユーザー基準を使用してナレッジベースの非認証ユーザーを制限するには、ナレッジベースレコードを選択し、そのユーザー基準を更新します。
ユーザー基準の作成の詳細については、「[OT ナレッジベースのユーザー基準の作成](#)」を参照してください。ユーザー基準の割り当ての詳細については、「[OT ナレッジベースへのユーザー基準のアサイン](#)」を参照してください。
4. オプション: `glide.knowman.block_access_with_no_user_criteria` プロパティ設定を使用して、ナレッジベースの非認証ユーザーを制限します。
 - a. 移動先 **すべて > ナレッジ > アドミニストレーション > プロパティ**。
 - b. `glide.knowman.block_access_with_no_user_criteria` プロパティの設定を `true` に設定します。
 - c. **[Save (保存)]** を選択します。

ナレッジワークフローの OT ナレッジベースへのアサイン

公開および廃止プロセスの各オペレーショナルテクノロジー (OT) ナレッジベースに異なるナレッジ管理ワークフローをアサインできます。

ナレッジワークフローの概要

次の表のデフォルトの ナレッジ管理 ワークフローを オペレーショナルテクノロジーのナレッジ管理に使用して、OT ナレッジベースに適用できます。

- i** 注: 承認が必要なワークフローの場合、KBWorkflow スクリプトインクルードで `getApprovers()` 機能を編集することによって、どのユーザーが承認または廃止を行うことができるかを設定できます。

デフォルトのナレッジ管理 ワークフロー

ワークフロー	説明
ナレッジ - 公開承認	ナレッジベースのマネージャーに承認を要求します。承認中の記事のステータスは、承認後に [公開] ステータスに移行する前は [レビュー中] です。後で公開するように設定されている場合は、[スケジュール済み] ステータスに移行します。マネージャーが要求を却下した場合、ワークフローはキャンセルされ、記事は [ドラフト] ステータスのままになります。 所有グループオプションが有効になっている場合、記事へのリンクを含むメール通知が所有グループのメンバーに送信され、承認されます。 所有グループオプションが有効になっていない場合、記事へのリンクを含むメール通知がナレッジベースアドミニストレーターに送信され、承認されます。 記事が承認または却下されたことを知らせるために、記事の作成者または改訂者にも通知が送信されます。 承認メール通知をオンにするには、<code>glide.knowman.enable_approval_notifications</code> プロパティを true に設定します。 i 注: アクティブなユーザーのみが通知を受け取ります。
ナレッジ - 廃止承認	記事を廃止ステータスに移行する前に、ナレッジベースのマネージャーからの承認を要求します。いずれかのマネージャーが要求を却下した場合、ワークフローはキャンセルされ、記事は [公開] ステータスのままになります。 所有グループオプションが有効になっている場合、記事へのリンクを含むメール通知が所有グループのメンバーに送信され、承認されます。 所有グループオプションが有効になっていない場合、記事へのリンクを含むメール通知がナレッジベースアドミニストレーターに送信され、承認されます。
ナレッジ - すぐに公開	承認を必要とせずにドラフト記事を即時公開するか、後で公開するように設定されている場合は公開予定日に公開します。
ナレッジ - すぐ廃止	承認を要求せずに公開記事をすぐに廃止します。

デフォルトのナレッジ管理 ワークフロー (続く)

ワークフロー	説明
ナレッジ - ナレッジの公開	ナレッジ記事を [公開] ステータスに移行するサブフロー。独自のワークフローを定義している場合にこのサブフローを使用できます。
ナレッジ - ナレッジの廃止	ナレッジ記事を [廃止] ステータスに移行するサブフロー。独自のワークフローを定義している場合にこのサブフローを使用できます。

承認ワークフローのメール通知

承認ワークフローのメール通知を送信できます。

- 承認のために送信されたナレッジ記事について承認者に通知します。
- ナレッジ記事の承認ステータスを作成者に通知します

承認ワークフローのメール通知を送信するには、[記事承認ワークフロー内の承認者と作成者に通知を送信する] プロパティ (*glide.knowman.enable_approval_notification*) を有効にします。New York リリース以降、このプロパティはデフォルトで有効になっています。New York リリースより前のリリースバージョンをお持ちの既存のお客様は、このプロパティを有効にしてメール通知を送信できます。このプロパティを有効にする前に、記事承認のカスタム通知を無効にします。*glide.knowman.enable_approval_notification* プロパティが利用できない場合、アドミニストレーターはプロパティを作成し、その値を true に設定できます。詳細については、「[ナレッジ管理のプロパティ](#)」を参照してください。

オペレーショナルテクノロジーナレッジベースのナレッジ管理プロパティの確認

アドミニストレーターは、オペレーショナルテクノロジー (OT) ナレッジベースの外観と機能を ナレッジ管理 プロパティで設定できます。

ナレッジ管理プロパティにアクセスするには、次に移動します: **すべて > ナレッジ > アドミニストレーション > プロパティ**。

次のテーブルにリストされているプロパティを使用して、ナレッジベースの不完全または不正確な記事にフラグを設定できるロールを制御します。

Glide.knowman.show_flag.roles プロパティ

プロパティ	説明
不完全/不正確な記事にフラグを設定できるロールのリスト (カンマ区切り形式) (<i>glide.knowman.show_flag.roles</i>)	ロール名を [表示] どおりに正確に入力します ユーザー管理 > ロール. [記事の評価セクションを表示] プロパティと [「記事にフラグ設定」オプションを表示] プロパティの両方が選択されている場合、このプロパティにリストされているロールを持つユーザーには、記事ビューで [記事にフラグ設定] オプションが表示されます。 このプロパティにリストされているロールも、すべて [記事の評価セクションを表示] できるロールのリスト] プロパティにリストされている必要があります。

その他の利用可能な ナレッジ管理 プロパティの詳細については、「[ナレッジ管理のプロパティ](#)」を参照してください。

オペレーショナルテクノロジーのナレッジ管理の使用

オペレーショナルテクノロジーのナレッジ管理に必要なセットアップタスクをすべて完了したら、オペレーショナルテクノロジー (OT) インシデントに関連するナレッジ記事の管理を開始できます。

オペレーショナルテクノロジーのナレッジ管理の概要

オペレーショナルテクノロジーのナレッジ管理を使用すると、チームのニーズに応じてナレッジ記事を作成、編集、および廃止できます。オペレーショナルテクノロジーインシデント管理 アプリケーションと併用すると、インシデントに関連する記事を参照したり、インシデントから記事を作成したりすることができます。

次の例は、チームに オペレーショナルテクノロジーのナレッジ管理 を適用する方法を示しています。

- 数年の経験を持つ OT エンジニアは、ガイドワーカーと若手技術者のために、OT デバイスの知識を 1 か所に集約したいと考えています。
- 生産プロセスオペレーションを担当する最前線の作業者と技術者は、工場フロアの問題に気づき、修復について説明するナレッジ記事を必要としています。

基本的な オペレーショナルテクノロジーのナレッジ管理 プロセス

次の ワークフロー では、オペレーショナルテクノロジーのナレッジ管理の基本的なプロセスについて説明します。

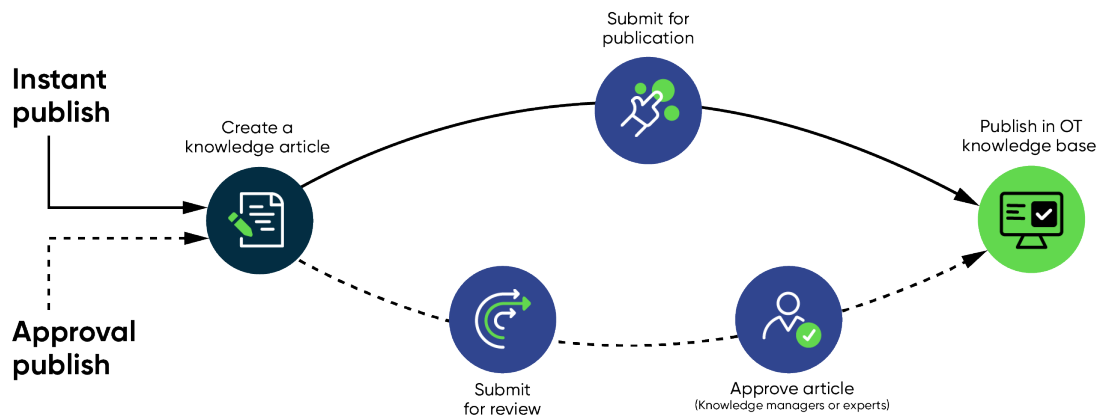
基本的な OT ナレッジワークフロー



ナレッジ記事の公開

次の ワークフロー では、ナレッジ記事の作成方法と公開方法を、承認あり (承認、公開)、承認なし (すぐに公開) の両方で説明します。

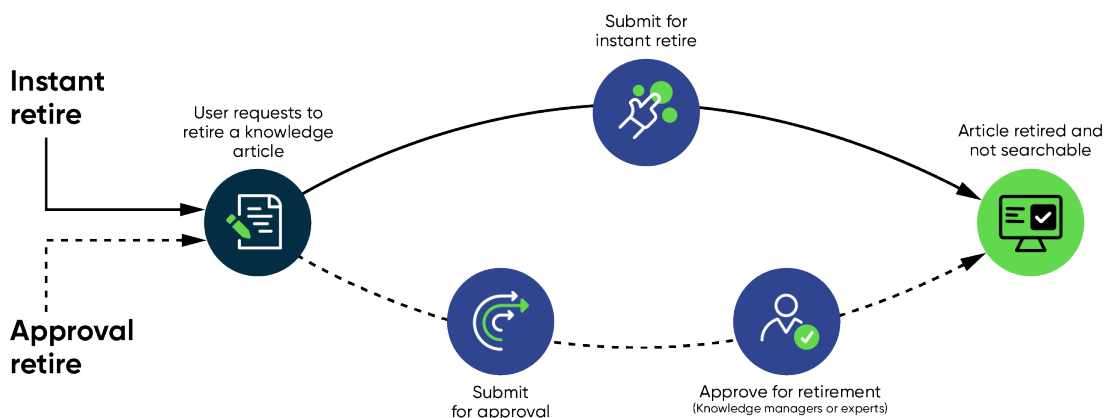
公開用ワークフロー



ナレッジ記事を廃止する

次の ワークフロー では、ナレッジ記事を承認あり (廃止承認) と承認なし (すぐに廃止) の両方で廃止する方法について説明します。すぐに廃止ワークフローを使用すると、承認を必要とせずに記事をすぐに廃止できます。廃止承認ワークフローは、ナレッジマネージャーまたはエキスパートに承認要求を送信して、記事の廃止が必要であることを確認します。

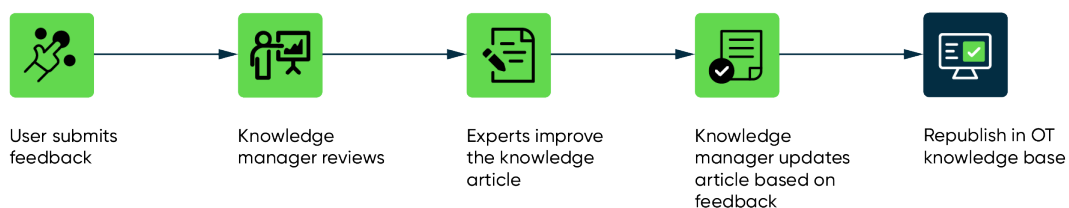
廃止用ワークフロー



ナレッジ記事の変更のレビューと承認

次の ワークフロー では、既存のナレッジ記事をユーザーフィードバックで更新する方法について説明します。

ユーザーフィードバックワークフロー



ナレッジ記事

ナレッジ記事は、職場の最新情報、セルフヘルプ、トラブルシューティング手順、および OT チームがアクセスする必要があるその他の情報を提供します。たとえば、次のケースに対して次のナレッジ記事を作成できます。

- 組織全体で使用される標準運用手順テンプレート。
- インシデント中に学んだ教訓。
- さまざまな生産資材に注釈を付ける画像。

産業用 ワークスペースナレッジ記事は、次の方法で表示できます。

- 産業用 ワークスペースリストビューのナレッジモジュールの下。
- OT インシデントを開いたときの [エージェントアシスト] ウィンドウ内。
- 産業用 ワークスペースヘッダーでのグローバル検索機能の使用

産業用 ワークスペースリストビューのナレッジモジュールでは、次のリストのナレッジ記事を表示できます。

- ❗ **注:** これらのリストモジュールを 産業用 ワークスペースに表示するには、ナレッジロールが割り当てられている必要があります。

未公開記事

作成したが、OT ナレッジベースにまだ公開されていない記事。

公開済みの記事

作成した、OT ナレッジベースに公開されている記事。

すべての記事

OT ナレッジベースで利用可能なすべての記事。

OT インシデントレコードからのナレッジ記事の作成

オペレーショナルテクノロジー (OT) インシデントとその解決に関連する情報を記録および保存するためのナレッジ記事を作成します。

始める前に

必要なロール:sn_ot_incident_write

- ❗ **注:** また、少なくとも 1 つのナレッジベースへの 寄稿可能 アクセスも必要です。詳細については、「[OT ナレッジベースの作成](#)」を参照してください。

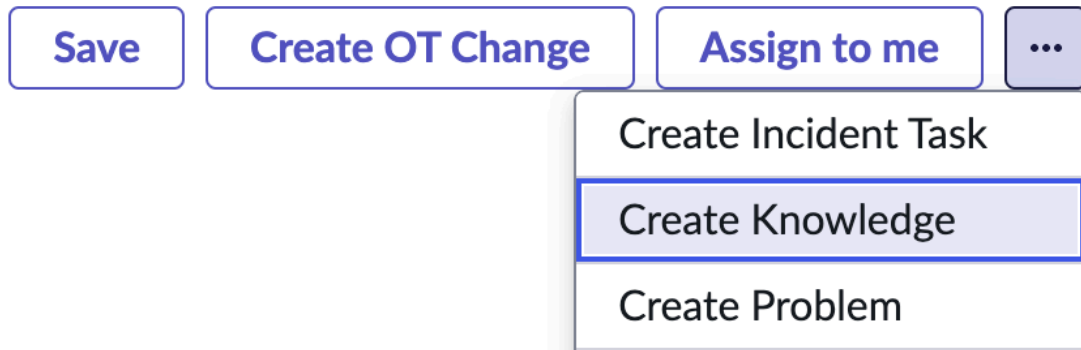
このタスクについて

インシデントレコードから直接ナレッジ記事を作成すると、ナレッジ記事がコンテキスト情報の正しいインシデントにリンクされていることを確認できます。ナレッジ記事には、適切な手順、課題、およびソリューションが含まれている場合に、チームが将来同様のインシデントを解決するのに役立ちます。

手順

1. 移動先 **すべて** > 産業用ワークスペース。
2. リストビューの [OT インシデント] モジュールで、利用可能なリストのいずれかを開きます。
3. ナレッジ記事を作成する OT インシデントレコードを選択します。
4. [その他のアクション] ...) を選択して、メニューを展開します。

5. [ナレッジを作成] を選択しま



す。

- i** 注: [ナレッジを作成] ボタンを表示するには、インシデントレコードのステータスを [解決済み] に設定する必要があります。

6. フォームで、フィールドに入力します。

ナレッジ記事フォーム

フィールド	説明
ナレッジベース	ナレッジ記事を含めるナレッジベース。 i 注: OT ナレッジベースの可視化が正しく構成されている場合、OT ユーザーはこの参照リストでナレッジベースを見つけることができます。
カテゴリ	ナレッジ記事の分類。
簡単な説明	ナレッジ記事のタイトルとして使用されるインシデント解決の簡単な説明。
記事本文	インシデントの手順、課題、およびソリューションを説明するナレッジ記事のコンテンツ。
有効期間終了日	ナレッジ記事の有効期限。

7. [Save (保存)] を選択します。

ナレッジ記事がドラフトとして保存され、親 OT インシデントに添付されます。

8. [Publish (公開)] を選択します。

結果

ナレッジ記事が OT ナレッジベースに公開されました。ナレッジ記事を表示するには、インシデントレコードの [添付されたナレッジ] 関連リストを開きます。

- i** 注: OT ナレッジベースの [公開ワークフロー] フィールドを [ナレッジ - 公開承認] に設定した場合、記事を公開する前に承認する必要があります。

でのナレッジ記事の作成 産業用 ワークスペース

産業用 ワークスペース でナレッジ記事を作成して、オペレーショナルテクノロジー (OT) インシデントに直接関係しないニーズとソリューションに記事のコンテンツを提供できるようにします。

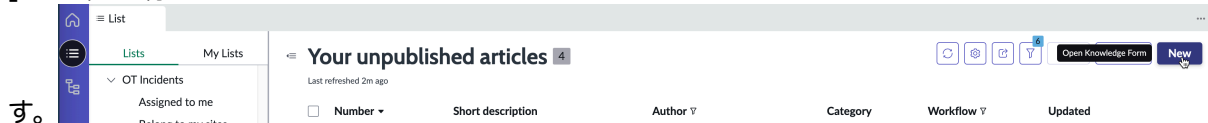
始める前に

必要なロール: knowledge

- i** 注: また、少なくとも 1 つのナレッジベースへの 寄稿可能 アクセスも必要です。詳細については、「[OT ナレッジベースの作成](#)」を参照してください。

手順

1. 移動先 [すべて > 産業用ワークスペース](#).
2. ナレッジモジュールのリストビューで、利用可能なリストのいずれかを開きます。
3. **[New (新規)]** を選択しま



4. フォームで、フィールドに入力します。

ナレッジ記事フォーム

フィールド	説明
ナレッジベース	ナレッジ記事を含めるナレッジベース。 i 注: OT ナレッジベースの可視化が正しく構成されている場合、OT ユーザーはこの参照リストでナレッジベースを見つけることができます。
カテゴリ	ナレッジ記事の分類。
簡単な説明	ナレッジ記事のタイトルとして使用されるインシデント解決の簡単な説明。
記事本文	インシデントの手順、課題、およびソリューションを説明するナレッジ記事のコンテンツ。
有効期間終了日	ナレッジ記事の有効期限。

5. **[Save (保存)]** を選択します。
ナレッジ記事がドラフトとして保存され、親 OT インシデントに添付されます。
6. **[Publish (公開)]** を選択します。

結果

ナレッジ記事が OT ナレッジベースに公開されました。

- i** 注: OT ナレッジベースの [公開ワークフロー] フィールドを [ナレッジ - 公開承認] に設定した場合、記事を公開する前に承認する必要があります。

OT インシデントレコードからのナレッジギャップの報告

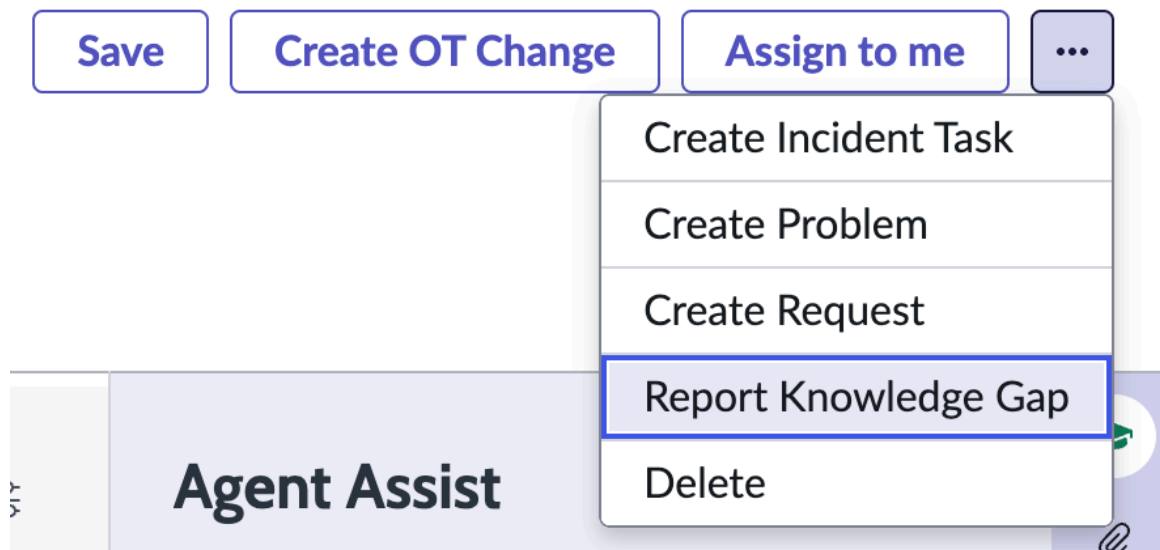
インシデントに関連するナレッジ記事が見つからない場合は、オペレーショナルテクノロジー (OT) インシデントからのナレッジギャップを報告します。

始める前に

必要なロール:sn_ot_incident_read

手順

1. 移動先 **すべて > 産業用ワークスペース**.
2. リストビューの [OT インシデント] モジュールで、利用可能なリストのいずれかを開きます。
3. ナレッジギャップを報告するインシデントレコードを選択します。
4. [その他のアクション] ...) を選択して、メニューを展開します。
5. [ナレッジギャップの報告] を選択しま



6. フォームの [説明] フィールドにナレッジギャップの概要を入力します。

i 注: [トピック] フィールドには、インシデントレコードの名前が自動的に入力されます。必要に応じて、このフィールドを変更できます。

7. [Submit (送信)] を選択します。

結果

ナレッジギャップが報告され、フィードバックタスクが作成されます。

次のタスク

フィードバックタスクは、インシデントレコードの [ナレッジギャップ] 関連リストの下に表示されます。

フィードバックタスクを適切なユーザーまたはユーザーグループにアサインするには、「[フィードバックタスクのアサイン](#)」を参照してください。

ナレッジ記事の公開または廃止要求の承認

ナレッジ記事の公開または廃止の要求を承認して、ナレッジベースを最新の状態に保ちます。

始める前に

必要なロール:knowledge_manager

このタスクについて

OT ナレッジベース受領のマネージャーとしてアサインされている場合は、ナレッジベースに属する記事の公開と廃止の承認要求を受け取ることができます。

手順

1. 承認要求に関するメール通知を開きます。
2. メール内のリンクを選択して、要求を開きます。
3. その要求を承認または却下します。
4. オプション: 却下された場合は、記事要求が却下された理由を説明するコメントを残します。

結果

承認要求を作成したユーザーにメールで通知されます。

フィードバックタスクのアサイン

フィードバックタスクをユーザーにアサインして、フィードバックタスクが対処され、関連するナレッジ記事が更新されていることを確認します。

始める前に

必要なロール:knowledge_manager

手順

1. 移動先 **すべて > 産業用ワークスペース**。
2. リストビューのナレッジモジュールで、[未アサインの OT ナレッジギャップ] リストを開きます。
3. ユーザーまたはアサイン先グループにアサインするフィードバックタスクを選択します。
4. [アサイン先] フィールドで、フィードバックタスクのアサイン先のユーザーを追加します。
5. **[Save (保存)]** を選択します。

結果

アサインされたユーザーは、[ナレッジモジュール] リストビューの [自分のフィードバックタスク] リストでフィードバックタスクを表示できるようになりました。

他のアサインされたフィードバックタスクを表示するには、**産業用 ワークスペース**のナレッジモジュールリストビューの下にある [アサインされたフィードバックタスク] リストを選択します。

未アサインの OT ナレッジギャップを表示するには、**産業用 ワークスペース**のナレッジモジュールリストビューの下にある [未アサインの OT ナレッジギャップ] リストを選択します。

OT インシデントの関連ナレッジ記事で情報を検索する

適用可能な以前の解決策について、オペレーショナルテクノロジー (OT) インシデントレコードに添付されている関連ナレッジ記事で情報を検索します。

始める前に

必要なロール:sn_ot_incident_read

- i 注:** このインシデントのコンテキストに一致する記事を含むナレッジベースへの sn_ot_incident_readロールと読み取りアクセス権が必要です。

手順

1. 移動先 **すべて > 産業用ワークスペース**。
2. リストビューの [OT インシデント] モジュールで利用可能なリストを開きます。
3. 表示するインシデントレコードを選択します。

4. インシデントレコードで、[エージェントアシスト] ボタン [] をクリックして [エージェントアシスト] ウィンドウを開きます (まだ開いていない場合)。
5. ナレッジ記事全体を表示するには、[その他のアクション] ボタン []
6. [全画面表示] を選択します。
7. オプション: オープンインシデントレコードにナレッジ記事を添付するには、[エージェントアシスト] ウィンドウで [添付] を選択します。
8. オプション: ナレッジ記事にフラグを設定するには、[エージェントアシスト] ウィンドウで [フラグ] を選択します。
9. オプション: ナレッジ記事を役に立つとマークするには、[その他のアクション] ボタン [] をクリックし、[役に立つ] を選択します。

オペレーショナルテクノロジーのナレッジ管理の参照

参照トピックには、オペレーショナルテクノロジーのナレッジ管理に関する追加情報が記載されています。

オペレーショナルテクノロジーのナレッジ管理 ロール

オペレーショナルテクノロジーのナレッジ管理ユーザーにナレッジ管理ロールを割り当てることができます。

次の表に、オペレーショナルテクノロジーのナレッジ管理機能にアクセスするためにユーザーに割り当てることができるナレッジ管理ロールを示します。

ナレッジ管理 適用可能なロール オペレーショナルテクノロジーのナレッジ管理

ロール	説明
ナレッジ	ナレッジロールは、デフォルトのナレッジベースに寄稿することができ、またナレッジアプリケーションメニューにアクセスすることができます。ナレッジロールは履行者ロールであり、要求者ロールではありません。  注: 要求者は、ナレッジ記事を表示したり、コメントしたり、フィードバックを提供したりすることができます。ただし、要求者は記事を作成または編集することはできません。
knowledge_manager	ナレッジマネージャーは、カテゴリの定義、重要な記事の固定、記事への変更の承認など、管理するナレッジベースの管理機能を実行できます。ナレッジベースのマネージャーとして選択されたユーザーは、このロールを自動的に受け取ります。  注: ナレッジロールは従属ロールとして提供されます。

ナレッジ管理 適用可能なロール オペレーショナルテクノロジーのナレッジ管理 (続く)

ロール	説明
knowledge_admin	ナレッジアドミニストレーターは、ナレッジ管理 システムのメンテナンスに関連するすべての管理タスクを実行できます。 i 注: - ナレッジアドミンとして選択されたユーザーは、スコープ付きナレッジベースを除くすべてのナレッジベースを変更できます。 - ナレッジロールは従属ロールとして提供されます。

ナレッジベース フォーム

新しいナレッジベースを作成する場合は、次のフォームフィールドに記入します。

ナレッジベースフォームのフィールド

フィールド	説明
タイトル	オペレーショナルテクノロジー (OT) ナレッジベースの一意の名前。
記事の有効期間	作成日以降に記事が有効なデフォルトの日数。
アイコン	OT ナレッジベースを説明する視覚的参照を提供する画像。画像は、記事検索結果ページのこのナレッジベースのすべての記事の横に表示されます。
コメントの無効化	コメントを無効化するオプション。選択すると、ユーザーは OT ナレッジベースの記事にコメントできません。
提案の無効化	編集の提案を無効にするオプション。選択すると、ユーザーは OT ナレッジベースの記事の編集を提案できません。
カテゴリ編集の無効化	OT ナレッジカテゴリの編集を無効にするオプション。選択すると、OT ナレッジマネージャーのみが OT ナレッジベースのナレッジカテゴリを追加または編集できます。
評価を無効化	記事の評価を無効にするオプション。選択すると、ユーザーは OT ナレッジベースの記事を評価できません。
役に立つとマークする機能を無効化	役に立つとマークを無効にするオプション。選択すると、ユーザーは OT ナレッジベースで記事を役に立つとマークできません。
ブロックを有効化	ナレッジブロック機能を有効にするオプション。選択すると、OT ナレッジベース内のナレ

ナレッジベースフォームのフィールド (続く)

フィールド	説明
	ジ記事に追加するナレッジブロックを作成できます。
チェックリスト	OT ナレッジベースの記事の品質を評価するためのチェックリスト。
アプリケーション	OT ナレッジベースのアプリケーションスコープ。
所有者	OT ナレッジベースを担当するユーザー。ナレッジベースの所有者は、他のロールをナレッジベースにアサインできます。
マネージャー	OT ナレッジベースで管理機能を実行するユーザー。
公開用ワークフロー	ナレッジベースに記事を公開するためのワークフロー: - ナレッジ - すぐに公開:承認の必要なしにナレッジベースに記事を公開します。 - ナレッジ - 公開承認:記事を公開ステータスに移行する前に、ナレッジベースのマネージャーからの承認を要求します。
廃止用ワークフロー	OT ナレッジベースの記事を廃止するためのワークフロー: - ナレッジ - すぐに廃止:承認の必要なくナレッジベースの記事を廃止します。 - ナレッジ - 廃止承認:記事を廃止ステータスに移行する前に、ナレッジベースのマネージャーからの承認を要求します。
アクティブ	OT ナレッジベースがアクティブであることを示すオプション。選択しない場合、admin ロールを持つユーザーまたはナレッジアドミニストレータのみが記事を作成、検索、または表示できます。
説明	
ナレッジフィールドのデフォルト値設定	OT ナレッジベースのデフォルト設定。
関連製品	OT ナレッジベースコンテンツに関連する製品のリスト。

関連情報

OT 拡張クラスと関連アプリケーションの詳細を確認してください。

拡張クラスの概要

拡張クラスは、オペレーショナルテクノロジー管理 が 構成管理データベース (CMDB)でどのように機能するかを理解するのに役立ちます。

オペレーショナルテクノロジー (OT) 拡張クラス

CMDB は OT のクラスを更新します。

関連アプリケーション

ナレッジ管理

ナレッジ管理アプリケーションを使用すると、ナレッジベースで情報を共有できます。これらのナレッジベースには、セルフヘルプ、トラブルシューティング、およびタスク解決などの情報をユーザーに提供する記事が含まれています。

オペレーショナルテクノロジーインシデント管理

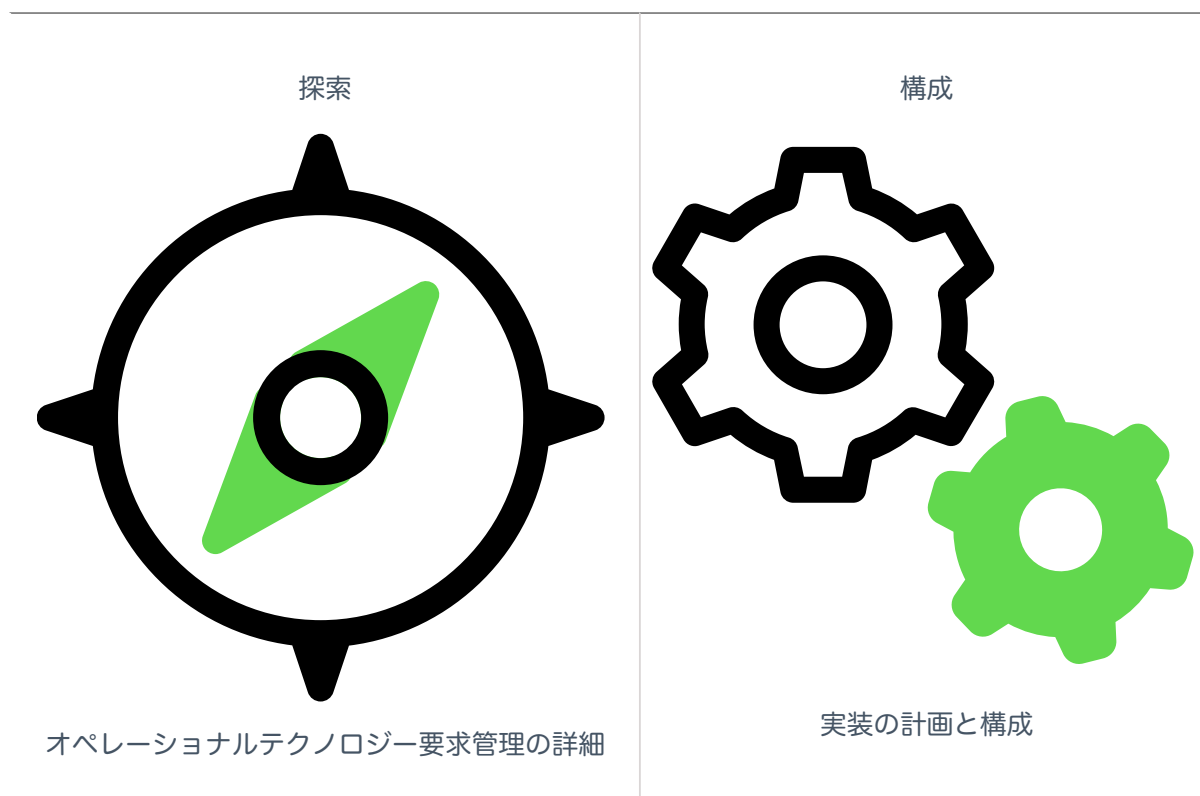
オペレーショナルテクノロジーインシデント管理 アプリケーションを使用すると、メーカーはインシデントがオープンされてから完了するまで、OT デバイスインシデントを管理できます。

IT Service Management

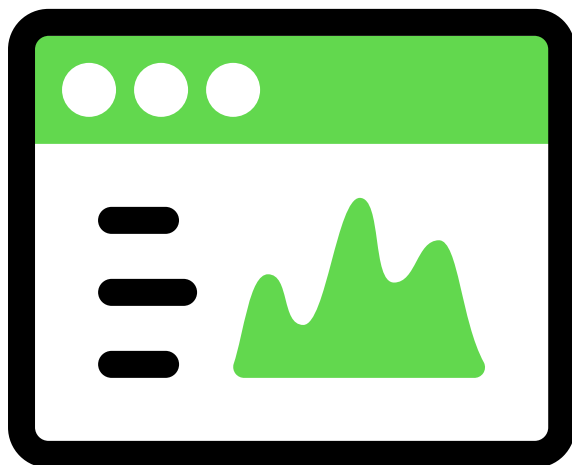
ServiceNow IT Service Management アプリケーションを オペレーショナルテクノロジーのナレッジ管理 と統合すると、エンジニアは OT デバイスと本番プロセスの問題を迅速に解決できます。

オペレーショナルテクノロジー要求管理

オペレーショナルテクノロジー要求管理 を使用すると、カタログアイテムを要求し、定義されたフローに基づいて履行できます。

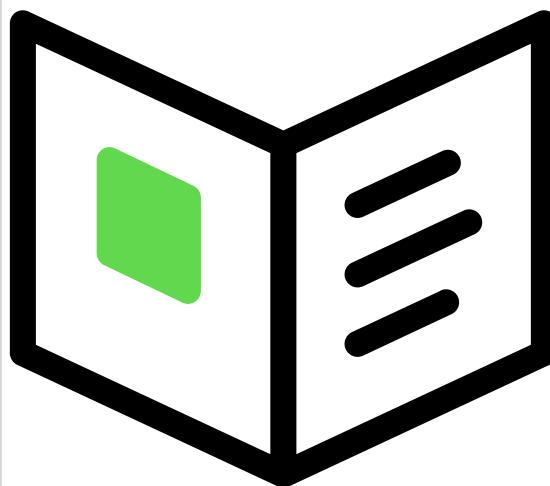


使用方法



オペレーショナルテクノロジー要求管理の使用

参照



関連情報とアプリケーションの詳細を取得

オペレーショナルテクノロジー要求管理の探索

オペレーショナルテクノロジー要求管理を使用すると、オペレーショナルテクノロジー (OT) サービスカタログにアクセスして OT カタログアイテムを要求し、定義されたフローに基づいて実行できます。OT ワーカーは、カタログアイテムから OT 要求を作成して送信できます。これにより、一貫したエクスペリエンスが提供され、部門横断型要求が容易になります。

オペレーショナルテクノロジー要求管理の概要

オペレーショナルテクノロジー要求管理の詳細については、Operational Technology Service Management製品スイートの概要をご覧ください。

[https://player.vimeo.com/video/1019801515?](https://player.vimeo.com/video/1019801515?badge=0&autoplay=0&player_id=0&app_id=58479)

[badge=0&autoplay=0&player_id=0&app_id=58479](https://player.vimeo.com/video/1019801515?badge=0&autoplay=0&player_id=0&app_id=58479)

オペレーショナルテクノロジー要求管理のメリット

オペレーショナルテクノロジー要求管理を使用すると、OT システムに次のメリットを適用し、チームがカタログ要求を管理するのに役立ちます。

- 単一のビューで複数のカタログ要求を効率的に管理できます。
- 透明性を高め、要求プロセスを迅速化し、自動通知と承認によって遅延を最小限に抑えます。
- カタログ要求の作成と更新に使用できる製品とサービスのメニューを維持します。

OT システムへの オペレーショナルテクノロジー要求管理の適用

オペレーショナルテクノロジー (OT) システムにオペレーショナルテクノロジー要求管理を適用して、他のユーザーが OT 製品やサービスの OT 要求を作成して送信できるようにすることができます。

オペレーショナルテクノロジー要求管理の概要

オペレーショナルテクノロジー要求管理を使用すると、カタログアイテムを要求し、定義されたフローに基づいて履行できます。OT ワーカーは、OT サービスカタログで要求を作成し、ニーズに最適なカタログアイテムを選択できます。

ユースケース

次の表では、さまざまな OT ペルソナと、オペレーショナルテクノロジー要求管理の使用方法について説明します。

オペレーショナルテクノロジー要求管理のユースケース

ペルソナ	説明
OT エンジニア	オペレーショナルテクノロジー要求管理を使用して、さまざまな OT 製品やサービスの OT 要求を 1 か所でファイルおよび管理できます。 要求できるカタログアイテムの例としては、サードパーティのリモートアクセス、新しい OT PC、新しい OT デバイス、新しい OT ホスト接続などがあります。
プラント長またはスーパーバイザー	オペレーショナルテクノロジー要求管理を使用して適切なチームと連携し、工場の現場で報告されたインシデントを修正できます。

オペレーショナルテクノロジー要求管理の構成

オペレーショナルテクノロジー (OT) ソリューションのデータ基盤を作成できるようにオペレーショナルテクノロジー要求管理を構成します。

admin ロールを持っている場合は、ガイド付きセットアップを使用してオペレーショナルテクノロジー要求管理のセットアップをガイドできます。ガイド付きセットアップは、アプリケーションまたは機能の構成を支援するツールです。構成アクティビティをカテゴリに整理します。これらのカテゴリには、セットアップタスクに関する情報、各タスクを完了するための手順、および構成を実行するインスタンス内のページへのリンクが含まれています。役立つヘルプコンテンツへのリンクも提供されます。

ガイド付きセットアップにアクセスするには、に移動します 産業用ワークスペースアドミン > ガイド付きセットアップ。

次の表に、ガイド付きセットアップタスクとそのオペレーショナルテクノロジー要求管理の目的を示します。

- i 注:** オペレーショナルテクノロジー要求管理は、Industrial Workspace Common に含まれています。追加に必要なロールはありません。

次の表は、セットアップと構成を正しく行うためにユーザーが完了する必要があるタスクを示しています。

オペレーショナルテクノロジー要求管理セットアップタスク

タスク	目的
デモデータをロードします。	オペレーショナルテクノロジー要求管理 のデモデータをロードするには、Industrial Workspace Common プラグインのデモデータをロードする必要があります。デモデータをロードするには、次の手順を実行します。 1. 移動先 すべて > システム定義 > プラグイン。 2. 検索バーで、Industrial Workspace Common プラグインを検索します。 3. 検索結果が読み込まれたら、[インストール済み] タブを選択し、Industrial Workspace の [共通] ページを開きます。 4. [クイックアクション] で、[デモデータのロード] を選択します。
オペレーショナルテクノロジー要求管理 ロールをアサインします。	各ユーザーが使用できるアクションを制御するルールを割り当てます。
カタログビルダーを使用して、OT サービスカタログのカタログアイテムを作成します。	カタログビルダーを使用して OT サービスカタログのカタログアイテムを作成し、他のユーザーが OT 要求を送信してニーズに最適なカタログアイテムを選択できるようにします。
OT サービスカタログで作成するカタログアイテムのカタログアイテムカテゴリを追加します。	OT サービスカタログで作成するカタログアイテムに対してさまざまなカテゴリを選択し、OT カタログアイテムを論理グループに整理します。
フローデザイナー で OT 要求の実行フローを作成します。	必要に応じて、カタログアイテムの フローデザイナー にあるカタログタスクを含む実行フローを作成し、OT 要求を実行します。

オペレーショナルテクノロジー要求管理ユーザーへのロールのアサイン

ユーザーにロールをアサインして、オペレーショナルテクノロジー要求管理の機能とデータへのアクセス権を制御できるようにします。

始める前に

必要なロール：admin

このタスクについて

ユーザーに割り当てることができる オペレーショナルテクノロジー要求管理 ロールの詳細については、「[オペレーショナルテクノロジー要求管理とともにインストールされるコンポーネント](#)」を参照してください。

手順

ServiceNow AI Platform ユーザー管理機能を使用して、ユーザーとグループにロールをアサインします。

タスク	ユーザー管理機能
ユーザーへのロールのアサイン	ユーザーへのロールの割り当て を参照してください。
グループへのロールのアサイン	グループへのロールのアサイン を参照してください。

カタログアイテムカテゴリ

オペレーショナルテクノロジー (OT) サービスカタログで作成するカタログアイテムに対して、さまざまなカテゴリを選択できます。カテゴリは、OT カatalogアイテムを論理グループに整理するのに役立ちます。要求者は OT 要求を送信するときに、指定されたカテゴリに基づいてニーズに最適なカタログアイテムを選択できます。

必要に応じて、カテゴリとサブカテゴリを定義して OT カatalogアイテムを整理し、ユーザーが必要な製品やサービスを見つけやすくすることができます。カタログアイテムカテゴリを定義する方法の詳細については、「[カテゴリの作成](#)」を参照してください。

オペレーショナルテクノロジーサービスカタログのカタログアイテムを作成する

カタログビルダーを使用して オペレーショナルテクノロジー (OT) サービスカタログのカタログアイテムを作成し、他のユーザーがカタログアイテム別に分類された OT 要求を送信できるようにします。

始める前に

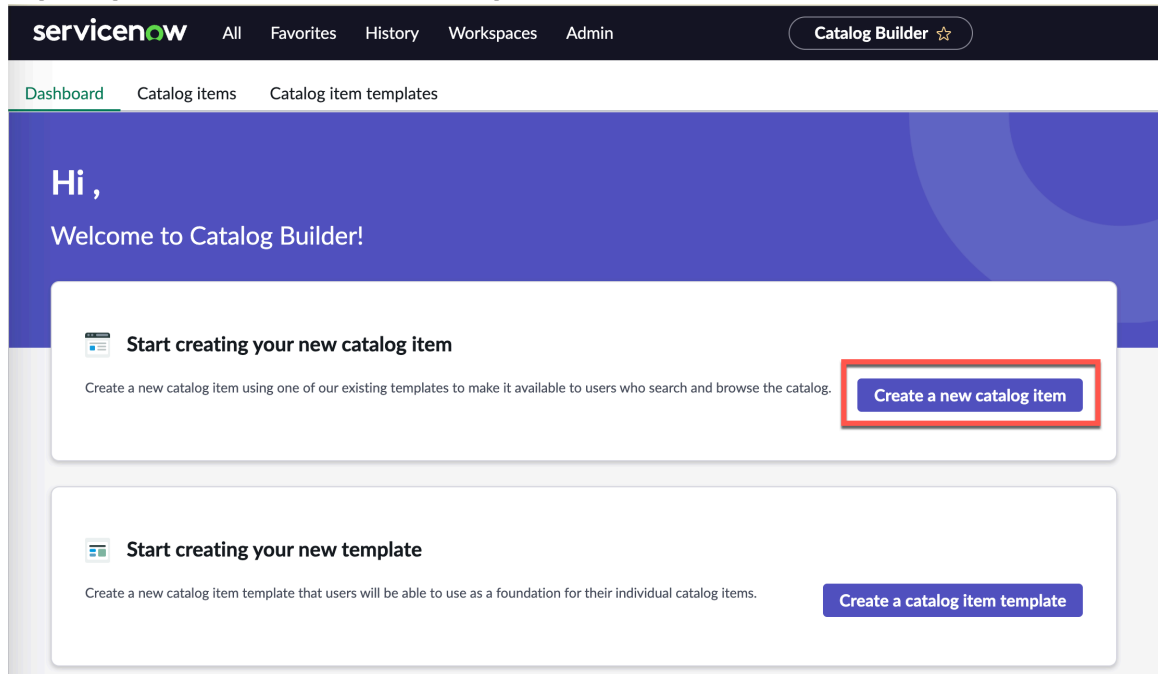
必要なロール：admin

このタスクについて

カタログビルダーで OT サービスカタログのカタログアイテムを作成できます。他のユーザーが OT 要求を送信するときに、ニーズに最適なカタログアイテムを選択できます。たとえば、OT デバイスへのリモートアクセスの要求を、OT サービスカタログで利用可能なカタログアイテムにすることができます。これにより、サードパーティは OT デバイスに関連する問題に取り組むことができます。

手順

1. 移動先 **すべて > サービスカタログ > カタログビルダー**。
2. [ダッシュボード] タブの [新しいカタログアイテムの作成を開始] で、[新しいカタログアイテムの作成] を選択しま



す。

または、[カタログアイテム] タブを選択して [新規] をクリックします。

3. [はじめに] ページで、[続行] を選択します。
4. [アイテムテンプレートを選択 (**Select your item template**)] ページで、**OT** カタログアイテムテンプレートを選択します。
5. [**Use this item template**] をクリックします。
6. [カタログアイテムを作成] フォームで、フィールドに入力します。

[カタログアイテム] フォームフィールドの詳細については、「[オペレーショナルテクノロジー カタログアイテムフォーム](#)」を参照してください。

注: [質問] セクションから OT カタログアイテム変数セットを削除することはできません。OT カタログアイテム変数セットは、OT 要求を他の要求と区別するものです。代わりに、[新しい質問の挿入] を選択して、アイテムフォームの新しい質問を作成できます。新しい質問を挿入する方法の詳細については、「[カタログビルダーでのカタログアイテムの質問の作成](#)」を参照してください。

7. オプション: カタログアイテムをプレビューするには、[プレビュー] を選択します。
8. オプション: 進行状況を保存するには、[保存] を選択します。
9. [レビューと送信] セクションに移動したら、追加したカタログアイテム情報を確認し、[送信] を選択します。
10. 作成するカタログアイテムごとに手順 1 ~ 9 を繰り返します。

結果

カタログアイテムが作成され、他のユーザーが OT サービスカタログで OT 要求を作成するときに選択できるようになります。

オペレーショナルテクノロジー要求の実行フローの作成

必要に応じて、オペレーショナルテクノロジー (OT) 要求を履行するために、カタログアイテムのフローデザイナーにあるカタログタスクを含む実行フローを作成します。

始める前に

必要なロール：admin

このタスクについて

実行フローをカタログアイテムにリンクできます。実行フローは、別のユーザーが OT 要求を送信したときに、カタログタスクの作成と通知をトリガーします。

手順

1. 移動先 **すべて** > プロセス自動化 > フローデザイナー。
2. [フロー] ボタンを選択します。
3. [新規] ドロップダウンで [フロー] を選択します。
4. プロパティフォームのフィールドに入力します。
プロパティフォームの詳細については、「[ワークフロースタジオ でのフローの作成](#)」を参照してください。
5. **[Build Flow (フローを構築)]** を選択します。
6. フローにトリガーを追加します。
詳細については、「[ワークフロースタジオ でのフローの作成](#)」を参照してください。
7. アクション、フロー、サブフロー、または Glow ロジックを追加します。
詳細については、「[ワークフロースタジオ でのフローの作成](#)」を参照してください。
8. **[Save (保存)]** を選択します。

結果

フローデザイナー は、実行フローのフロー、トリガー、およびアクションのドラフトを保存します。これで、実行フローを選択してカタログアイテムに適用できるようになりました。

オペレーショナルテクノロジー要求管理 の使用

オペレーショナルテクノロジー要求管理 に必要なすべてのセットアップタスクを完了すると、ユーザーは オペレーショナルテクノロジー (OT) 要求の作成と管理を開始できます。

でオペレーショナルテクノロジー 要求を作成する 産業用 ワークスペース

OT デバイスまたはインシデントに必要な製品またはサービスに対処するために、産業用 ワークスペース で オペレーショナルテクノロジー (OT) 要求を作成します。

始める前に

必要なロール:任意の OT ユーザー

手順

1. 移動先 **すべて** > 産業用ワークスペース。
2. 産業用 ワークスペースリストビューを開きます。
3. **[OT 要求]** リストモジュールで、[自分の要求] リストを選択します。

i 注:

[自分の要求] リストには、産業用 ワークスペースにアクセスできるすべての OT ユーザーがアクセスできます。

4. **[New (新規)]** を選択します。

5. OT サービスカタログで、ニーズに最適な利用可能なカタログアイテムを 1 つ選択します。

6. 必要に応じて、要求に応じてフィールドに入力します。

7. **[要求]** を選択します。

次のタスク

OT 要求が送信されると、要求の詳細が記載されたメールが届きます。メールに記載されているリンクを使用して、要求レコードを開き、そのステータスを追跡できます。要求を完了するために必要な追加のコンテキストを使用して、要求レコードを編集することもできます。

要求レコードに変更が加えられた場合は、行われた変更を説明するメールで通知されます。たとえば、作業メモがレコードに追加された、またはステータスが更新されました。

オペレーショナルテクノロジー要求管理のリスト 産業用 ワークスペース

オペレーショナルテクノロジー (OT) 要求とカタログタスクを産業用 ワークスペースリストビューで表示できます。

OT 要求

次のリストは、**[OT 要求]** モジュールの **[産業用 ワークスペース]** リストビューで OT 要求を表示してアクセスするために使用できます。

i 注: これらのリストにアクセスするには、sn_request_read ロールが必要です。

OT 要求リスト

リスト	説明
自分の要求	ユーザーによって、または管理者によって提出された OT 要求。
オープン中の要求アイテム	すべての OT 要求

OT カatalogタスク

OT カatalogタスクは、**[OT タスク]** モジュールで利用可能なリストで確認できます。OT カatalogタスクの場合、**[タスクタイプ]** 列の値は **[カatalogタスク]** です。

オペレーショナルテクノロジー要求管理の参照

参照トピックには、オペレーショナルテクノロジー要求管理に関する追加情報が記載されています。

オペレーショナルテクノロジー要求管理とともにインストールされるコンポーネント

いくつかのタイプのコンポーネント (ユーザーロール、サービスカタログなど) が、オペレーショナルテクノロジー要求管理のアクティブ化とともにインストールされる場合があります。

インストールされているロール

オペレーショナルテクノロジー要求管理のロール

名前	説明	ロールを含む
sn_request_read	要求 (sc_request,)、要求アイテム (sc_req_item)、またはカタログタスク (sc_task) への読み取りアクセス。	NA
sn_request_write	要求 (sc_request)、要求アイテム (sc_req_item)、またはカタログタスク (sc_task) への書き込みアクセス。	• task_editor • dependency_views • agent_workspace_user • view_changer • cmdb_read • cmdb_query_builder_read • sn_request_read
sn_request_comment_write	要求アイテム (sc_req_item) のコメントへの書き込みアクセス。 i 注: sn_request_comment_write ロールだけではコメントの書き込みアクセス権が付与されないため、テーブルへの書き込みアクセス権が必要です。	NA

インストールされているサービスカタログ

オペレーショナルテクノロジー要求管理サービスカタログ

名前	説明
OT サービスカタログ	ユーザーが OT 要求を送信するために提供されるサービスカタログ。

オペレーショナルテクノロジー カatalogアイテムフォーム

オペレーショナルテクノロジー (OT) サービスカタログの新しいカタログアイテムを作成する場合は、次のフォームフィールドに入力します。

次の表では、OT カatalogアイテムフォームの各セクションで利用可能なフィールドについて説明します。

詳細

フィールド	説明
基本情報	
アイテム名	カタログに表示される名前。
簡単な説明	サービスカタログホームページ、検索結果、注文フォームのタイトルバーに表示されるテキスト。
アイテムの詳細	
イメージ	アイテムの画像。
説明	アイテムの完全な説明。この説明は、ユーザーがアイテムを選択するか、関連するプレビューリンクをクリックしたときにカタログに表示されます。 ビデオ、画像、社内ナレッジベース (KB) 記事へのリンク、外部情報源や指示書へのリンクを埋め込むことができます。

場所

フィールド	説明
カタログ	
選択されているカタログ	このアイテムが表示されるカタログ。
カテゴリ	
選択したカテゴリ	アイテムのカテゴリ。カテゴリは、[カタログ] フィールドの入力後にのみ選択できます。 カタログ検索では、サービスポータルのカテゴリに割り当てられたアイテムのみが検索されます。
トピック	
選択されたトピック	アイテムのトピック。カタログアイテムが公開されると、要求者は、追加されたトピックを使用してカタログアイテムを検索してアクセスできます。

質問

フィールド	説明
OT カatalogアイテム変数セット	
サイト	カタログアイテムの影響を受けるサイト。

設定

フィールド	説明
ポータル設定	
送信ボタンラベル	要求者がカタログアイテムフォームへの入力を完了した後の送信ボタンのラベル。
[カートに追加] ボタンを非表示	選択すると、アイテムに [カートに追加] ボタンが表示されません。ウィジェットの [カートに追加を表示する] インスタンスオプションが false に設定されている場合、この設定は無視されます。 この設定は、[要求の方法] が [要求] または [送信] の場合はデフォルトで選択されています。 アップグレードシナリオでは、プラットフォームで [カートなし] フィールドが選択されている場合は、CatalogPortalSettingsMigration スクリプトインクルードを実行して、この設定を更新して、[ポータル設定] タブの [カートに追加] フィールドを非表示にします。 i 注: カatalogアイテムと注文ガイドに適用されます。
[下書きとして保存] ボタンを非表示	選択すると、アイテムに [ドラフトとして保存] ボタンが表示されません。
数量セクターを非表示	選択すると、カタログアイテムに [量] リストが表示されません。 これは、[要求の方法] が [要求] または [送信] の場合はデフォルトで選択されています。 アップグレード顧客の場合は、プラットフォームで数量なしフィールドが選択されている場合は、CatalogPortalSettingsMigration 移行スクリプトを実行して、ポータル設定タブの数量を非表示にするフィールドにこの設定を更新します。 i 注: カatalogアイテムに適用されます。 注文ガイドは、含まれているカタログアイテムからこの設定を継承します。
配送時間を非表示	選択すると、カタログアイテムに [配送時間] フィールドが表示されません。 これは、[要求の方法] が [送信] の場合はデフォルトで選択されています。 i 注: カatalogアイテムに適用されます。

設定 (続く)

フィールド	説明
	注文ガイドは、含まれているカタログアイテムからこの設定を継承します。
[添付ファイル] ボタンを非表示	選択すると、カタログアイテムに [添付ファイルを追加] ボタンが表示されません。 i 注: カatalogアイテムとレコードプロデューサーに適用されます。 注文ガイドは、含まれているカタログアイテムからこの設定を継承します。
添付を必須に設定	選択すると、カタログアイテムに添付ファイルを追加することが必須になります。 i 注: カatalogアイテムとレコードプロデューサーに適用されます。

アクセス

フィールド	説明
利用可能	
アクセスを許可するユーザー基準	カタログアイテムにアクセスできるユーザー基準を選択します。
利用不可	
アクセスを拒否するユーザー基準	カタログアイテムにアクセスできないユーザー基準を選択します。

フルフィルメント

フィールド	説明
実行方法	
プロセスエンジン	アイテム要求の実行の順序。
選択されたフロー	アイテム要求の実行方法を定義するフロー。 i 注: このフィールドは、[プロセスエンジン] フィールドで [フローデザイナーフロー] を選択した場合にのみ表示されます。
選択したワークフロー	アイテム要求の実行方法を定義するワークフロー。

フルフィルメント (続く)

フィールド	説明
	i 注: このフィールドは、[プロセスエンジン] フィールドで [ワークフロー] を選択した場合にのみ表示されます。

関連情報

オペレーショナルテクノロジー (OT) 拡張クラスと関連アプリケーションの詳細を確認してください。

拡張クラスの概要

拡張クラスは、オペレーショナルテクノロジー管理 が 構成管理データベース (CMDB)でどのように機能するかを理解するのに役立ちます。

[オペレーショナルテクノロジー \(OT\) 拡張クラス](#)

CMDB は OT のクラスを更新します。

関連アプリケーション

[要求管理](#)

要求管理を使用すると、定義されたフローに基づいてカタログアイテムを要求して実行できます。

[IT Service Management](#)

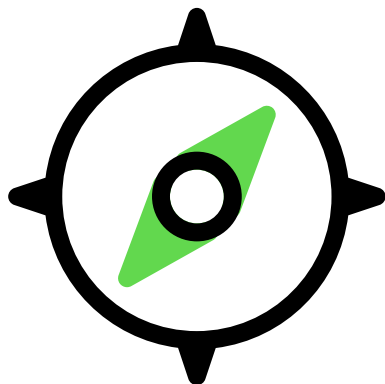
ServiceNow IT Service Management アプリケーションを使用すると、エンジニアは OT デバイスと本番プロセスの問題を迅速に解決できます。

Operational Technology Service Management (OTSM) の推奨アクション

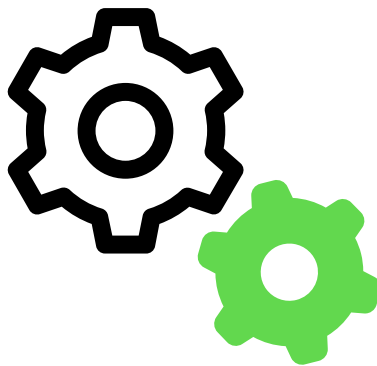
Operational Technology Service Management の推奨アクション (OTSM) を使用すると、リアルタイムのアクション可能な推奨事項を設定して適用し、トリアージプロセスを迅速化し、オペレーショナルテクノロジー (OT) インシデントを含む産業用ワークスペース内のさまざまなレコードにわたる問題を迅速に解決できます。

開始するには

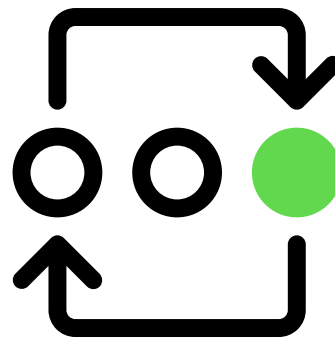
探索	構成	使用方法



OTSM の推奨アクションが OT システムの管理にどのように役立つかについて説明します。



特定のニーズに合わせて、OTSM の推奨アクションを設定および構成します。



OTSM の推奨アクションで OTSM レコードを管理します。

役に立つリソース

役立つ情報を提供できる ServiceNow リソースは次のとおりです。



ServiceNow コミュニティ

[ServiceNow コミュニティ](#)



Customer Success Center

[Customer Success Center](#)



ディベロッパー

developer.servicenow.com



Impact

<http://impact.servicenow.com>



ServiceNow University

[ServiceNow University](#)



Now Create

[Now Create](#)



パートナー

<https://www.servicenow.com/partners.html>



ServiceNow

<https://www.servicenow.com/>



ServiceNow Store

https://store.servicenow.com/sn_appstore_store.do#!/store/home



支える

- <https://support.servicenow.com/now>

- [既知のエラーポータル](#)

の推奨アクションの詳細 **Operational Technology Service Management**

Operational Technology Service Managementの推奨アクション (OTSM) を使用すると、リアルタイムのアクション可能な推奨事項を設定して適用し、トリアージプロセスを迅速化し、オペレーショナルテクノロジー (OT) インシデントなどのさまざまなレコードの問題を迅速に解決できます。

OTSM の推奨アクション の概要

推奨事項は、産業用ワークスペース で OT インシデントレコードを更新または作成するときに、サイドパネルにアクション可能なリアルタイムの推奨事項として表示されます。産業用ワークスペースの推奨事項にアクセスするには、サイドパネルの [推奨事項] アイコン () を選択します。

OTSM の推奨アクション ワークフロー

OTSM の推奨アクションのワークフローには、コンテキストの使用が含まれます。OT インシデントコンテキストを使用して、産業用ワークスペース の推奨事項を検索して使用します。

i 注: OT インシデントの場合は、[推奨事項] パネルでガイダンススペースの推奨事項を使用できます。

オペレーショナルテクノロジーサービス管理の推奨アクションの概要

Operational Technology Service Management の推奨アクション (OTSM) には、オペレーショナルテクノロジー (OT) インシデントなど、産業用ワークスペースのさまざまなレコードの推奨アクションを構成するために使用される次のコンテキストコンポーネントが含まれています。

OTSM の推奨アクションのコンテキスト

コンテキストを使用すると、特定のルールが満たされたときに特定のタイプのレコードの推奨事項を表示できます。これらの推奨事項は、レコードのコンテキストに基づいて実行するアクションを提案することで役立ちます。詳細については、「[推奨アクション のコンテキスト](#)」を参照してください。

OTSM コンテキストには、次の表で説明されている OT インシデントコンテキストが付属しています。

コンテキストの説明

コンテキスト	説明
OT インシデントコンテキスト	これにより、産業用ワークスペース のアクティブな推奨事項に基づいて、OT インシデントに関するすべての有効な推奨事項が表示されます。

i 注: コンテキストを作成するには、「[推奨アクション でのコンテキストの作成](#)」を参照してください。

検索結果マッピング

検索結果マッピングは、産業用ワークスペース の OT インシデントレコードの AI 検索結果に表示されます。

OTSM コンテキストには、コンテキストタイプに基づく次の検索結果マッピングが含まれます。

OT インシデント:ナレッジ [kb_knowledge]、OT インシデント [sn_ot_incident]

検索アプリケーション構成

OTSM コンテキストには、**OTSM** 検索構成の **[AIS]** 推奨アクションが含まれています。このアプリケーションは、OT インシデントを含む、産業用ワークスペース内のさまざまなレコードの AI 検索をサポートしています。

でのオペレーショナルテクノロジーサービス管理の推奨アクションの構成 産業用ワークスペース

ユーザーが、オペレーショナルテクノロジーサービス管理 (OTSM) の推奨アクションによって提供される関連する推奨事項で作業できるようにします。

OTSM の推奨アクションは、オペレーショナルテクノロジーインシデント管理 アプリケーションの新機能として提供されます。

オペレーショナルテクノロジーサービス管理の推奨アクションの設定

関連する推奨事項を 産業用ワークスペースに表示する推奨アクションを設定します。

始める前に

必要なロール：admin

手順

1. OTSM の推奨アクションでルールを作成します。

OTSM では、新しいルールを作成できます。詳細については、「[推奨アクション でのルールの作成](#)」を参照してください。

2. 推奨事項を作成します。

OTSM では、新しい推奨事項を作成できます。詳細については、「[推奨アクション での推奨事項の作成](#)」を参照してください。

3. リソースジェネレーターを作成します。

OTSM を使用すると、新しいリソースジェネレーターを作成できます。詳細については、「[推奨アクション でのリソースジェネレーターの作成](#)」を参照してください。

4. ガイダンスおよびフィールドの推奨事項を作成します。

OTSM を使用すると、ガイダンスおよびフィールドの推奨事項を構成または作成できます。詳細については、「[推奨アクション でのガイダンスおよびフィールドの推奨の作成](#)」を参照してください。

Operational Technology Service Management の AI 検索 の構成

Operational Technology Service Management の推奨アクション (OTSM) のAI 検索を構成してインテリジェントなクエリ機能を有効にし、OT インシデントに必要な回答をすばやく見つけられるようにします。

始める前に

必要なロール：admin

このタスクについて

Operational Technology Service Management ユーザーの場合、OT インシデントレコードにAI 検索を使用するには、OT インシデント [sn_ot_incident] テーブルをインデックス付きソースとして定義する必要があります。インデックス作成の詳細については、「[のインデックス付きソース AI 検索](#)」を参照してください。

- i** 注: ナレッジ [kb_knowledge] は OSTM の推奨アクションのインデックス付きソースとしても使用されますが、ナレッジは既にインデックス化されています。

インデックス付きソースを定義するには、ガイド付きセットアップ for AI 検索 を使用できます。次の手順では、[インデックス付きソースの定義] タスクにアクセスする方法について説明します。AI 検索のガイド付きセットアップの詳細については、「[AI 検索の構成](#)」を参照してください。

手順

1. 移動先 **AI 検索** > ガイド付きセットアップ。
2. [検索可能なコンテンツの定義] セクションで、[インデックス付きソースの定義] タスクを選択します。
3. [**Configure**] を選択します。
4. [**AI 検索インデックス付きソース**] リストで、OT インシデントレコードを選択します。
5. [選択したテーブルのインデックス化] ボタンを選択します。

オペレーショナルテクノロジーサービス管理の推奨アクションの使用

オペレーショナルテクノロジーサービス管理 (OTSM) の推奨アクションに必要なすべてのセットアップタスクを完了すると、ユーザーは OT インシデントの推奨アクションの利用を開始できます。

オペレーショナルテクノロジーインシデントへの推奨アクションの適用

オペレーショナルテクノロジー (OT) インシデントに推奨アクションを適用し、OT インシデントレコードのコンテキストに基づいて関連するアクションをユーザーに表示する。

始める前に

必要なロール:sn_ot_incident_write

- i** 注: OT インシデントの推奨アクションを表示できるのは、OT インシデントがアクセス可能なサイトに関連している場合、またはインシデントが [クローズ済み] または [キャンセル] ステータスでない場合のみです。

このタスクについて

OT インシデントレコードを表示するときに [推奨事項] パネルと AI 検索を使用して、インシデントに関連するアクションを表示および選択できます。

推奨アクションの詳細については、「[推奨アクション アプリケーションの使用](#)」を参照してください。

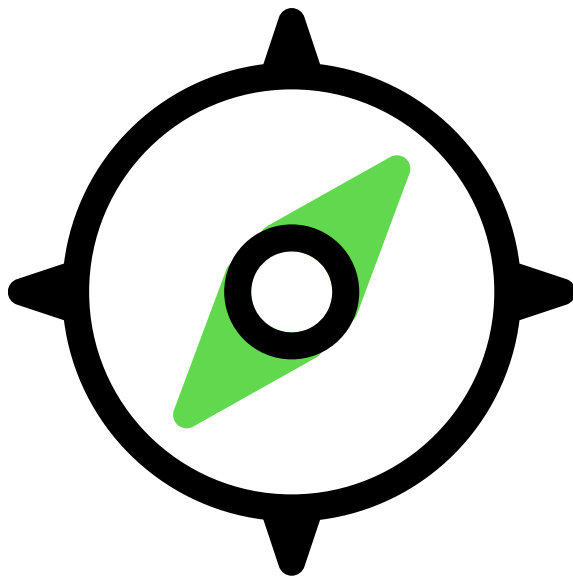
手順

1. 移動先 **すべて** > 産業用ワークスペース。
2. 産業用ワークスペースリストビューを開きます。
3. [OT インシデント] リストモジュールで、利用可能なリストのいずれかを選択します。
4. 推奨アクションを確認するインシデントレコードを開きます。
5. 推奨アクション () アイコンを選択します。
6. [推奨事項] パネルで、推奨アクションを確認して選択します。

産業用 ワークスペース

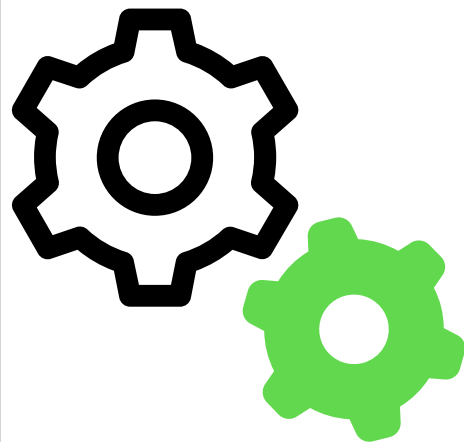
産業用 ワークスペース は、オペレーショナルテクノロジー (OT) ユーザーが OT データを管理するために必要なツールを提供するユーザーインターフェイスです。

探索



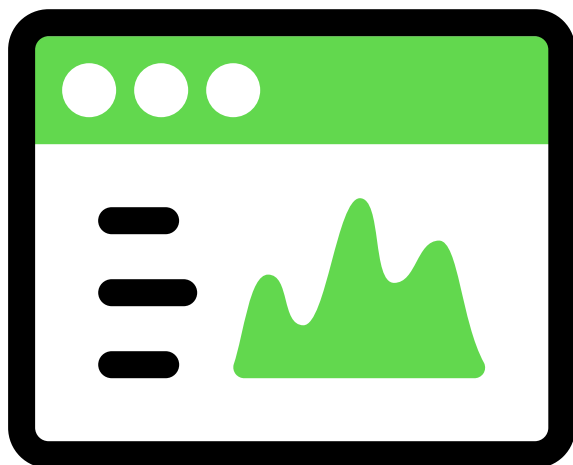
産業用ワークスペースの探索

構成



実装の計画と構成

使用方法



産業用ワークスペースの使用

自動翻訳

産業用ワークスペースの探索

産業用 ワークスペース は、オペレーショナルテクノロジー (OT) ユーザーが OT データを管理するために必要なツールを提供するユーザーインターフェイスです。

産業用 ワークスペース 航法

産業用 ワークスペースは次のページで構成されています。

産業用 ワークスペースページ

ページ	説明
OT アクション指向ランディングページ	ホーム (🏠) アイコンを選択すると、OT アクション指向のランディングページが表示されます。ランディングページは、OT ネットワークに関連する重要なタスクを追跡するのに役立ちます。
ダッシュボードライブラリ	ダッシュボードライブラリ (📊) アイコンを選択すると、以下のダッシュボードを含むダッシュボードライブラリに移動します。 OT ヴィジビリティダッシュボード OT デバイスに関連するデータが含まれています。 オペレーショナルテクノロジー脆弱性対応 (PA) ダッシュボード OT 脆弱性一致アイテムの初期分析と検出から封じ込めや修復までのボリューム、パフォーマンス、および進捗状況を追跡します。 OT 脆弱性リスクロールアップダッシュボード 機器モデルの各レベルでの OT デバイスのリスクスコアが含まれます。
OT 進捗状況スコアカード	OT 進捗状況スコアカード (📈) アイコンを選択すると、OT 進捗状況スコアカードが表示されます。OT 進捗状況スコアカードを使用すると、1 つのビューでサイトデータを比較できます。
Industrial Workspace のリストビュー	リスト (☰) アイコンを選択すると、産業用ワークスペースリストビューが表示され、OT データレコードに関連するすべてのリストにアクセスできます。次のリストモジュールと後続のリストにアクセスできます。 • オペレーショナルテクノロジー (OT) • 情報技術 (IT) ハードウェア • 産業用プロセスマネージャー • OT インシデント

産業用 ワークスペースページ (続く)

ページ	説明
	• OT 変更要求 • OT 修復タスク • OT 脆弱性一致アイテム • OT タスク • ナレッジ
機器モデルマネージャー	機器モデル () アイコンを選択すると、機器モデルマネージャーが表示され、サイトとその機器モデルデータを表示できます。

オペレーショナルテクノロジー アクション指向ランディングページ

オペレーショナルテクノロジー (OT) アクション指向ランディングページを使用して、OT ネットワークに関連する重要なタスクを追跡できます。

OT アクション指向ランディングページの概要

OT アクション指向ランディングページは、OT エンジニアなどのユーザーが自分、サイト、またはグループにアサインされたタスクを表示するのに役立ちます。ランディングページには、サインインしているユーザーにとって優先順位を付ける必要がある重要なアクションが呼び出され、既存の OT インシデント、OT 変更要求、OT 修復タスク、OT 脆弱性一致アイテム、およびその他のタスクの概要が含まれます。

ランディングページには、日常のタスクと重要なアクションの詳細なロールベースのビューが表示されます。[重要なアクション] セクションの各タスクには、デフォルトでオープン日でソートされたタスクが表示されます。タスクが重要な場合は、[重要なアクション] セクションに表示されます。

OT アクション指向ランディングページにアクセスするには、次に移動します。すべて > 産業用ワークスペースで、[ホーム] () アイコンを選択します。

ランディングページのコンテンツ

次のセクションでは、OT アクション指向ランディングページで表示できるコンテンツについて説明します。

重要なアクション

[重要なアクション] セクションには、重要と見なされ、できるだけ早く対処する必要がある OT タスクまたはアクションが含まれています。デフォルトでは、タスクはオープン日順に整理され、サインインしているユーザーに割り当てられた最近作成された重要なタスクが最初に表示されます。

このセクションに表示されるタスクは、[概要] セクションから抽出された最も重要なタスクであり、処理できます。タスクの重要度は、次の基準によって決定されます。

- 優先度は「重要」です
- タスクは修復タスクであり、そのリスク評価は重大です

このセクションに含まれるタスクは、次のように整理されています。

- サインインしているユーザーに直接アサインされているすべてのタスクが最初に表示されます。
- ユーザーのグループにアサインされていて、どのユーザーにもアサインされていないタスクは、後に表示されます。
- グループまたはユーザーには割り当てられていないが、サインインしているユーザーがアクセスできるサイトに割り当てられているタスクが最後に表示されます。

概要

[概要] セクションには、自分、自分のグループ、またはサイトにアサインされた OT インシデント、変更要求、修復タスク、脆弱性一致アイテム、およびその他のタスクの概要が含まれています。

次のフィルターを使用して、レコードの [アサイン先]、[アサイン先グループ]、および [サイト] フィールドに基づいて表示されるレコードを表示できます。

あなたの仕事

自分にアサインされたレコード。

グループの作業

自分のグループにアサインされたレコード。

サイトの作業

1 つまたは複数のサイトにアサインされたレコード。

次の表では、[概要] セクションのタイルについて説明します。

概要タイル

タイル	説明
自分にアサインされた OT インシデント/グループにアサインされた OT インシデント/サイトにアサインされた OT インシデント	自分、自分のアサイン先グループ、またはサイトのいずれかにアサインされた OT インシデントレコードの数。 すべての OT インシデントレコードのリストを表示するには、[すべてのレコード] を選択します。 ステータスまたはタイプに基づいてレコードのリストのみを表示するには、利用可能なグラフのそれぞれのセクションを選択します。たとえば、優先度に基づいてインシデントレコードのみを表示する場合は、グラフの [重大] セクションを選択します。
自分にアサインされた OT 変更要求 / グループにアサインされた OT 変更要求 / サイトにアサインされた OT 変更要求	自分、自分のアサイン先グループ、またはサイトのいずれかにアサインされた OT 変更要求レコードの数。 すべての OT 変更要求レコードのリストを表示するには、[すべてのレコード] を選択します。 ステータスに基づいてレコードのリストのみを表示するには、利用可能なグラフのそれぞれのセクションを選択します。たとえば、スケジュールされている変更要求レコードのみを表示する場合は、グラフの [スケジュール済み] セクションを選択します。
自分にアサインされた OT 修復タスク / グループにアサインされた OT 修復タスク / サイトにアサインされた OT 修復タスク	自分、自分のアサイン先グループ、またはサイトのいずれかにアサインされた OT 修復タスクレコードの数。

概要タイル (続く)

タイル	説明
	すべての OT 修復タスクレコードのリストを表示するには、[すべてのレコード] を選択します。 ステータスに基づいてレコードのリストのみを表示するには、利用可能なグラフのそれぞれのセクションを選択します。たとえば、レビュー中の修復タスクレコードのみを表示する場合は、グラフの [レビュー中] セクションを選択します。
自分にアサインされた OT 脆弱性一致アイテム / グループにアサインされた OT 脆弱性一致アイテム / サイトにアサインされた OT 脆弱性一致アイテム	自分、アサイン先グループ、またはサイトのいずれかにアサインされた OT 脆弱性一致アイテムレコードの数。 すべての OT 脆弱性一致アイテムレコードのリストを表示するには、[すべてのレコード] を選択します。 リスク評価に基づいてのみレコードのリストを表示するには、利用可能なグラフのそれぞれのセクションを選択します。たとえば、優先度の高い脆弱性一致アイテムレコードのみを表示する場合は、グラフの [高] セクションを選択します。
自分にアサインされたその他の OT タスク / グループにアサインされたその他の OT タスク / サイトにアサインされたその他の OT タスク	自分、自分のアサイン先グループ、またはサイトにアサインされた他の OT タスクレコードの数。 他のすべての OT タスクレコードのリストを表示するには、[すべてのレコード] を選択します。 優先度に基づいてレコードのリストのみを表示するには、利用可能なグラフのそれぞれのセクションを選択します。たとえば、優先度が低いと見なされる OT タスクのみを表示する場合は、グラフの低のセクションを選択します。

OT CMDB の健全性

OT CMDB ヘルスは、構成管理データベース (CMDB) 内のデバイスの健全性を監視および維持するのに役立ちます。OT デバイスの数をタイプ別に整理して表示できます。

- i** 注: このセクションは、オペレーショナルテクノロジーマネージャー がインストールされている場合にのみ表示されます。

次の表では、[OT CMDB の健全性] セクションのタイルについて説明します。[OT CMDB の健全性] セクションを表示するには、**cmdb_ot_isa_viewer** ロールが必要です。

[OT CMDB ヘルス] タイル

タイル	説明
未分類の OT デバイス	OT ネットワーク内で OT デバイスタイプカテゴリが割り当てられていない OT デバイスの数。

[OT CMDB ヘルス] タイル (続く)

タイル	説明
	未分類の OT デバイスレコードのリストを表示するには、[すべてのレコード] を選択します。
未アサインの OT デバイス	ユーザーにアサインされていない OT ネットワーク内の OT デバイスの数。 未アサインの OT デバイスレコードのリストを表示するには、[すべてのレコード] を選択します。
マッピングされていない OT デバイス	アサインされたサイトの機器モデルエンティティにマッピングされていない、OT ネットワーク内の OT デバイスの数。 マッピングされていない OT デバイスレコードのリストを表示するには、[すべてのレコード] を選択します。 i 注: このタイルは、製造業プロセス マネージャー がインストールされていて、サインインしているユーザーが cmdb_ot_isa_viewerロールを持っている場合にのみ使用できます。タイルでは、OT デバイスを本番プロセスにマッピングするための機器モデルが組織にある必要があります。
サイトがアサインされていません	サイトにアサインされていない OT ネットワーク内の OT デバイスの数。 i 注: このタイルは、サインインしているユーザーがcmdb_ot_isa_viewerロールを持っている場合にのみ使用できます。 サイトのない OT デバイスレコードのリストを表示するには、[すべてのレコード] を選択します。
IP アドレスなし OT デバイス	IP アドレスが割り当てられていない OT ネットワーク内の OT デバイスの数。 IP アドレスのない OT デバイスレコードのリストを表示するには、[すべてのレコード] を選択します。

のダッシュボードライブラリ 産業用ワークスペース

産業用ワークスペースのダッシュボードライブラリには、オペレーショナルテクノロジーヴィジビリティダッシュボード、オペレーショナルテクノロジー脆弱性対応 (PA) ダッシュボード、および オペレーショナルテクノロジー 脆弱性リスクロールアップダッシュボードが含まれています。

オペレーショナルテクノロジー ヴィジビリティダッシュボード

オペレーショナルテクノロジー (OT) ヴィジビリティダッシュボードは、OT デバイスを一元管理するのに役立ちます。OT ヴィジビリティダッシュボードでは、OT デバイスデータにアクセスできます。

OT ヴィジビリティダッシュボードの概要

OT ヴィジビリティダッシュボードは、産業用 ワークスペース内の一元化された場所です。このダッシュボードを使用して、オペレーショナルテクノロジーマネージャー および 製造業プロセスマネージャー データを確認できます。また、これを使用して、OT ネットワーク内の OT デバイスおよび機器モデルエンティティの詳細情報を確認または編集することもできます。

OT ヴィジビリティダッシュボードを使用すると、次のことを実現できます。

- 過去 1 週間に OT ネットワークで変更された OT デバイス情報を把握します。
- 産業施設全体の OT デバイスインベントリの進行状況を表示します。
- OT デバイスを意味のある方法で分析します。たとえば、本番プロセスにマッピングされている本番デバイスの数に関するインサイトを得ることができます。

ダッシュボードのコンテンツ

OT ヴィジビリティダッシュボードで OT デバイスデータにアクセスするには、次に移動します。すべて > 産業用ワークスペースを選択し、ダッシュボードライブラリ () アイコンを選択して、[オペレーショナルテクノロジーのヴィジビリティ] を選択します。次の表で説明されているタイルの重要業績評価指標 (KPI) グラフにアクセスするには、タイルの数値、カウント、またはチャートコンポーネントを選択します。

次の表では、ダッシュボードのさまざまなタイルに表示される OT デバイスデータについて説明します。

ダッシュボードタイル

タイル	説明
過去 7 日間の更新	
新しい OT デバイスの検出	過去 7 暦日間に OT ネットワーク内の オペレーショナルテクノロジー およびその他の自動化プロセスについてディスカバリーによって検出された新しい OT デバイスの数。
非アクティブな OT デバイス	過去 7 暦日間に OT ネットワークに表示されなかった OT デバイスの数。これらのデバイスは非アクティブと見なされます。
OT デバイスの概要	
OT デバイスの合計CMDB	
未分類の OT デバイス	OT ネットワーク内で OT デバイスタイプカテゴリがアサインされていない OT デバイスの数。
未アサインの OT デバイス	ユーザーにアサインされていない OT ネットワーク内の OT デバイスの数。

ダッシュボードタイル (続く)

タイル	説明
マッピングされていない OT デバイス	アサインされたサイトの機器モデルエンティティにマッピングされていない、OT ネットワーク内の OT デバイスの数。 i 注: このタイルは、組織に OT デバイスを本番プロセスにマッピングするための機器モデルが必要なため、製造業プロセスマネージャー がインストールされている場合にのみ使用できます。
カテゴリ別の OT デバイス	
監督システム	監督システムカテゴリにアサインされている OT ネットワーク内の OT デバイスの数。
コントロールシステム	[コントロールシステム] カテゴリにアサインされている OT ネットワーク内の OT デバイスの数。 i 注: コントロールモジュールはこの数に含まれません。
フィールドデバイス	フィールドデバイスカテゴリにアサインされている OT ネットワーク内の OT デバイスの数。
コンピューターとサーバー	[コンピューターとサーバー] カテゴリにアサインされている OT ネットワーク内の OT デバイスの数。
ネットワーク機器	ネットワーク機器カテゴリにアサインされている OT ネットワーク内の OT デバイスの数。
Industrial IoT (産業用 IoT)	産業用モノのインターネット (IoT) カテゴリにアサインされている OT ネットワーク内の OT デバイスの数。
Purdue レベル別の OT デバイス	OT ネットワーク内の OT デバイスの数を、アサインされた Purdue レベル別に表示する棒グラフ。 i 注: OT システムの Purdue レベルの詳細については、「https://subscription.packtpub.com/book/networking_and_servers/9781788395151/1/ch01lvl1sec10/the-purdue-model-for-industrial-control-systems」を参照してください。
タイプ別の OT デバイス (トップレベル)	OT デバイスデータを OT デバイスタイプ別に分類した棒グラフ。
メーカー別の OT デバイス (トップレベル)	OT ネットワーク内の OT デバイスの数を、アサインされたメーカー別に表示する円グラフ。

ダッシュボードタイル (続く)

タイル	説明
重要度別の OT デバイス	OT ネットワーク内の OT デバイスの数を、アサインされた重要度別に示す円グラフ。

ダッシュボードを表示するために必要なロール

OT ヴィジビリティダッシュボードにアクセスするには、 **cmdb_ot_viewer** ロールと **cmdb_ot_isa_viewer** ロールが必要です。

Site filter (サイトフィルター)

サイトフィルターを使用して、ダッシュボードに表示するサイトを検索して選択できます。サイトフィルターにアクセスして使用するには、表示するサイトへのアクセス権を持つ **cmdb_ot_isa_viewer** ロールが必要です。

詳細については、「[サイトフィルターを使用](#)」を参照してください。

オペレーショナルテクノロジー脆弱性対応 (PA) ダッシュボード

オペレーショナルテクノロジー (OT) 脆弱性一致アイテム (VI) の初期分析と検出から封じ込めや修復までのボリューム、パフォーマンス、および進捗状況を追跡します。アサイン先グループ、エクспロイト、リスク評価、またはステータスでレポートをフィルタリングして、脆弱性エクスポージャーと影響を受けるサービスに関するインサイトを得ることができます。

必要な オペレーショナルテクノロジー ロールと オペレーショナルテクノロジー脆弱性対応 ロール

OTVR (PA) ダッシュボードにアクセスするには、 **sn_otvr.remediation_owner** ロールが必要です。

オペレーショナルテクノロジー脆弱性対応 (PA) ダッシュボードを表示するには、次に移動します: すべて > 産業用ワークスペース をクリックし、ナビゲーションパネルの [ダッシュボードライブラリ] ( アイコン) を選択します。次に、[オペレーショナルテクノロジー脆弱性対応] を選択します。

ユースケース

次の表は、組織内のさまざまなユーザーがこのダッシュボードをどのように使用できるかの例をいくつか示しています。

オペレーショナルテクノロジー脆弱性対応 (PA) ダッシュボードのユースケース

ユーザー	ダッシュボードの使用方法
OT サイトマネージャー、OT アナリスト、脆弱性修復オーナー	どの OT 脆弱性一致アイテムが最もリスクが高いかを判断することで、脆弱性の悪用によって増加するセキュリティインシデントに組織が対処できるようにします。このダッシュボードは、OT 脆弱性一致アイテムのアクティビティをグラフィカルに表示し、修復計画とステータスの進捗状況の設計に役立ちます。影響を受ける重要なデバイスと目立った脆弱性に関連する重要業績評価指標 (KPI) に集中できます。

ダッシュボードタブ

経時的な傾向データを示すレポートと、リアルタイムデータを含むレポートを表示できます。また、重要なメトリクスの傾向を定期的に表示して、ビジネスプロセス全体を分析し、改善が必要な領域を特定することもできます。

[脆弱性一致アイテム] タブ、[修復] タブ、および [例外] タブの内容について説明します。

[脆弱性一致アイテム] タブ

[脆弱性一致アイテム] タブでは、脆弱性のリスクとそのまん延、影響を受けるデバイス、修復ターゲットの遵守、および修復の進捗状況の KPI を確認できます。

[脆弱性一致アイテム] タブでは、次のレポートを表示できます。

- OT 脆弱性一致アイテムの合計
- 新しい OT 脆弱性一致アイテム
- 未アサインの OT 脆弱性一致アイテム
- ステータス別の OT 脆弱性一致アイテム
- リスク評価別の OT 脆弱性一致アイテム
- 修復ターゲットを満たした OT VI

 注: データは、先月、3 か月、6 か月、年、または全期間で表示できます。

- OT VI 平均修正時間 (MTTR)

 注: データは、先月、3 か月、6 か月、年、または全期間で表示できます。

- 経過時間別の OT VI
- 修復ターゲットステータス別のクローズ済み OT 脆弱性一致アイテム
- アサイン先グループ別の重大な OT 脆弱性一致アイテム
- アサイン先グループ別の期限切れの重大な脆弱なアイテム

[修復] タブ

[修復] タブは、修復アクションの進捗状況を把握し、その完了に最も支援が必要なサポートチームを確認するのに役立ちます。

[修復] タブでは、次のレポートをリアルタイムで表示できます。

- OT 修復タスク
- 期限間近の重大な OT 修復タスク
- リスク評価別の OT 修復タスク
- ターゲットステータス別の OT 修復
- ステータス別の OT 修復タスク
- 未アサインの OT 修復タスク
- アサイン先グループ別の OT 重大な修復タスク
- アサイン先グループ別の期限切れの重大な OT 修復タスク

[例外] タブ

[例外] タブは、修正が過度に保留される可能性があるために組織がリスクを負っている場所を把握するのに役立ちます。

[例外] タブでは、次のレポートをリアルタイムで表示できます。

- 理由別の保留された OT 脆弱性一致アイテム
- アサイン先グループ別の重大な脆弱性一致アイテムの OT 例外。

Site filter (サイトフィルター)

サイトフィルターを使用して、ダッシュボードに表示するサイトを検索して選択できます。サイトフィルターにアクセスして使用するには、表示するサイトへのアクセス権を持つ **cmdb_ot_isa_viewer** ロールが必要です。

詳細については、「[サイトフィルターを使用](#)」を参照してください。

インジケータースource

オペレーショナルテクノロジー脆弱性対応インジケータースourceは、次のsourceからデータを収集します。

- OTVI.アクティブ
- OTVI.クローズ済み
- OTRT.アクティブ

ダッシュボードに使用されるインジケータースourceの詳細については、「[オペレーショナルテクノロジー脆弱性対応 \(PA\) ダッシュボードのインジケータースourceとインジケータースource](#)」を参照してください。

インジケータースourceから 100 万件を超えるレコードが収集されることが予想される場合は、インジケータースourceの [レコード収集] セクションで予想される数を上書きする必要があります。詳細については、「[多数のレコードのインジケータースourceを確認する](#)」を参照してください。

インジケータースource

オペレーショナルテクノロジー脆弱性対応 アプリケーションの脆弱性修復の進捗状況を測定および追跡するために、いくつかのインジケータースourceが使用されます。ダッシュボードに使用されるインジケータースourceの詳細については、「[オペレーショナルテクノロジー脆弱性対応 \(PA\) ダッシュボードのインジケータースourceとインジケータースource](#)」を参照してください。

インジケータースourceの レコード収集 オプションは、オペレーショナルテクノロジー脆弱性対応 アプリケーションではデフォルトで無効になっています。このオプションは、各インジケータースourceの大量のデータを収集するときに発生する可能性のあるパフォーマンスの問題を回避するためにオフになっています。

ブレイクダウン

ブレイクダウンは、収集されたレコードを定性的属性でフィルタリングしてグループ化します。ダッシュボードのインジケータースourceは、次のように分析されます。

- 経過時間
- クローズした経過時間
- アサイン先グループ
- CI マネージャー

- 保留の理由
- エクスプロイト攻撃ベクトル
- エクスプロイト有無
- エクスプロイトスキルレベル
- 修復ターゲットルール
- 修復ターゲットステータス
- 修復ターゲットステータス (クローズ済み)
- リスク評価
- 重大度
- 状況

ブレイクダウンソースは、ブレイクダウンに含まれる一意の値を指定します。一意の値はブレイクダウン要素と呼ばれます。ダッシュボードでは、次のブレイクダウンソースを使用します。

- アサイン先グループ
- Deferred.Reason.Non.Closed
- エクスプロイト攻撃ベクトル
- エクスプロイト有無
- エクスプロイトスキルレベル
- OT 経過時間範囲
- 修復ターゲットステータス
- 修復ターゲットステータス (クローズ済み)
- Remediation.Target.Rule
- リスク評価
- 過酷
- 状態
- Vulnerable.Item.CI.Manager

ブレイクダウンとブレイクダウンソースの詳細については、「[オペレーショナルテクノロジー脆弱性対応 \(PA\) ダッシュボードのブレイクダウン](#)」を参照してください。

収集ジョブ

ダッシュボードでは、次の収集ジョブを使用して、ダッシュボードに表示される OT 脆弱性データを収集します。

- [PA OT VR]履歴脆弱性データの収集
- [PA OT VR]修復タスクの日次収集
- [PA OT VR]脆弱性一致アイテム 1 の日次収集
- [PA OT VR]脆弱性一致アイテム 2 の日次収集

収集ジョブの詳細については、「[オペレーショナルテクノロジー脆弱性対応 \(PA\) ダッシュボード収集ジョブ](#)」を参照してください。

データの可視化

オペレーショナルテクノロジー脆弱性対応 (PA) ダッシュボードでは、データのビジュアル化を使用して OT 脆弱性データを表示します。たとえば、システム内の OT 脆弱性一致アイテムの合計数は、[OT 脆弱性一致アイテムの合計] 棒グラフに表示され、OT デバイスタイプ別にグループ化されます。

ダッシュボードで使用されるデータの可視化の詳細については、「[オペレーショナルテクノロジー脆弱性対応 \(PA\) ダッシュボードで使用されるデータの可視化](#)」を参照してください。

オペレーショナルテクノロジー リスク管理ダッシュボード

オペレーショナルテクノロジー (OT) リスク管理ダッシュボードには、機器モデルの各レベルの OT デバイスのリスクスコアと脆弱性一致アイテム (VIT) が含まれています。

OT リスク管理ダッシュボードについて

OT リスク管理ダッシュボードは、産業用ワークスペース のダッシュボードライブラリ (🔗) で利用できます。OT リスク管理ダッシュボードのロールアップされた脆弱性リスクスコアについては、次のテーブルを利用できます。

- 機器モデルエンティティの脆弱性リスクテーブル
- サイトがアサインされていない OT デバイスの脆弱性リスクテーブル

OT リスク管理ダッシュボードのテーブル

テーブル	説明
機器モデルエンティティの脆弱性リスクテーブル	サイトの機器モデルエンティティとその VIT のリスクスコアを表示します。また、最もリスクの高い領域と VIT の数も強調表示されます。
サイトにアサインされていない OT デバイスの脆弱性リスクテーブル	どのサイトにもアサインされていない OT デバイスのリスクスコアと脆弱性一致アイテムの数を表示します

表示された VIT の数を選択すると、エンティティに対して作成されたすべての VIT レコードを表示できます。さらに、VIT レコードを選択してその詳細を表示できます。

ダッシュボードを表示するために必要なロール

OT リスク管理ダッシュボードにアクセスするには、**sn_otvr.remediation_owner**、**cmdb_ot_isa_viewer**、および **admin** ロールが必要です。

サイトの OT 脆弱性リスクを表示する

[サイト] リストを使用して、ダッシュボードに表示するサイトを検索して選択できます。

[リスクタイプを選択] リストから **OT 脆弱性リスク** を選択して、選択したサイトのロールアップされたリスクスコアと VIT を表示します。

オペレーショナルテクノロジー 進捗状況スコアカード

オペレーショナルテクノロジー (OT) 進捗状況スコアカードを使用すると、サイト間でデバイスと脆弱性一致アイテムのデータを比較できます。

OT 進捗状況スコアカードの概要

OT 進捗状況スコアカードは、サイトデータを比較できる 産業用 ワークスペース 内の一元化された場所です。サイトデータには、OT デバイスデータと脆弱性データの両方が含まれます。OT 進捗状況スコアカードを使用すると、サイトの進捗状況を追跡し、注意が必要なサイトを特定できます。

次の オペレーショナルテクノロジー アプリケーションのサイトデータを表示することもできます。

- オペレーショナルテクノロジーマネージャー
- オペレーショナルテクノロジー脆弱性対応
- オペレーショナルテクノロジーインシデント管理
- オペレーショナルテクノロジー変更管理

産業用ワークスペースアドミン ガイド付きセットアップを使用して OT 進捗状況スコアカードを設定できます。セットアップタスクの詳細については、「[オペレーショナルテクノロジー進捗状況スコアカードの設定](#)」を参照してください。

スコアカードの内容

OT 進捗スコアカードにアクセスするには、次に移動します: すべて > 産業用ワークスペース をクリックし、[**OT 進捗状況スコアカード**] アイコン () を選択します。

次の表では、OT 進捗スコアカードの列について説明します。

OT 進捗状況スコアカードの列

列	説明
全体スコア (%)	スコアカードのインジケータによって決定されるサイトの進捗状況。重み付けを編集して、インジケータが全体のスコアにどの程度寄与するかを制御できます。詳細については、「 オペレーショナルテクノロジー進捗状況スコアカードのシステムプロパティを設定します 」を参照してください。
で予想される OT デバイスの割合 (%) CMDB	構成管理データベース (CMDB)に含めると予想される OT デバイスの割合。 i 注: 値が -1 の場合は、[CMDB で予想される OT デバイスの割合 (%)] インジケータの 1 つ以上の値に、[OTPSC 属性] テーブルの [予想される OT デバイス] 属性がありません。予想される OT デバイスの構成方法については、「 サイトに想定される OT デバイスの構成 」を参照してください。
分類済み OT デバイス (%)	分類済み OT デバイスの割合。分類済み OT デバイス (%) には、cldb_ci_ot として分類された OT デバイスは含まれません。
アサイン済み OT デバイス (%)	次のフィールドに値を持つ OT デバイスの割合: • アサイン先 • 所有者

OT 進捗状況スコアカードの列 (続く)

列	説明
	• 管理担当者 • サポート担当者 • 承認グループ • 管理対象グループ • サポート担当者 (Support by) • 変更グループ
OT デバイスデータの完全性 (%)	データ目標を達成する OT デバイスの割合。このメトリクスは、CMDB 健全性ダッシュボード - 完全性スコア計算ジョブによって異なり、CI クラスマネージャーで必須フィールドと推奨フィールドを設定する必要があります。詳細については、「CMDB ヘルスの構成」を参照してください。 完全性は、次のメトリクスによって決定される KPI です。 必須 必須として定義されたフィールドが入力されていない CI の割合を測定します。欠落しているフィールドは、この CI の情報が欠落していることを示して、未完了としてタグ付けされます。 推奨 推奨として設定されたフィールドが入力されていない CI の割合を測定します。 データの完全性の詳細については、次を参照してください。 CMDB ヘルス KPI とメトリクス i 注: 値が -1 の場合は、CMDB 健全性ダッシュボード:完全性スコア計算ジョブがまだ実行されていません。または、ジョブが未完了ステータスで実行されました。
マッピングされた OT デバイス (%)	機器モデルエンティティにマッピングされた OT デバイスの割合。 i 注: 値が 0 の場合は、OT デバイスが見つかりません。
バックアップされた OT デバイス (%)	バックアップレコードが作成された OT デバイスの割合。

OT 進捗状況スコアカードの列 (続く)

列	説明
	i 注: 値が 0 の場合は、OT デバイスが見つかりません。
アサインされた OT 脆弱性一致アイテム (%)	クローズおよび対処されていない OT 脆弱性一致アイテムの割合。 i 注: 値が 0 の場合は、OT デバイスが見つかりません。
承認された OT 変更要求 (%)	送信および承認された OT 変更要求の割合。 i 注: 値が 0 の場合は、OT デバイスが見つかりません。
OT コンテキストのある OT インシデント (%)	OT デバイスまたは機器モデルデータを含む OT インシデントの割合。 i 注: 値が 0 の場合は、OT デバイスが見つかりません。

オペレーショナルテクノロジー での統一マップエクスペリエンス 産業用ワークスペース

産業用ワークスペース で利用可能な オペレーショナルテクノロジー (OT) 統一マップは、デバイスと他の構成アイテム (CI) との関係を表示し、OT インシデントや変更要求などの関連アイテムを表示するための統一されたエクスペリエンスを提供します。

統一マップの概要

OT 統一マップエクスペリエンスでは、選択した CI (ホームノード) を中心に、CI とその関係の階層マップが表示されます。このエクスペリエンスでは、依存関係ビューとサービスマッピングの機能が単一のマップエクスペリエンスに結合されます。

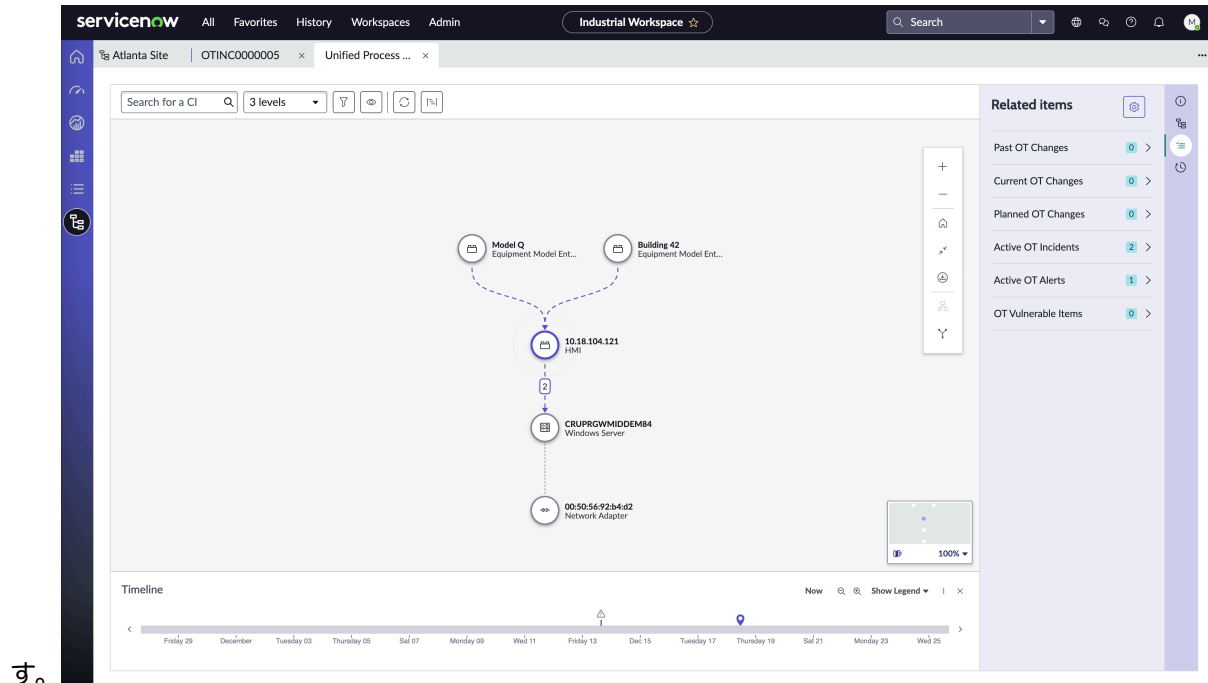
統一マップには、産業用ワークスペース内の次の場所からアクセスできます。

- 機器モデルマネージャーの ISA レコード
- OT インシデントレコード
- OT 変更レコード

統一マップでは、次の関連アイテムのノードがハイライト表示されているのもわかります。

- 過去の OT 変更
- 現在の OT 変更
- 予定されている OT 変更
- アクティブな OT インシデント
- アクティブ OT アラート
- OT 脆弱性一致アイテム

次の画像は、ホームノードがハイライト表示された OT インシデントレコードの統一マップを示しています。



す。

OT 統一マップエクスペリエンスの構成の詳細については、「[オペレーショナルテクノロジー統一マップエクスペリエンスの設定](#)」を参照してください。

OT 統一マップを表示する方法の詳細については、「[オペレーショナルテクノロジー統一マップを表示](#)」を参照してください。

オペレーショナルテクノロジー ハードウェア脆弱性アセスメント

オペレーショナルテクノロジー (OT) ハードウェア脆弱性アセスメント (HVA) アプリケーションを使用すると、インベントリ内の OT デバイスのファームウェア脆弱性を評価し、影響を受ける OT デバイスに対して脆弱性一致アイテム (VIT) を作成できます。

ハードウェア脆弱性アセスメントの概要

ハードウェア脆弱性アセスメント は、ファームウェアディスカバリーモデルに正規化されたコンテンツを使用してアセスメントを実行します。正規化されたコンテンツには、メーカー、ファームウェアバージョン、製品モデルなどの OT デバイスデータが含まれています。これは、エンタープライズ資産管理 で利用可能な正規化プロセスに基づいています。OT デバイスの正規化されたコンテンツは、脆弱性情報データベース (NVD) によって提供される共通プラットフォーム一覧 (CPE) 形式に従ってマッピングされます。NVD データベースで利用可能な共通脆弱性識別子 (CVE) データが CPE マッピングされた正規化されたコンテンツで利用可能な OT デバイスデータと一致する場合、OT デバイスはリスクがあると見なされます。産業用ワークスペース で利用可能な ハードウェア脆弱性アセスメント メニューには、リスクのある OT デバイスが表示されます。

HVA は、正規化されたコンテンツがなく、まだ CPE マッピングされていないファームウェアディスカバリーモデルを評価できます。HVA は、マッチングスコアルゴリズムを使用して、CPE 値を既存のファームウェアディスカバリー値と比較します。照合アルゴリズムは、同じディスカバリーパブリッシャー名、モデル名、およびバージョンを持つ OT デバイスに一致する CPE を検索します。HVA一致アルゴリズムは、CPE とマッピングされていないファームウェアディスカバリーモデルのデータを比較します。比較に基づいて、マッチングアルゴリズムは、マッピングされていないファームウェアディスカバリーモデルに対して可能な限り最適な CPE 一致を評価します。結果が完全に正確でなくても、CPE にマッピングされた正規化コンテンツが利用可能になるまでは、脆弱性アセスメントに役立ちます。

また、HVA は NVD によって提供される範囲情報を使用して、脆弱性をより正確に評価します。たとえば、次のようになります。

- CPE でバージョン情報を利用できない場合は、特定の OT デバイスの公開者とモデルで利用可能な範囲情報を使用して、ハードウェア脆弱性アセスメントが実行されます。
- バージョンの場合、比較アルゴリズムを使用して、入力バージョンが範囲内にあるかどうかを判断します。

i 重要: 既に HVA を使用している場合は、NVD 統合を再実行して範囲情報機能を使用します。詳細については、「[の NVD 統合を実行 ハードウェア脆弱性アセスメント](#)」を参照してください。

ハードウェア脆弱性アセスメントを自動的かつ定期的に行うために、次のスケジュール済みジョブをアクティブ化してスケジュールする必要があります。

- *Hardware Vulnerability Assessment - Full*
- *Hardware Vulnerability Assessment - Delta*

必要なオペレーショナルテクノロジー ロールと ハードウェア脆弱性アセスメント ロール

[ハードウェア脆弱性アセスメント (HVA)] メニューを使用するには、次のロール持っている必要があります

- `sn_vul.manage_exposure_assessment`: 必要に応じてアドミンユーザーまたはユーザーグループにロールをアサインします。これにより、アドミンユーザーまたはユーザーグループは、HVA のプロパティを表示または編集できます。
- `sn_otvr.vul_event_manager` (OT 脆弱性イベントマネージャー): 必要に応じて HVA ユーザーまたはユーザーグループにロールをアサインします。これにより、アセスメントレコードを表示してそれに応じて行動できるようになります。

ユースケース

OT ハードウェア脆弱性アナリストは、HVA を使用して次のことができます。

- OT デバイスのサイバーセキュリティリスクを特定します。
- OT デバイスデータの完全一致アセスメントにより、高リスクの脆弱性に焦点を当てます。
- 完全に一致したアセスメントに対して脆弱性一致アイテムの自動作成を設定します。
- 部分的に一致したアセスメントを調査して対処し、潜在的なリスクを特定し、それに応じて対処します。
- 完全なディスカバリーまたはコンテンツの更新が保留中の未処理の OT デバイスを [正規化待ち] タブから監視します。

HVA のタブ

[HVA] メニューには HVA OT デバイス用に作成されたレコードが表示されます。これらのアセスメントレコードは、多くの基準に基づいて作成されます。たとえば、CVE 脆弱性、リスクのある OT デバイス、共通脆弱性採点システム (CVSS) スコア、信頼スコア、デバイスの重要度などです。

- [完全に一致したアセスメント] タブには、CVE が OT デバイスのメーカー、製品モデル、およびファームウェアバージョンと完全に一致するアセスメントレコードが表示されます。完全に一致したアセスメントとは、OT デバイスが CVE で指定されたすべての脆弱性要因と一致することを意味します。

- [部分的に一致したアセスメント] タブには、CVE が OT デバイスのファームウェアバージョンまたはメーカーとモデルと部分的に一致するアセスメントレコードが表示されます。また、HVA は、利用可能なファームウェアバージョンがない正規化されたディスカバリーモデルの部分的な評価を作成します。照合アルゴリズムを使用して、パブリッシャーとモデルが同じ OT デバイスの正規化されたコンテンツのバージョン情報を使用してアセスメントが作成されます。
- [脆弱性一致アイテム] タブには、自動的に作成された VIT またはアセスメントに基づいて手動で作成した VIT が表示されます。
- [無視されたアセスメント] タブには、無視することを選択したデバイスのアセスメントが表示されます。
- [正規化待ち] タブには、正規化されたデータを持たず、アセスメントに使用されていない OT デバイスデータが表示されます。

i 重要:

- 自動 VIT を作成するプロパティが有効になっている場合、[完全に一致したアセスメント] タブにデータは表示されません。この情報は、[脆弱性一致アイテム] タブ表示できます。
- OT デバイスデータを正規化に使用できるように、エンタープライズ資産管理 でファームウェアディスカバリーモデルのオプトイン機能を有効にします。詳細については、「[エンタープライズ資産管理コンテンツサービスへのオプトイン](#)」を参照してください。

その他のリソース

関連トピック

[エンタープライズ資産管理 正常化](#)

[産業用 ワークスペース](#)

[ガイド付きセットアップを使用したオペレーショナルテクノロジーデバイスのハードウェア脆弱性アセスメント設定](#)

[e のハードウェア脆弱性アセスメントメニュー産業用ワークスペース](#)

ハードウェア脆弱性アセスメントの信頼スコア算出

信頼スコアは、部分的に一致したアセスメント、脆弱性一致アイテム (VIT)、および無視されたアセスメントに表示されます。

信頼スコアの計算について

HVA は、信頼スコアと呼ばれるスコアリングメカニズムを使用して、OT デバイスの CPE マッピングされた正規化されたコンテンツに一致する CVE データの精度を示します。信頼スコアは、HVAのマッチングアルゴリズムによって作成されたマッチングスコアの集計計算です。

信頼スコアは、次のアセスメントによって異なります。

- 完全に一致したアセスメント:CVE 情報内のすべてのパラメーターが OT デバイスで利用可能なデバイスディスカバリーモデル値と一致するため、完全なアセスメントの場合、信頼スコアは 1 です。
- 部分的に一致するアセスメント:CPE 情報内のすべてのパラメーターが OT デバイスで利用可能なデバイスディスカバリーモデル値と一致しないため、部分的なアセスメントの場合、信頼スコアは 1 未満になります。

OT デバイスで利用可能な共通プラットフォーム一覧 (CPE) 情報から信頼スコアを計算する例を次に示します。

脆弱性アセスメントレコード **CVE-2019-13946** のサンプルを次に示します。

Vulnerability	Description	OT device	Confidence score	CPE Firmware	Discovery model	Vendor	Product Model	Version	Firmware Version	Last assessed
CVE-2019-13946	Profinet-IO (PNIO) stack versions prior V3.0.0 do not properly limit internal resource allocation when multipl...	OT_device_demo_internal_963	0.7	Siemens SIMATIC ET200MP IM155-5 PN HF Firmware...	Siemens ET200 FW: V3.0.0	Siemens Aktiengesellschaft	SIMATIC ET 200	4.2		2025-06-20 08:31:31

次に、OT デバイスにマッピングされた CPE ファームウェアで使用可能な情報 **OT_device_demo_internal_963**例を示します。

OT デバイスのディスカバリーモデルで利用可能な情報の例を次に示します (**OT_device_demo_internal_963**)。

信頼スコアの計算方法

OTデバイスにマップされたCPEファームウェアのサンプルとOTデバイスの検出モデルを比較すると、次のことがわかります：

- モデル情報には部分一致のみがあります。部分一致のため、モデルスコアには値 20 が割り当てられます。
- バージョン情報が一致しないため、バージョンスコアには値 0 が割り当てられます。

信頼スコアの範囲は 0 ~ 1 です。信頼スコアは、CPE 情報に基づいて次の式で計算されます。

$$((\text{BASE SCORE}) + (\text{publisher score}) + (\text{model score}) + (\text{version score})) / 100$$

=

$$((25) + (25) + (20) + (0)) / 100$$

=

$$70 / 100$$

=

$$.70$$

- i** 注: 信頼スコアの計算に使用される値を参照するには、「[ハードウェア脆弱性アセスメントの信頼スコア参照テーブル](#)」を参照してください。

ハードウェア脆弱性アセスメントの信頼スコア参照テーブル

信頼スコアの計算に使用される参照値。

参照テーブル

信頼スコア計算参照テーブル

OT デバイスのディスカバリーモデルで利用可能な情報	OT デバイスにマッピングされた CPE で利用可能な情報	部分一致スコア	完全一致の追加スコア
検出されたパブリッシャー名	パブリッシャー	20	5
検出されたモデル名	モデル	20	5
検出されたバージョン	バージョン	0	25

信頼スコアサマリーテーブル

スコア	値
すべてのスコアの合計	75
基本スコア	25
i 注: 一致したすべてのディスカバリーモデルに与えられる最小スコア。	
合計スコア	100

の構成 産業用 ワークスペース

オペレーショナルテクノロジー (OT) データを管理できるように産業用 ワークスペースを構成します。

admin ロールを持っている場合は、ガイド付きセットアップを使用して 産業用 ワークスペースのセットアップをガイドできます。ガイド付きセットアップ は、アプリケーションまたは機能の構成を支援するツールです。構成アクティビティをカテゴリに整理します。これらのカテゴリには、セットアップタスクに関する情報、各タスクを完了するための手順、および構成を実行するインスタンス内のページへのリンクが含まれています。役立つヘルプコンテンツへのリンクも提供されます。

ガイド付きセットアップにアクセスするには、に移動します 産業用ワークスペースアドミン > ガイド付きセットアップ。

次の表に、産業用 ワークスペースのガイド付きセットアップタスクとその目的を示します。

産業用 ワークスペース セットアップタスク

タスク	目的
産業用 ワークスペースロールをアサインします。	産業用 ワークスペース を構成する必要があるユーザーに、構成産業用ワークスペース [configure_industrial_workspace] ロールを割り当てます。
ホームページ宛先ルールを確認します。	ユーザー基準に基づいて、ユーザーを 産業用 ワークスペース 内の別のページにリダイレクトします。
OT アクション指向ランディングページの構成タスクを完了します。	ユーザーが 産業用 ワークスペース のランディングページにアクセスできるように、OT アクション指向ランディングページを構成します。
OT 進捗スコアカードの構成タスクを完了します。	ユーザーがサイトデータと 産業用 ワークスペース の進捗状況の比較を開始できるように、OT 進捗状況スコアカードを構成します。
OT ヴィジビリティダッシュボードの構成タスクを完了します。	ユーザーが 産業用 ワークスペース のダッシュボードにアクセスできるように、OT ヴィジビリティダッシュボードのタブを構成します。
オペレーショナルテクノロジー脆弱性対応 (PA) ダッシュボードの構成タスクを完了します。	産業用 ワークスペース の オペレーショナルテクノロジー脆弱性対応 (PA) ダッシュボードを構成します。
OT 統一マップエクスペリエンスの構成タスクを完了します	デフォルト設定を変更する場合は、OT 統一マップエクスペリエンスを構成します。

産業用 ワークスペースロールをアサインする

ワークスペースの機能とデータへのアクセス権を制御できるように、ユーザーに 産業用 ワークスペース ロールをアサインします。

始める前に

必要なロール：admin

このタスクについて

次の表にリストされているロールを持つユーザーは、OT アクション指向ランディングページと OT 進捗スコアカードの ガイド付きセットアップ にアクセスできます。

OT 進捗状況スコアカードロール

ロール	説明
産業用ワークスペースの構成 [configure_industrial_workspace]	OT アクション指向ランディングページと OT 進捗状況スコアカードの 産業用 ワークスペース と ガイド付きセットアップ にアクセスできます。

手順

ServiceNow AI Platform ユーザー管理機能を使用して、ユーザーとグループにロールをアサインします。

タスク	ユーザー管理機能
ユーザーへのロールのアサイン	ユーザーへのロールの割り当て を参照してください。
グループへのロールのアサイン	グループへのロールのアサイン を参照してください。

のホームページ宛先ルールの確認 産業用 ワークスペース

産業用 ワークスペースのホームページ宛先ルールを確認します。

始める前に

必要なロール：admin

このタスクについて

ホームページ宛先ルールは、ユーザー基準に基づいてユーザーを 産業用 ワークスペース 内の別のページにリダイレクトします。ホームページ宛先ルールの詳細については、「[産業用ワークスペース ホームページ宛先ルール](#)」を参照してください。

手順

1. **[All (すべて)]** に移動します。
2. **[フィルター]** フィールドに `sys_homepage_destination_rule.list` を追加します。
3. Enter キーを押します。
4. ユーザー基準を編集する次の 産業用 ワークスペース ホームページ宛先ルールのいずれかを選択します。
 - OT 進捗状況スコアカードページ
 - Industrial Workspace ホームページ
 - OT ダッシュボードライブラリページ
 - i 注：** OT ダッシュボードライブラリページルールは、オペレーショナルテクノロジーマネージャー がインストールされている場合にのみ表示されます。
 - ISA 設備階層モデルページ
 - i 注：** ISA 設備階層モデルページルールは、製造業プロセスマネージャー がインストールされている場合にのみ表示されます。
 - 産業用ワークスペースリストページ
5. **[ユーザー基準]** フィールドで、ユーザー基準をコピーします。
6. 選択した 産業用 ワークスペース ページにユーザーをリダイレクトするユーザー基準を適用するには、次の手順を実行します。
 - a. 移動先 **すべて > ユーザー基準**.
 - b. リストビューの検索バーで、手順 5 でコピーしたホームページ宛先ルールのユーザー基準を検索します。

c. リダイレクトする必要ユーザーがユーザー基準と一致するように、ユーザー基準レコードを変更します。

d. **[Update (更新)]** を選択します。

結果

これで、ユーザー基準レコードで定義されたユーザー、グループ、ロールが、産業用 ワークスペース内の選択したページに自動的にリダイレクトされるようになりました。

オペレーショナルテクノロジーアクション指向ランディングページの設定

ユーザーが重要なタスクにアクセスできるように、産業用 ワークスペースに オペレーショナルテクノロジー (OT) アクション指向ランディングページを設定します。

次の表に、OT アクション指向ランディングページの ガイド付きセットアップ タスクとその目的を示します。

OT アクション指向ランディングページのセットアップタスク

タスク	目的
1. OT アクション指向ランディングページのシステムプロパティを設定します。	sn_mfg_common.landing_page_important_actions_limit システムプロパティを使用して、[重要なアクション] の下に表示されるカードの数を変更します。

オペレーショナルテクノロジーアクション指向ランディングページのシステムプロパティを設定します

必要に応じてプロパティを有効にできるように、オペレーショナルテクノロジー (OT) アクション指向ランディングページのシステムプロパティを設定します。

始める前に

必要なロール:configure_industrial_workspace

手順

1. 移動先 **すべて > 産業用ワークスペースアドミン > ワークスペースのシステムプロパティ**。
2. 必要に応じて、次のプロパティを編集します。

システムプロパティ	説明
OT ホーム (アクション指向ランディングページ) システムプロパティ	
sn_mfg_common.landing_page_important_actions_limit	OT アクション指向ランディングページの [重要なアクション] セクションでフェッチされる重要なアクションの最大数。デフォルトは 50 です。

3. **[Save (保存)]** を選択します。

オペレーショナルテクノロジー進捗状況スコアカードの設定

産業用 ワークスペースにオペレーショナルテクノロジー (OT) 進捗状況スコアカードを設定して、ユーザーがサイトのデータと進捗状況と比較できるようにします。

次の表に、OT 進捗スコアカードの ガイド付きセットアップ タスクとその目的を示します。

OT 進捗状況スコアカードセットアップタスク

タスク	目的
1. OT 進捗スコアカードのロールをアサインします。	OT 進捗スコアカードのロールをユーザーにアサインして、OT 進捗スコアカードの機能とデータへのアクセスを制御できるようにします。
2. 完全性スコアの計算を検証します。	OT 進捗状況スコアカードに OT デバイスデータの完全性 (%) インジケータを含める場合は、 CMDB ヘルスダッシュボード・完全性スコア計算がアクティブ化されて実行されていることを検証します。
3. [オプション] インジケータソースを確認します。	多数のレコードのインジケータソースをレビューします。デフォルト値の合計レコード数 100 万を超えることが予想される場合は、レコードコレクションを上書きする必要があります。
4. サイトに想定される OT デバイスを構成します。	OT 進捗状況スコアカードの CMDB で予想される OT デバイスの割合 (%) インジケータを使用できるように、サイトの予想される OT デバイスの数を構成します。
5. [PA OTPSC] 月次データコレクションジョブを完了します。	[OT 進捗状況スコアカード] タブの パフォーマンスアナリティクス から、すべてのインジケータの日次データを収集して表示します。他のユーザーがこのタブでデータを表示する前に、この手順を完了する必要があります。
6. OT 進捗状況スコアカードインジケータを設定します。	各インジケータの表示がニーズを満たすように、OT 進捗状況スコアカードインジケータを構成します。
7. OT 進捗スコアカードのシステムプロパティを設定します。	OT 進捗状況スコアカードに表示されるしきい値と、計算されたスコアを決定するために使用されるコンポーネントを構成します。
8. モジュール名をカスタマイズします。	OT 進捗状況スコアカードのモジュール名をカスタマイズして、名前をデフォルト値からニーズにより適した名前に変更します。

オペレーショナルテクノロジー進捗状況スコアカードのロールをアサインする

オペレーショナルテクノロジー (OT) 進捗スコアカードのロールをユーザーにアサインして、OT 進捗スコアカードの機能、機能、およびデータへのアクセスを制御できるようにします。

始める前に

必要なロール：admin

このタスクについて

次の表にリストされているロールを持つユーザーは、OT 進捗状況スコアカードを使用できます。

OT 進捗状況スコアカードロール

ロール	説明
OT 進捗状況スコアカードビューアー [ot_progress_scorecard_viewer]	すべてのサイトデータが利用可能な OT 進捗状況スコアカードを表示できます。

OT 進捗状況スコアカードロール (続く)

ロール	説明
OT 進捗状況スコアカードエディター [ot_progress_scorecard_editor]	すべてのサイトデータが利用可能な OT 進捗状況スコアカードを表示および編集できます。

手順

ServiceNow AI Platform ユーザー管理機能を使用して、ユーザーとグループにロールをアサインします。

タスク	ユーザー管理機能
ユーザーへのロールのアサイン	ユーザーへのロールの割り当て を参照してください。
グループへのロールのアサイン	グループへのロールのアサイン を参照してください。

完全性スコア計算の検証

オペレーショナルテクノロジー (OT) 進捗状況スコアカードに **OT** デバイスデータの完全性 (%) インジケーターを含める場合は、[**CMDB** ヘルスダッシュボード - 完全性スコアの計算] がアクティブ化されて実行されていることを検証します。

始める前に

必要なロール：admin

手順

1. 移動先 **すべて > 産業用ワークスペースアドミン > ガイド付きセットアップ**.
2. [**Industrial Workspace**] セクションで、[**OT 進捗状況スコアカード**] を選択します。
3. [完全性スコア計算の検証] タスクで、[**構成**] を選択します。
4. **CMDB** ヘルスダッシュボード - 完全性スコア計算スケジュール済みスクリプト実行レコードで、次のアイテムを検証します。
 - a. [**アクティブ**] チェックボックスがオンになっていることを検証します。
 - b. 月末のレポート用に正確なスコアが収集されるようにするには、[**実行**] フィールドが構成されていることを検証します
5. [**Update (更新)**] を選択します。

完全性の計算方法の詳細については、[CMDB ヘルス KPI とメトリクス](#) の「完全性」セクションを参照してください。

多数のレコードのインジケーターソースを確認する

多数のレコードが必要な場合は、インジケーターソースを確認してください。レコード収集を上書きして、オペレーショナルテクノロジー (OT) 進捗状況スコアカードにデフォルト値の 100 万件よりも多くのレコードが表示されるようにすることができます。

始める前に

必要なロール：admin

このタスクについて

パフォーマンスアナリティクスを伴う移行のため、OT 進捗状況スコアカードの各インジケータにはデフォルトで 100 万件のレコードのみを表示できます。admin ロールを持っていて、[PA OTPSC] 月次データ収集を実行した後にレコード数が 100 万件を超えた場合は、ジョブログに誘導するエラーメッセージが表示されます。

- 注: admin ロールがなく、[PA OTPSC] 月次データコレクションジョブを実行した後にレコード数が 100 万件を超えた場合は、アドミニストレーターに問い合わせるよう指示するエラーメッセージが表示されます。

admin ロールを持っている場合は、エラーメッセージ内のリンクからジョブログ関連リストを確認し、情報をフィルタリングして、エラーが発生しているインジケータースソースを確認できます。エラーのあるインジケータースソースを見つけたら、多数のレコードのインジケータースソースを変更して、インジケータースソースデータを上書きすることができます。その後、他のユーザーにはエラーメッセージが表示されなくなり、インジケータースソースのデータが表示されます。インジケータースソースの詳細については、「[インジケータースソース](#)」を参照してください。

- 注: 新しいインジケータースソースを作成する必要がある場合は、Industrial Workspace Common に含まれるサイトブレイクダウンを使用する必要があります。オペレーショナルテクノロジーマネージャー アプリケーションのサイトブレイクダウン部分は廃止されました。

ジョブログには、インジケータースソースに関するものではないエラーが含まれている場合があります。[レベル] 列でジョブログレコードをフィルタリングし、インジケータースソースに関するエラーメッセージを見つける必要があります。

手順

- 移動先 **すべて > パフォーマンスアナリティクス > ソース > インジケータースソース**。
- フィルターを適用するには、[フィルターを表示/非表示] アイコンを選択し、次のフィルターを追加します。
[アプリケーション][次の値に等しい][産業用ワークスペース共通]
- 変更する必要があるインジケータースソースレコードを選択します。
どのインジケータースソースを調整する必要があるかは、エラーメッセージのジョブ ログ リンクで確認できます。
- [レコード収集] タブで、[レコード収集を上書き] フィールドの横にあるチェックボックスをオンにします。
- [フェッチされるレコードの最大数] フィールドで、値を XM に変更します。
- [Update (更新)] を選択します。

サイトに想定される OT デバイスの構成

OT 進捗状況スコアカードの **CMDB** で予想される OT デバイスの割合 (%) インジケータースソースを使用できるように、サイトの予想される OT デバイスの数を構成します。

始める前に

必要なロール: ユーザー基準で関連するサイトにアサインされたサイトアクセス権を持つ
ot_progress_scorecard_editor と cmdb_ot_isa_viewer

- 注: ユーザー基準によるサイトアクセスの詳細については、「[のホームページ宛先ルールの確認 産業用 ワークスペース](#)」を参照してください。

手順

1. 移動先 **すべて > 産業用ワークスペースアドミン > OT 進捗状況スコアカード属性**.
2. サイトでレコードを作成する必要がある場合は、これらのアクションを完了します。
 - a. **[New (新規)]** を選択します。
 - b. **[サイト]** フィールドにサイトを追加します。
 - c. **[値]** フィールドに、そのサイトの予想される OT デバイスの数を追加します。

 注: この値には OT コントロールモジュールを含めないでください。
 - d. **[Save (保存)]** を選択します。
3. サイトにレコードが存在し、予想されるデバイスを変更する場合は、これらのアクションを完了します。
 - a. 編集するレコードを選択します。
 - b. **[値]** フィールドで、そのサイトの予想される OT デバイスの数を変更します。

 注: この値には OT コントロールモジュールを含めないでください。
 - c. **[Update (更新)]** を選択します。

オペレーショナルテクノロジー進捗状況スコアカードのデータ収集の構成

パフォーマンスアナリティクスからすべてのインジケーターの日次データを収集して表示できるように、オペレーショナルテクノロジー (OT) 進捗状況スコアカードのデータ収集を構成します。この構成により、OT データがスコアカードに正確に表示されるようになります。

始める前に

必要なロール: admin

このタスクについて

[PA OTPSC] 月次データコレクションジョブを実行しない場合、OT 進捗スコアカードに使用できるデータはありません。admin ロールを持っている場合は、ジョブを実行するように求める警告メッセージが表示されます。

-  注: admin ロールがない場合は、アドミニストレーターにサポートを求めるように求める警告メッセージが表示されます。

手順

1. 移動先 **すべて > データコレクター > パフォーマンスアナリティクス > ジョブ**。
OT 進捗状況スコアカードが表示されている場合は、エラーメッセージで **[ジョブを今すぐ実行]** を選択して、**[スケジュール設定済みデータ収集]** テーブルに移動します。
2. フィルターを適用するには、**[フィルターを表示/非表示]** ( アイコンを選択し、**[名前]** [次の値に等しい] **[[PA OTPSC] 月次データコレクション]** のフィルターを追加します。
3. ジョブパラメーターセクションの **アクティブ** フィールドの横にあるチェックボックスをオンにしてデータの収集を開始し、**時間** フィールドで時間をスケジュールします。
[今すぐ実行] ボタンを使用して、データを手動で収集できます。そうしないと、タブを表示したときにデータが表示されません。**[今すぐ実行]** ボタンは、ジョブを最初に実行するときのみ使用してください。この時点以降に収集されるデータは、スケジュールされた時刻に収集する必要があります。

4. デフォルトのスケジュール収集時間が有効かどうかを確認します。

デフォルトの時刻は毎月初めの 00:00:00 です。デフォルトの収集時間を変更する場合は、ジョブのアクティブ化後に変更できます。この変更については、必ずユーザーに通知してください。

結果

OT 進捗状況スコアカードに、ユーザーに適切なサイトデータが表示されるようになりました。

- i** 注: OT 進捗状況スコアカードは パフォーマンスアナリティクスを使用します。パフォーマンスアナリティクス スコアは 5 か月間のみ保存されます。スコアを保存し、サイトデータを 5 か月以上比較する場合は、 [パフォーマンスアナリティクス サブスクリプションのアクティブ化](#) をご覧ください。

しきい値、重み付け、および順序によるインジケータの構成

オペレーショナルテクノロジー (OT) 進捗状況スコアカードインジケータを構成して、各インジケータの表示がニーズを満たすようにします。

始める前に

必要なロール:ot_progress_scorecard_editor または configure_industrial_workspace

このタスクについて

次のインジケータを構成できます。

- 全体スコア (%)
- CMDB で予想される OT デバイスの割合 (%)
- 分類済み OT デバイス (%)
- アサイン済み OT デバイス (%)
- OT デバイスデータの完全性 (%)
- マッピングされた OT デバイス (%)
- バックアップされた OT デバイス (%)
- 承認された OT 変更要求 (%)
- OT コンテキストのある OT インシデント (%)

手順

1. 移動先 **すべて > 産業用ワークスペースアドミン > OT 進捗状況スコアカード構成**。
2. 編集するインジケータを選択します。
3. フォームで次のフィールドに入力します。

インジケータ構成フィールド

フィールド	説明
下限しきい値	インジケータが満たすことができる最も低いしきい値。
上限しきい値	インジケータが満たすことができる最大のしきい値。
重み付け	インジケータが全体的なスコアに寄与する合計重み付け。
順序	左から右への重要度に基づくインジケータのランク。

4. インジケータを表示する必要がない場合は、[アクティブ] フィールドの選択を解除します。

5. **[Update (更新)]** を選択します。

オペレーショナルテクノロジー進捗状況スコアカードのシステムプロパティを設定します

必要に応じてプロパティを有効にできるように、オペレーショナルテクノロジー (OT) 進捗状況スコアカードのシステムプロパティを設定します。

始める前に

必要なロール:configure_industrial_workspace

手順

1. 移動先 すべて > 産業用ワークスペースアドミン > ワークスペースのシステムプロパティ。

2. 必要に応じて、次のプロパティを編集します。

システムプロパティ	説明
OT 進捗状況スコアカード構成	
sn_mfg_common.otpsc.page_title	OT 進捗スコアカードに表示されるページタイトル。デフォルトは [OT 進捗状況スコアカード] です。
sn_mfg_common.otpsc.records_per_page	1 ページあたりに表示されるレコードの数です。デフォルトは 10 です。
sn_mfg_common.otpsc.low_threshold_color	OT 進捗スコアカードの下限しきい値を表す色。
sn_mfg_common.otpsc.medium_threshold_color	OT 進捗状況スコアカードで中程度のしきい値を表す色。
sn_mfg_common.otpsc.high_threshold_color	OT 進捗状況スコアカードの上限しきい値を表す色。

3. **[Save (保存)]** を選択します。

モジュール名をカスタマイズする

オペレーショナルテクノロジー (OT) 進捗状況スコアカードのモジュール名をカスタマイズして、その名前をデフォルト値からニーズにより適した名前に変更します。

始める前に

必要なロール: admin

手順

1. 移動先 すべて > 産業用ワークスペースアドミン > ガイド付きセットアップ。

2. **[Industrial Workspace (産業用ワークスペース)]** モジュールで、**[OT 進捗状況スコアカード (OT Progress Scorecard)]** セクションを選択します。

3. [オプション] モジュール名のカスタマイズタスク で、[構成] を選択します。

4. [値] フィールドで、「OT 進捗状況スコアカード」の「メッセージ」値をニーズに合った名前に編集します。

5. **[Update (更新)]** を選択します。

オペレーショナルテクノロジーヴィジビリティダッシュボードの設定

ガイド付きセットアップタスクを完了すると、組織のデータコレクション、インジケータリソース、およびフィルターを使用して、オペレーショナルテクノロジー (OT) ヴィジビリティダッシュボードの設定を開始できます。

OT ヴィジビリティダッシュボードのガイド付きセットアップにアクセスするには、すべて > 産業用ワークスペースアドミン > ガイド付きセットアップ をクリックし、[オペレーショナルテクノロジーマネージャー] の下にある [オペレーショナルテクノロジーヴィジビリティダッシュボード] セクションを選択します。

OT ヴィジビリティダッシュボードとそのコンテンツの詳細については、「[オペレーショナルテクノロジー ヴィジビリティダッシュボード](#)」を参照してください。

次の表は、ダッシュボードの設定に使用されるガイド付きセットアップタスクを示しています。

OT ヴィジビリティダッシュボードのガイド付きセットアップタスク

タスク	目的
1. OT デバイスの日次データコレクションジョブを完了します。	OT ヴィジビリティダッシュボードのパフォーマンスアナリティクスからすべてのインジケータの日次データを収集して表示します。他のユーザーがダッシュボードデータを表示する前に、この手順を完了する必要があります。
2. [オプション] インジケータソースを確認します。	多数のレコードのインジケータソースをレビューします。デフォルト値の合計レコード数 100 万を超えることが予想される場合は、レコードコレクションを上書きする必要があります。

オペレーショナルテクノロジー デバイスのデータ収集の設定

オペレーショナルテクノロジー (OT) デバイスのデータ収集を構成して、パフォーマンスアナリティクスからすべてのインジケータの日次データを収集して表示できるようにします。この構成により、OT データが OT ヴィジビリティダッシュボードに正確に表示されるようになります。

始める前に

必要なロール：admin

このタスクについて

OT デバイスの日次データコレクションジョブがまだ実行されていない場合は、OT ヴィジビリティダッシュボードで利用可能なデータがなく、最終更新日のタイムスタンプが非表示になります。admin ロールを持っている場合は、OT デバイスの日次データコレクションジョブを実行するように求める次の警告メッセージが表示されます。

ⓘ No Data is shown on the dashboard because the 'OT Devices Daily Data Collection' job has not been run yet. [Run job now](#)

i 注：admin ロールがない場合は、アドミニストレーターにサポートを求めるように求める警告メッセージが表示されます。

手順

1. 移動先 すべて > データコレクター > パフォーマンスアナリティクス > ジョブ。

OT ヴィジビリティダッシュボードを表示している場合は、エラーメッセージで [ジョブを今すぐ実行] を選択することで、[スケジュール設定済みデータ収集] テーブルに移動できます。

2. フィルターを適用するには、[フィルターを表示/非表示] ( アイコンを選択し、[名前][次の値に等しい][OT デバイスの日次データ収集] のフィルターを追加します。
3. ジョブパラメーターセクションの アクティブ フィールドの横にあるチェックボックスをオンにしてデータの収集を開始し、時間 フィールドで時間をスケジュールします。
[今すぐ実行] ボタンを使用して、データを手動で収集できます。そうしないと、ダッシュボードを表示したときにデータが表示されません。[今すぐ実行] ボタンは、ジョブを最初に行うときにのみ使用してください。この時点以降に収集されるデータは、スケジュールされた時刻に収集する必要があります。
4. デフォルトのスケジュール収集時間が有効かどうかを確認します。
デフォルトの時刻は毎日 00:00:00 です。デフォルトの収集時間を変更する場合は、ジョブのアクティブ化後に変更できます。この変更については、必ずユーザーに通知してください。

結果

OT ヴィジビリティダッシュボードに、ユーザーのために収集された OT デバイスの正しいデータが表示されるようになりました。

次のタスク

これで、インジケータソースを確認し、デフォルトのレコードコレクションを上書きする必要がありますかどうかを判断できます。詳細については、「[多数のレコードのインジケータソースを確認する](#)」を参照してください。

多数のレコードのインジケータソースを確認する

多数のレコードが必要な場合は、インジケータソースを確認してください。レコードコレクションを上書きして、オペレーショナルテクノロジー (OT) ヴィジビリティダッシュボードにデフォルト値の 100 万を超えるレコードが表示されるようにすることができます。

始める前に

必要なロール: admin

このタスクについて

パフォーマンスアナリティクスを伴う移行のため、OT ヴィジビリティダッシュボードの各インジケータにはデフォルトで 100 万件のレコードのみを表示できます。admin ロールを持っていて、OT デバイスの日次データコレクションジョブを実行した後にレコード数が 100 万件を超えた場合、エラーメッセージが表示され、ジョブログが表示されます。

-  **注:** アドミンロールがなく、OT デバイスの日次データコレクションジョブを実行した後にレコード数が 100 万件を超えた場合は、アドミニストレーターに問い合わせるよう指示するエラーメッセージが表示されます。

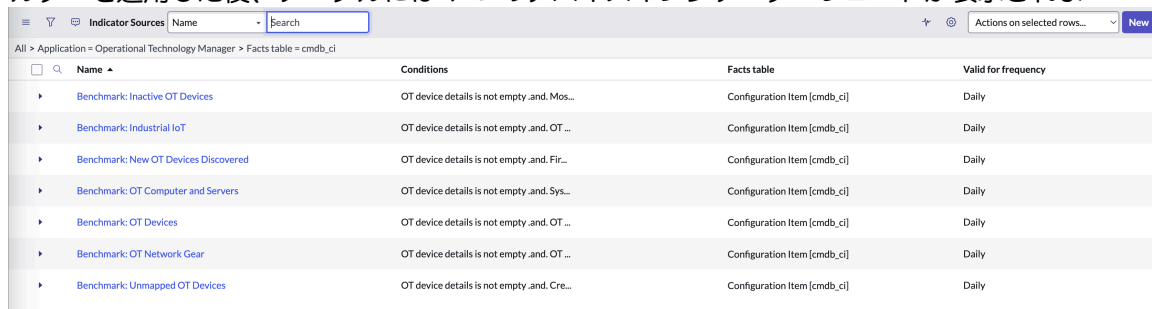
admin ロールを持っている場合は、エラーメッセージ内のリンクからジョブログ関連リストを確認し、情報をフィルタリングして、エラーが発生しているインジケータソースを確認できます。エラーのあるインジケータソースを見つけたら、多数のレコードのインジケータソースを変更して、インジケータソースデータを上書きすることができます。その後、他のユーザーにはエラーメッセージが表示されなくなり、インジケータソースのデータが表示されます。インジケータソースの詳細については、「[インジケータソース](#)」を参照してください。

-  **注:** 新しいインジケータを作成する必要がある場合は、Industrial Workspace Common に含まれるサイトブレイクダウンを使用する必要があります。オペレーショナルテクノロジーマネージャー アプリケーションのサイトブレイクダウン部分は廃止されました。

ジョブログには、インジケータソースに関するものではないエラーが含まれている場合があります。インジケータソースに関するエラーメッセージを見つけるには、ジョブ ログ レコードを [レベル] 列でフィルタリングする必要があります。

手順

1. 移動先 **すべて > パフォーマンスアナリティクス > ソース > インジケーターソース**.
2. フィルターを適用するには、[フィルターを表示/非表示]  アイコンを選択し、次のフィルターを追加します。
 - [アプリケーション][次の値に等しい][オペレーショナルテクノロジーマネージャー]
 - [ファクトテーブル][次の値に等しい][cmdb_ci]
 フィルターを適用した後、テーブルには 7 つのデバイスインジケーターレコードが表示されま



Name	Conditions	Facts table	Valid for frequency
Benchmark: Inactive OT Devices	OT device details is not empty and. Mos...	Configuration Item [cmdb_ci]	Daily
Benchmark: Industrial IoT	OT device details is not empty and. OT ...	Configuration Item [cmdb_ci]	Daily
Benchmark: New OT Devices Discovered	OT device details is not empty and. Fir...	Configuration Item [cmdb_ci]	Daily
Benchmark: OT Computer and Servers	OT device details is not empty and. Sys...	Configuration Item [cmdb_ci]	Daily
Benchmark: OT Devices	OT device details is not empty and. OT ...	Configuration Item [cmdb_ci]	Daily
Benchmark: OT Network Gear	OT device details is not empty and. OT ...	Configuration Item [cmdb_ci]	Daily
Benchmark: Unmapped OT Devices	OT device details is not empty and. Cre...	Configuration Item [cmdb_ci]	Daily

3. 変更する必要があるインジケーターソースレコードを選択します。
どのインジケーター ソースを調整する必要があるかは、エラー メッセージのジョブ ログ リンクで確認できます。
4. [レコード収集] タブで、[レコード収集を上書き] フィールドの横にあるチェックボックスをオンにします。
5. [フェッチされるレコードの最大数] フィールドで、値を XM に変更します。
6. [Update (更新)] を選択します。

オペレーショナルテクノロジー脆弱性対応 (PA) ダッシュボードの設定

ユーザーが重要なタスクにアクセスできるように、産業用 ワークスペースに オペレーショナルテクノロジー脆弱性対応 (PA) ダッシュボードを設定します。

次の表に、オペレーショナルテクノロジー脆弱性対応 (PA) ダッシュボードのガイド付きセットアップタスクとその目的を示します。

オペレーショナルテクノロジー脆弱性対応 (PA) ダッシュボードのセットアップタスク

タスク	目的
1. データ収集ジョブを構成します。	OTVR (PA) ダッシュボードの パフォーマンスアナリティクス からすべてのインジケーターの日次データを収集して表示します。他のユーザーがこのタブでデータを表示する前に、この手順を完了する必要があります。
2. [オプション] インジケーターソースを確認します。	多数のレコードのインジケーターソースをレビューします。デフォルト値の合計レコード数 100 万を超えることが予想される場合は、レコードコレクションを上書きする必要があります。

オペレーショナルテクノロジー脆弱性対応 (PA) ダッシュボードのデータ収集の構成

オペレーショナルテクノロジー脆弱性対応 (PA) ダッシュボードに表示されるデータのデータ収集を構成します。スケジュール済みジョブは、特定の時間または繰り返しスケジュールで実行できる自動化された作業です。

始める前に
必要なロール：admin

手順

1. 移動先 すべて > データコレクター > パフォーマンスアナリティクス > ジョブ。
2. フィルターを表示するには、[フィルターを表示/非表示] ( アイコンを選択し、次のフィルターを追加します。
 - [アプリケーション][次の値に等しい][オペレーショナルテクノロジー脆弱性対応]
 - [クラス][次の値に等しい][スケジュールされたデータ収集]
 フィルターを適用すると、次のスケジュール済みジョブが表示されます。
 - [PA OT VR]履歴脆弱性データの収集

注： [PA OT VR] 履歴脆弱性データコレクションジョブは、一度だけ実行する必要があるオンデマンドジョブです。履歴データが収集された後、日次データコレクションジョブは毎日スケジュールされた時刻に実行されます。履歴データの詳細については、「[履歴データの収集](#)」を参照してください。

 - [PA OT VR]修復タスクの日次収集
 - [PA OT VR]脆弱性一致アイテム 1 の日次収集
 - [PA OT VR]脆弱性一致アイテム 2 の日次収集
 - [PA OT VR]脆弱な構成アイテム (CI) の日次収集
3. データの収集を開始するには、スケジュール済みジョブレコードを選択します。
4. ジョブパラメーターセクションの アクティブ フィールドの横にあるチェックボックスをオンにし、時間 フィールドで時間をスケジュールします。
[今すぐ実行] ボタンを使用して、データを手動で収集できます。そうしないと、タブを表示したときにデータが表示されません。[今すぐ実行] ボタンは、ジョブを最初に実行するときのみ使用してください。この時点以降に収集されるデータは、スケジュールされた時刻に収集する必要があります。
5. デフォルトのスケジュール収集時間が有効かどうかを確認します。
デフォルトの時刻は毎日 00:00:00 です。デフォルトの収集時間を変更する場合は、ジョブのアクティブ化後に変更できます。この変更については、必ずユーザーに通知してください。
6. スケジュール済みジョブごとに手順 3 ～ 5 を繰り返します。

結果

オペレーショナルテクノロジー脆弱性対応 (PA) ダッシュボードに、ユーザーに適切なデータが表示されるようになりました。

次のタスク

これで、インジケータソースを確認し、デフォルトのレコードコレクションを上書きする必要があるかどうかを判断できます。詳細については、「[多数のレコードのインジケータソースを確認する](#)」を参照してください。

多数のレコードのインジケータソースを確認する

インジケータソースから 100 万件を超えるレコードが収集されることが予想される場合は、インジケータソースを確認して更新し、予想されるレコード数を上書きします。このアクションは、産業用 ワークスペースのデータを収集する際のシステムパフォーマンスの問題を回避するのに役立ちます。

始める前に
必要なロール：admin

手順

1. 移動先 すべて > パフォーマンスアナリティクス > インジケーター > インジケーター (自動).
2. [アプリケーション] [次の値に等しい] [オペレーショナルテクノロジー脆弱性対応] フィルターを適用します。
3. [インジケーター ソース] 列で、編集するインジケーター ソース レコードを選択します。
4. [レコード収集] セクションで、[レコード収集を上書き] フィールドの横にあるチェックボックスをオンにします。
5. [フェッチされるレコードの最大数] フィールドに、デフォルト値の 100 万レコードより大きい数を追加します。
たとえば、**200** 万です。
6. [Update (更新)] を選択します。

オペレーショナルテクノロジー統一マップエクスペリエンスの設定

ユーザーが統一マップにアクセスできるように、産業用ワークスペース で オペレーショナルテクノロジー (OT) 統一マップエクスペリエンスを設定します。

次の表に、OT 統一マップエクスペリエンスの ガイド付きセットアップ タスクとその目的を示します。admin ロールが必要です。

- i** 注：これらの ガイド付きセットアップ タスクは、利用可能な構成識別子のデフォルト設定を変更するため、完了するためのオプションです。

これらの構成識別子の設定は、すべてのユーザーに影響します。個々のユーザーが設定を構成することはできません。

OT 統一マップエクスペリエンスのセットアップタスク

タスク	目的
Industrial Workspace 構成識別子のデフォルト設定を変更します。	産業用ワークスペース構成識別子の次のデフォルト設定を変更して、OT 統一マップエクスペリエンスを構成します。 • ワークスペース構成プロパティ • ノードマッププロファイル • ノードマップの関連アイテム • 運用ライフサイクルのモード • テーブル属性

オペレーショナルテクノロジー統一マップエクスペリエンスのデフォルト設定

オペレーショナルテクノロジー (OT) 統一マップエクスペリエンスで利用可能なデフォルト設定を変更できます。

admin ロールを使用すると、OT 統一マップエクスペリエンスで利用可能な産業用ワークスペース構成識別子のデフォルト設定を変更できます。構成識別子または構成識別子は、構成識別子フレームワーク内の構成要素です。構成識別子には、ワークスペースなどの UX アプリケーションで使用される設定とテーブル駆動構成が含まれています。

プロパティが設定されていない場合、またはテーブル駆動構成にエントリがない場合、ルックアップでは代わりにデフォルトの構成識別子の値が使用されます。構成識別子フレームワークの詳細については、「[構成識別子フレームワーク](#)」を参照してください。

Industrial Workspace 構成識別子レコードにアクセスするには、[すべて] に移動し、フィルターバーに「sn_cmdb_ws_config_identifier.list」と入力します。次に、[産業用ワークスペース構成識別子] を選択します。

次のセクションでは、Industrial Workspace 構成識別子で変更できるデフォルト設定について説明します。

- 注:** ここで説明する設定は、すべてのユーザーに影響します。個々のユーザーが設定を構成することはできません。

ワークスペースの構成プロパティ

デフォルトでは、次の構成プロパティが sn_cmdb_ws_config_property.list に一覧表示され、デフォルトの構成識別子に割り当てられます。

- unifiedmap.map_search.max_nodes
- unifiedmap.map_search_filter.default_levels
- unifiedmap.map_search_filter.max_levels
- unifiedmap.map_search_filter.endpoint_deduplication_fields

ノードマッププロファイル

クラスのデフォルトのマップフィルターとデフォルトのマップの向きを設定するプロファイルを構成できます。たとえば、マップ済みアプリケーションサービスクラスのサービスマッピングデータを表示する場合などです。

これらのクラスプロファイルは、特定の構成アイテム (CI) ノードの統一マップに表示されるレイヤーを識別するのに役立ちます。クラスプロファイルは、現在のマップでフィルタープリセットが使用されていない場合に適用されます。このアプリケーションは通常、フィルタープリセットなしでマップを最初にロードしたとき、またはフィルタープリセットをデフォルトビューに設定したときに発生します。

クラスプロファイルでは、フィルターパネルの レイヤー カテゴリのみを構成できます。

ノードマップ参照

マップ参照を使用すると、関係性で接続されていない 2 つのクラスの CI 間をマップ上で接続できます。

ノードマップの関連アイテム

統一マップの [関連アイテム] モジュールを使用して、アクティブなインシデントやアクティブな問題など、CI に表示される関連アイテムカテゴリを設定できます。[関連アイテム] モジュールを選択すると、関連アイテムがコンテキストサイドパネルでカテゴリ別にグループ化されます。

運用ライフサイクルのモード

CI が統一マップに含まれるために必要な運用状況を指定できます。

テーブル属性

各クラスには、CI の [統一マップ属性] パネルに表示される一意の拡張プロパティのセットがあります。多くの共通クラスは、これらのプロパティで事前設定されています。デフォルト設定を変更し、追加のクラスの拡張プロパティをグローバルに構成できます。

ガイド付きセットアップを使用したオペレーショナルテクノロジーデバイスのハードウェア脆弱性アセスメント設定

産業用ワークスペースアドミン uided セットアップを使用して、産業用ワークスペースメニューで利用できるハードウェア脆弱性アセスメント機能を構成する手順を説明します。

始める前に

必要なロール：admin

このタスクについて

産業用ワークスペースアドミンガイド付きセットアップを使用して、必要なユーザーロールを割り当て、システムプロパティを設定し、オペレーショナルテクノロジーデバイスのハードウェア脆弱性アセスメントを実行するジョブをスケジュールします。

手順

1. 移動先 **すべて** > **産業用ワークスペースアドミン** > **ガイド付きセットアップ** > **オペレーショナルテクノロジー脆弱性対応**。
2. オペレーショナルテクノロジー脆弱性対応 アプリケーションで **[開始]** を選択します。
3. ハードウェア脆弱性アセスメントタスクを選択します。
4. 次のタスクタブを選択し、**[構成]** を選択して構成タスクを完了します。

タスク	目的
ユーザーロールのアサイン	ユーザーまたはユーザーグループに、ハードウェア脆弱性アセスメント 機能を使用できるようにするロールをアサインします。
NVD 統合のインストールと実行	脆弱性情報データベース (NVD) 統合を実行して NIST NVD データベースからデータをインポートし、ご使用の環境で見つかった CVE の重大度と詳細を判断できるようにします。
脆弱性アセスメントプロパティの構成	OT デバイスのハードウェア脆弱性アセスメントを実行するために必要なプロパティを構成します。
脆弱性アセスメントジョブをスケジュール	インベントリ内の OT デバイスの脆弱性アセスメントを有効にするスケジュール済みジョブを実行し 期限切れのアセスメント 削除する必要がある) をマークします。
正規化のオプトイン	ServiceNow 資産管理コンテンツサービスのファームウェアディスカバリーモデルの オプトインオプションを選択して、OT デバイスの正規化されていないファームウェアの詳細を収集し、正規化されたコンテンツライブラリを更新します。このプロセスにより、CVE への正規化されたデータマッピングの比率が向上し、脆弱性の評価が向上します。
使用停止アセスメントを削除	古いアセスメントや期限切れのアセスメントが削除されるまでの期間を設定します。

関連トピック

[ガイド付きセットアップ](#)

[オペレーショナルテクノロジー ハードウェア脆弱性アセスメント](#)

へのロールのアサイン ハードウェア脆弱性アセスメント

ユーザーにロールをアサインして、プロパティを構成し、ハードウェア脆弱性アセスメントの機能、能力、およびデータを使用できるようにします。

始める前に

必要なロール：admin

このタスクについて

次の表にリストされているユーザーおよびユーザーグループ、またはハードウェア脆弱性アナリストユーザーまたはユーザーグループに、次のロールをアサインします。

ハードウェア脆弱性アセスメントのロール

ロール	説明
[sn_vul.manage_exposure_assessment]	ハードウェア脆弱性アセスメントのプロパティを表示または編集できます。
OT 脆弱性イベントマネージャー [sn_otvr.vul_event_manager]	ハードウェア脆弱性アセスメントに関連するアセスメントを表示および実行できます。

手順

1. 移動先 **すべて > 産業用ワークスペースアドミン > ガイド付きセットアップ > オペレーショナルテクノロジー脆弱性対応 > ハードウェア脆弱性アセスメント > ユーザーロールのアサインの構成 > 構成**.
または、 **ユーザーロールのアサイン > 構成 > ユーザー**.
2. ServiceNow AI Platform ユーザー管理機能を使用して、ユーザーとグループにロールをアサインします。

タスク	ユーザー管理機能
ユーザーへのロールのアサイン	ユーザーへのロールの割り当て を参照してください。
グループへのロールのアサイン	グループへのロールのアサイン を参照してください。

の NVD 統合を実行 ハードウェア脆弱性アセスメント

脆弱性情報データベース (NVD) 統合をインストールして実行し、ハードウェア脆弱性アセスメントを実行します。

始める前に

必要なロール:sn_otvr.vul_event_manager および admin

このタスクについて

ハードウェア脆弱性アセスメント は、脆弱性対応 の脆弱性アセスメント機能に基づいています。NVD データベースの共通脆弱性識別子 (CVE) データにアクセスするには、HVA NVD 統合を実行する必要があります。

さまざまな NVD 統合とその仕組みを理解するには、以下を参照してください。

- [NVD 統合の概要](#)
- [脆弱性対応 Integration with the NIST National Vulnerability Database のインストール](#)

手順

1. 移動先 **すべて > 産業用ワークスペースアドミン > ガイド付きセットアップ > オペレーショナルテクノロジー脆弱性対応 > ハードウェア脆弱性アセスメント > NVD 統合のインストールと実行の構成 > 構成**.
または、 **すべて > 脆弱性対応 > アドミニストレーション > 統合**

2. 次の NVD 統合をインストールして実行します。

- *NIST National Vulnerability Database Integration-API (CVE only)*
- *NIST National Vulnerability Database Integration-API (CPE only)*
- *NIST National Vulnerability Database Integration-API (Unmapped CPE)*

ハードウェア脆弱性アセスメントのプロパティの設定

ハードウェア脆弱性アセスメントを実行するために必要なプロパティを設定します。

始める前に

必要なロール:sn_vul.manage_exposure_assessment および admin

手順

1. 移動先 **すべて > 産業用ワークスペースアドミン > ガイド付きセットアップ > オペレーショナルテクノロジー脆弱性対応 > ハードウェア脆弱性アセスメント > 脆弱性アセスメントプロパティの構成 > 構成 > 脆弱性アセスメント**.
または、 **すべて > 脆弱性対応 > アドミニストレーション > プロパティ > 脆弱性アセスメント**.
2. 次の構成を実行します。

プロパティ	説明
sn_vul_analyst.auto_create_vits:このプロパティは、完全に一致したハードウェア脆弱性アセスメントに対して新しい脆弱性一致アイテムレコードを自動的に作成するかどうかを決定します。true に設定すると、完全に一致したハードウェア脆弱性アセスメントに対して新しい脆弱性一致アイテムレコードが自動的に作成されます。	[はい] を選択します。 デフォルト値は [はい] です。[はい] を選択すると、完全に一致したハードウェア脆弱性アセスメントに対して新しい脆弱性一致アイテムレコードが自動的に作成されます。 脆弱性一致アイテム (VIT) を手動で作成する場合は、選択を解除します。
sn_vul_analyst.assess_unmapped_disc_models:このプロパティを有効にすると、アセスメントに CPE マッピングのないディスカバリーモデルが含まれます。	デフォルト値は [なし] です。 CPE マッピングされていない OT デバイスのディスカバリーモデルの脆弱性アセスメントを実行するには、[はい] を選択します。
hva_confidence_score_threshold :このプロパティは、脆弱性アセスメントの作成に必要な最小信頼スコアしきい値を制御します。スコアがこのしきい値以上の一致のみで、脆弱性アセスメントが生成されます。しきい値は、0.0 ~	要件に応じて値を編集します。 デフォルト値は 0.75 です。 i 注: 信頼スコアの値は 0 に設定できません。ただし、信頼スコアが 0 のアセスメントは作成されません。

プロパティ	説明
1.0 の 10 進数である必要があります。デフォルト値 OOB は 0.75 です。	

3. [Save (保存)] を選択します。

スケジュール済みジョブを実行して実行する ハードウェア脆弱性アセスメント

スケジュール済みジョブを実行して、ハードウェア脆弱性アセスメントを実行します。

始める前に

必要なロール:sn_otvr.vul_event_manager および admin

このタスクについて

インベントリ内の OT デバイスのファームウェア脆弱性を検出するには、次のスケジュール済みジョブを実行する必要があります。

手順

1. 移動先 **すべて > 産業用ワークスペースアドミン > ガイド付きセットアップ > オペレーショナルテクノロジー脆弱性対応 > ハードウェア脆弱性アセスメント > スケジュール設定済みの脆弱性アセスメントジョブ > 構成 > スケジュール済みジョブ**。

重要:

- *Hardware Assessment - Delta*ジョブをスケジュールする前に、*Hardware Assessment - Full*を実行する必要があります。*Hardware Assessment - Full*はオンデマンドで実行できます。
- 毎日、毎週、または必要な頻度に従って *Hardware Assessment - Delta* ジョブを実行するようにスケジュールできます。

2. 選択 **ハードウェアアセスメント:完全 > 今すぐ実行**。

このジョブは、以前のアセスメントに関係なく、インベントリ内のすべての OT デバイスでアセスメントを実行し、ファームウェアの脆弱性を検出します。

3. 選択 **ハードウェアアセスメント:デルタ > アクティブ**。

[実行] を選択し、リストから頻度を選択します。ハードウェアアセスメント - デルタジョブは、選択した頻度に従って実行されます。

このジョブは、前回のアセスメント実行以降の変更または更新のみを対象に、増分アセスメントを実行します。ハードウェア脆弱性アセスメントの前回の正常な実行以降のファームウェア、正規化されたコンテンツ、および脆弱性の変更をキャプチャします。このジョブにより、継続的な監視とタイムリーな更新を維持できます。

4. 選択 **ハードウェア脆弱性アセスメント:期限切れのマークアセスメント > アクティブ** をクリックして、このジョブを開始します。

[実行] を選択し、リストから頻度を選択します。*Hardware Vulnerability Assessment - Mark Expired Assessments*ジョブは、選択した頻度に従って実行されます。

ハードウェア脆弱性評価は、デバイスで利用可能なファームウェアデータに基づいています。デバイスのファームウェアバージョンを更新すると、以前のファームウェアバージョンに基づく既存のアセスメントは無効になり、期限切れのアセスメントと見なされます。1 か月以上経過した期限切れのアセスメントは削除できます。ただし、ファームウェアバージョンが更新されたデバイスについては、新しい脆弱性アセスメントを実行する必要があります。

関連トピック

[スケジュール済みジョブ](#)

の正規化オプトインの構成 ハードウェア脆弱性アセスメント

ServiceNow 資産管理 コンテンツサービスの [ファームウェアディスカバリーモデルのオプトイン] オプションを選択して、オペレーショナルテクノロジー (OT) デバイスの正規化されていないファームウェアの詳細を収集し、正規化されたコンテンツライブラリを更新します。このプロセスにより、CVE への正規化されたデータマッピングの比率が向上し、脆弱性の評価が向上します。

始める前に

必要なロール:sn_eam.enterprise_admin または admin

手順

1. 移動先 **すべて > 産業用ワークスペースアドミン > ガイド付きセットアップ > オペレーショナルテクノロジー脆弱性対応 > ハードウェア脆弱性アセスメント > 正規化のオプトイン > 構成**.
2. [はい] を選択します。
3. [ファームウェアディスカバリーモデルの有効化] トグルボタン

関連トピック

[エンタープライズ資産管理コンテンツサービスへのオプトイン](#)

古いハードウェア脆弱性アセスメントや期限切れのハードウェア脆弱性アセスメントを削除する
古いアセスメントレコードや期限切れのアセスメントレコードの自動削除を設定します。

始める前に

必要なロール : admin

このタスクについて

クリーニングする古いアセスメントまたは期限切れのアセスメントの経過時間を設定します。

- 古いアセスメント:無視されている、または関連付けられている脆弱性一致アイテム (VIT) が 2 年以上クローズされている無効なアセスメント。
- 期限切れのアセスメント:デバイスのファームウェアバージョンを更新すると、以前のファームウェアバージョンに基づく既存のアセスメントは無効になり、期限切れのアセスメントと見なされます。1 か月以上経過した期限切れのアセスメントは削除できます。ただし、ファームウェアバージョンが更新されたデバイスについては、新しい脆弱性アセスメントを実行する必要があります。

手順

1. 移動先 **すべて > システムデータ管理 > データ管理ポリシー**.
2. **sn_vul_analyst_firmware_vulnerability_assessment**ポリシーを検索して選択します。
3. [アクティブ] チェックボックスをオンにして、要件に従ってクリーンアップルールを設定します。クリーンアップルール 1、2、および 3 で経過時間を設定します。この経過時間が経過すると、古いアセスメントや期限切れのアセスメントが削除されます。

- ルール 1:VIT が 2 年間クローズされているファームウェア脆弱性アセスメントを削除します (関連付けられている VIT の最終更新日に基づく)。
- ルール 2:2 年間 (作成日に基づく) 無視されているファームウェア脆弱性アセスメントを削除します。
- ルール 3:1 か月後に期限切れになったファームウェア脆弱性アセスメントを削除します (最終更新日に基づく)。

4. [Update (更新)] を選択します。

産業用 ワークスペース の使用

産業用ワークスペースに必要なすべてのセットアップタスクを完了すると、ユーザーは産業用ワークスペースで利用可能なさまざまなページとダッシュボードでオペレーショナルテクノロジーデータの管理を開始できます。

産業用ワークスペース ホームページ宛先ルール

アサインされたロールに応じて、ホームページ宛先ルールを含む 産業用 ワークスペース 内のさまざまなページにリダイレクトされます。これにより、必要なデータにより迅速かつ効率的にアクセスできるようになります。

ホームページ宛先ルールの概要

各宛先ルールは、アサインされた 1 つまたは複数のロールに基づいて、さまざまな OT ユーザーを産業用 ワークスペース 上のさまざまなページにリダイレクトします。一部のロールでは 1 つのページのデータにアクセスできない場合があるため、データを表示できるページにユーザーをリダイレクトすると、産業用 ワークスペースをより適切にナビゲートできます。たとえば、オペレーショナルテクノロジーエディター [cmdb_ot_editor] ロールのみを持つユーザーは、OT アクション指向ランディングページでデータを表示できないため、空のランディングページのみが表示されます。代わりに、該当する OT デバイスデータを表示できる産業用ワークスペースリストにリダイレクトされます。

産業用 ワークスペース ホームページ宛先ルールの説明

次の表に、産業用 ワークスペース ホームページの宛先ルールとその宛先を示します。

ホームページ宛先ルール

ルール	宛先	リダイレクトされるロール	説明
OT 進捗状況スコアカードページ	now/mfg/ot-progress-scorecard/ (OT 進捗スコアカード)	ot_progress_scorecard	OT 進捗スコアカードルールは、ルールに記述されたロールを持つユーザーがログインしたときに OT 進捗スコアカードに直接誘導します。
Industrial Workspace ホームページ	now/mfg/home (OT アクション指向ランディングページ)	- sn_ot_incident_read - sn_ot_change_read - sn_otvr.remediation_owner	Industrial Workspace ホームページルールは、ルールに記述されているロールを持つユーザーがログインしたときに、OT アクション指向ランディング

ホームページ宛先ルール (続く)

ルール	宛先	リダイレクトされるロール	説明
			ページに直接誘導します。
OT ダッシュボードライブラリページ	now/mfg/dashboard-library (OT ダッシュボードライブラリ)	cmdb_ot_viewer + cmdb_ot_isa_viewer	OT ダッシュボードライブラリページルールでは、ルールに記述されたロールを持つユーザーがログインすると、OT ヴィジビリティダッシュボードに直接誘導されます。 i 注: OT ダッシュボードライブラリページルールは、オペレーショナルテクノロジーマネージャー がインストールされている場合にのみ表示されます。
ISA 設備階層モデルページ	now/mfg/isa-equipment-model (設備モデルマネージャー)	cmdb_ot_isa_viewer	ISA 設備階層モデルページルールでは、ルールに記述されているロールを持つユーザーがログインすると、機器モデルマネージャーに直接誘導されます。 i 注: ISA 設備階層モデルページルールは、製造業プロセスマネージャー がインストールされている場合にのみ表示されます。
産業用ワークスペースリストページ	now/mfg/list (産業用ワークスペースリスト)	cmdb_ot_viewer	Industrial Workspace リストページルールでは、ルールに記述されているロールを持つユーザーがログインしたときに、Industrial Workspace リストに直接アクセスします。

でレコードを検索する 産業用ワークスペース

オペレーショナルテクノロジー (OT) データまたは構成管理データベース (CMDB)データに関連する産業用ワークスペース内のレコードを検索します。

始める前に

- この検索エクスペリエンスは、検索エンジンが AI 検索 のインスタンスにのみ適用されます。検索エンジンとして Zing を使用するインスタンスでは、検索エクスペリエンスが異なります。
- 必要なロール:cmdb_ot_viewer

このタスクについて

産業用ワークスペース検索は、各検索の 自然言語クエリー (NLQ) Genius 結果を表示するように構成されています。産業用ワークスペース での NLQ Genius 結果の使用の詳細については、「[NLQ で使用される Genius 結果 産業用ワークスペース](#)」を参照してください。NLQ Genius 結果の詳細については、「[NLQ Genius 結果](#)」を参照してください。

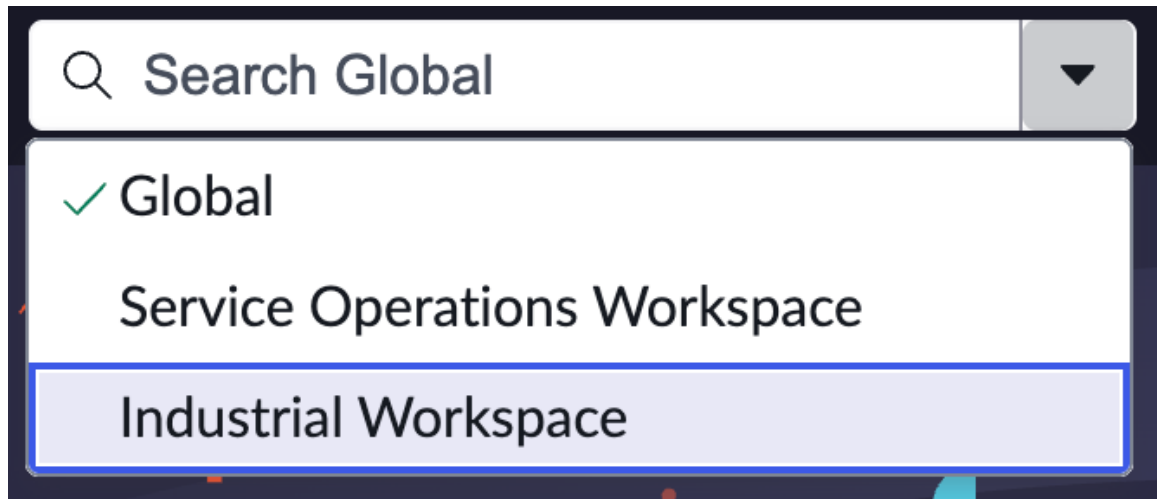
産業用ワークスペースの検索バーを使用すると、次のレコードの結果を検索して見つけることができます。

- IT インシデント
- OT インシデントおよびインシデントタスク
 - ❗ 注: OT インシデントレコードとインシデントタスクレコードは、オペレーショナルテクノロジーインシデント管理 がインストールされている場合にのみ使用できます。
- OT 変更および変更タスク
 - ❗ 注: OT 変更レコードおよび変更タスクレコードは、オペレーショナルテクノロジー変更管理 がインストールされている場合にのみ使用できます。
- カタログタスク
- ナレッジ
- ユーザー

手順

1. 移動先 **すべて** > 産業用ワークスペース.
2. 検索バーで、キーワードまたはレコード番号を使用してレコードを検索します。
3. 検索結果で、表示するレコードを選択します。
タブを選択しても返されたレコードにアクセスできない場合は、「結果なし」というメッセージが表示されます。
4. 産業用ワークスペースにいらなくても、産業用ワークスペース内のレコードを検索する場合は、次のアクションを実行します。

- a. 検索バーで、[検索コンテキストを選択] ( アイコン) を選択します。
- b. メニューから **[Industrial Workspace]** を選択します。



NLQ で使用される **Genius** 結果 産業用ワークスペース

産業用ワークスペースでは、検索ごとに 自然言語クエリー (NLQ) Genius 結果を活用します。

NLQ Genius 結果の概要

構成管理データベース (CMDB) テーブルを AI 検索でインデックス化することはできません。産業用ワークスペース検索は、各検索の NLQ Genius 結果を表示するように構成されており、これを使用して CMDB テーブルを検索できます。NLQ Genius 結果は NLQ 処理を使用して、検索クエリに一致するテーブルから関連する結果を表示します。

NLQ Genius 結果の詳細については、「[NLQ Genius 結果](#)」を参照してください。

OT CI の検索

NLQ Genius 結果を利用して、テーブルと列を指定することで、オペレーショナルテクノロジー (OT) 構成アイテム (CI) を検索できます。

次の表に、PLCのさまざまな情報を検索するための例を示します。検索する必要がある追加の列がある場合は、この一般的なパターンに従うことができます。

情報タイプ	検索入力
名前でPLCを検索する	PLC 名 <名前を挿入>
モデル ID で PLC を検索する	PLC モデル ID <モデル ID を挿入>
PLC を説明で検索する	PLCの説明<説明を挿入>
メーカーからPLCを検索	PLCメーカー<インサートメーカー>

のサイトフィルター 産業用ワークスペース

オペレーショナルテクノロジー (OT) ヴィジビリティダッシュボード、オペレーショナルテクノロジー脆弱性対応 (PA) ダッシュボード、および OT 脆弱性リスクロールアップダッシュボードのサイトフィルターを使用して、特定のサイトのデータを表示できます。

サイトフィルターを使用すると、次のダッシュボードに表示する OT デバイスまたは脆弱性データを指定できます。

- OT ヴィジビリティダッシュボード
- OTVR (PA) ダッシュボード
- OT 脆弱性リスクロールアップダッシュボード

サイトフィルターを使用するには、表示するサイトへのアクセス権を持つ **cmdb_ot_isa_viewer** ロールが必要です。

サイトフィルターを使用すると、次のアクションを実行できます。

- 特定のサイトを検索します。
- 1 つまたは複数のサイトの OT データを表示します。
- アサインされていないサイトの OT データを表示します。

i 注: OT デバイスにサイトがアサインされていない場合、フィルターには [サイトがアサインされていません] と表示されます。ダッシュボードに正しいサイトを表示するには、サイトにサイトを割り当ててから、そのサイトに事業部門を割り当てる必要があります。

サイトフィルターを使用

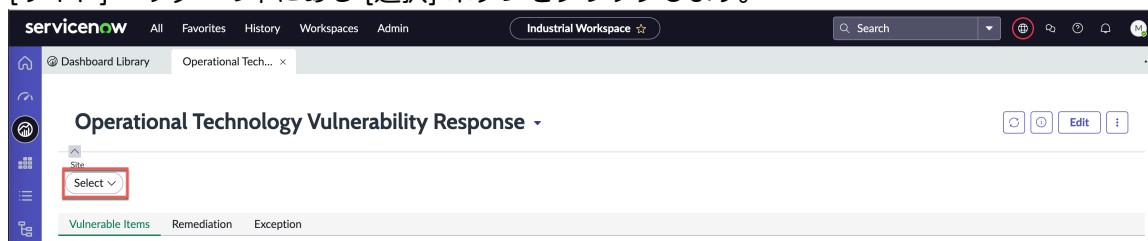
オペレーショナルテクノロジー (OT) ヴィジビリティダッシュボード、オペレーショナルテクノロジー脆弱性対応 (PA) ダッシュボード、および OT 脆弱性リスクロールアップダッシュボードのサイトを使用して、選択したサイトでデータをフィルタリングします。

始める前に

必要なロール: サイトアクセス権を持つ **cmdb_ot_isa_viewer**

手順

1. 移動先 **すべて > 産業用ワークスペース**.
2. [ダッシュボードライブラリ] アイコン () を選択します。
3. OT ヴィジビリティダッシュボードまたはオペレーショナルテクノロジー脆弱性対応ダッシュボードのいずれかを選択します。
4. [サイト] ヘッダーの下にある [選択] ボタンをクリックします。



5. オプション: 特定のサイトを検索するには、検索機能を使用します。
6. 1 つ以上のサイトをダッシュボードに適用するには、次のアクションを実行します。
 - a. [利用可能] 列で、データを表示する各サイトを選択します。
 - b. 選択したサイトを [適用済み] 列に移動するには、[選択したアイテムを移動] アイコン () をクリックします。

オペレーショナルテクノロジー 進捗状況スコアカードフィルター

オペレーショナルテクノロジー (OT) 進捗状況スコアカードのフィルターを使用して、スコアカードに表示するデータをサイト、事業部門 (BU)、または日付別に指定できます。

スコアカードフィルターの概要

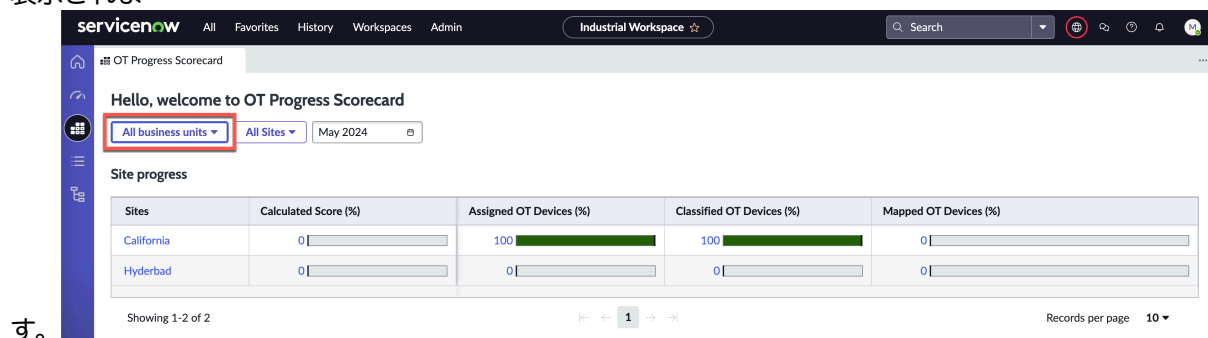
事業部門、サイト、および日付のフィルターを使用して、OT 進捗スコアカードに表示するスコアカードメトリクスを指定できます。1 つ以上の事業部門、それぞれのサイト、および特定の暦月でフィルタリングできます。

事業部門フィルター

事業部門 (BU) フィルターを使用すると、次のアクションを実行できます。

- すべての事業部門のスコアカードメトリクスを表示します。
- 特定の事業部門のスコアカードメトリクスを表示します。
- 複数の事業部門のスコアカードメトリクスを表示します。

デフォルトでは、次の例に示すように、スコアカードには利用可能なすべての BU のメトリクスが表示されま



す。

BU フィルターを設定すると、選択した BU に含まれるすべてのサイトのデータがスコアカードに表示されます。次に、次のセクションで説明する [すべてのサイト] メニューからサイトを選択できます。BU フィルターを変更して別の BU を選択すると、選択した BU に関連付けられているサイトのみが含まれるようにサイト フィルターが更新されます。

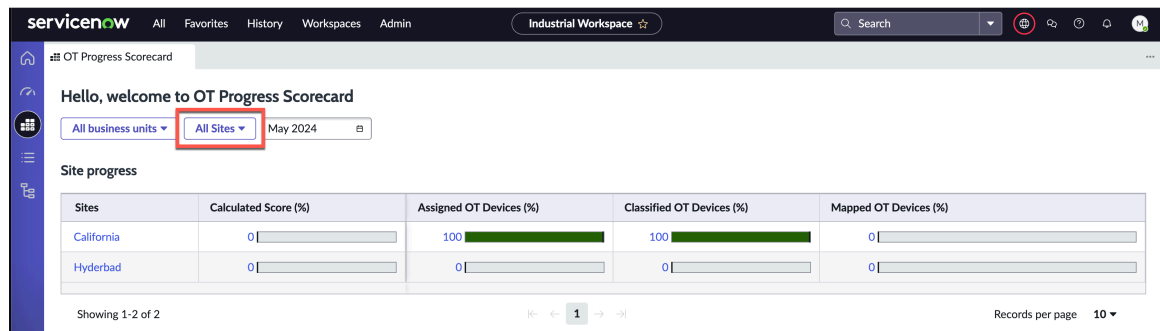
BU とサイト フィルターの使用方法の詳細については、「[オペレーショナルテクノロジー進捗状況スコアカードフィルターの使用](#)」を参照してください。

Site filter (サイトフィルター)

サイトフィルターを使用すると、次のアクションを実行できます。

- すべてのサイトのスコアカードメトリクスを表示します。
- 特定のサイトのスコアカードメトリクスを表示します。
- 複数のサイトのスコアカードメトリクスを表示します。

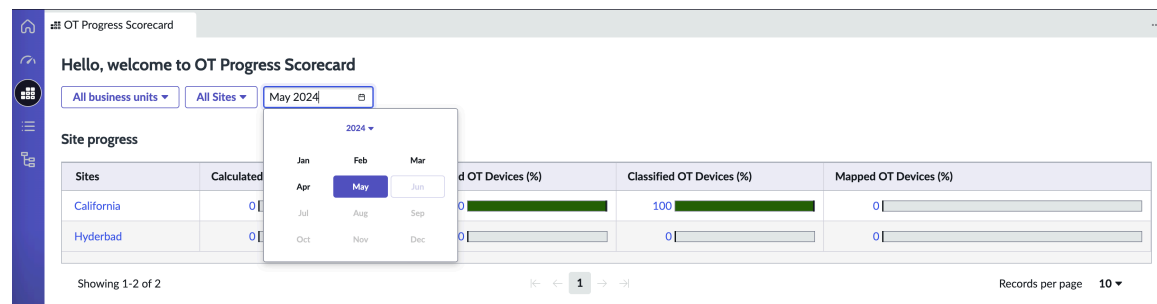
デフォルトでは、スコアカードには、次の例に示されているすべてのサイトのメトリクスが表示されます。



日付フィルター

日付フィルターを使用すると、選択した年の特定の暦月のスコアカードメトリクスを表示できます。デフォルトでは、スコアカードには前月と前の年のメトリクスが表示されます。

注: [PA OTPSC] 月次データコレクションジョブがまだ実行されていない場合、スコアカードにはスコア 0 と表示されます。[PA OTPSC] 月次データコレクションジョブの詳細については、「[オペレーショナルテクノロジー進捗状況スコアカードのデータ収集の構成](#)」を参照してください。



オペレーショナルテクノロジー進捗状況スコアカードフィルターの使用

オペレーショナルテクノロジー (OT) 進捗状況スコアカードの事業部門 (BU) とサイトフィルターを使用して、事業部門、サイト、または日付でデータをフィルタリングします。

始める前に

必要なロール：admin

手順

1. 移動先 **すべて > 産業用ワークスペース**.
2. OT 進捗状況スコアカードを開きます。
3. 1 つ以上の BU のスコアカードメトリクスを表示します。
 - a. ヘッダーで、[**すべての事業部門**] メニューを選択します。
 - b. リストから、データを表示する 1 つ以上の BU を選択します。検索機能を使用して、特定の BU を検索できます。
4. 1 つ以上のサイトのスコアカードメトリクスを表示します。

- a. ヘッダーで、[すべてのサイト] メニューを選択します。
- b. リストから、データを表示する 1 つ以上のサイトを選択します。

i 注: 検索機能を使用して、特定のサイトを検索できます。検索バーにサイトの名前またはショートコードを入力します。ショートコードは、サイトの略語です。

5. カレンダー日付のスコアカードメトリクスを表示します。

- a. ヘッダーで、カレンダー () アイコンを選択します。
- b. データの対象とする月と年を選択します。

オペレーショナルテクノロジー進捗状況スコアカードを昇順または降順でソートします

オペレーショナルテクノロジー (OT) 進捗状況スコアカードを昇順または降順でソートして、スコアカードの表示をカスタマイズします。

始める前に

必要なロール:ot_progress_scorecard_viewer

手順

1. 移動先 **すべて > 産業用ワークスペース**.
2. **[OT 進捗状況スコアカード]** アイコン () を選択します。
3. 昇順  順アイコン () を選択します。

結果

OT 進捗状況スコアカードが、昇順または降順で整理されるようになりました。ログアウトすると、ソート構成は次回ログイン時のために保存されます。

オペレーショナルテクノロジーアクション指向ランディングページでの重要なアクションの順序の構成

オペレーショナルテクノロジー (OT) アクション指向ランディングページで重要なアクションの順序を構成して、タスクの表示方法をカスタマイズします。

始める前に

必要なロール:cmdb_ot_viewer

手順

1. 移動先 **すべて > 産業用ワークスペース**.
2. **[ホーム]** () アイコン
3. **[重要なアクションを構成 (Configure )]** を選択します。
4. **[アイテムの並べ替え]** を選択します。
5. **[属性を選択]** フィールドで、重要なアクションをフィルタリングする属性を選択します。
[検索] フィールドを使用して、アクションをソートする属性を見つけることができます。
6. **[順序]** フィールドで、**[昇順]** または **[降順]** を選択します。

オペレーショナルテクノロジー脆弱性対応 (PA) ダッシュボードのインジケータースソースとインジケーター

オペレーショナルテクノロジー脆弱性対応 アプリケーションは、インジケータースソースとインジケーターを使用してデータを収集し、脆弱性修復の進捗状況を追跡します。

インジケータースソース

オペレーショナルテクノロジー脆弱性対応インジケーターは、次のインジケータースソースからデータを収集します。インジケーター ソースから 100 万件を超えるレコードが収集されることが予想される場合は、インジケーター ソースの [レコード収集] セクションで予想される数を上書きする必要があります。詳細については、「[多数のレコードのインジケータースソースを確認する](#)」を参照してください。

OTVI.New

sn_vul_vulnerable_itemテーブルを使用して、新しい OT 脆弱性一致アイテムを収集します。

OTVI.アクティブ

sn_vul_vulnerable_itemテーブルを使用し、OT システム内のすべてのアクティブな脆弱性一致アイテムを含めます。

OTVI.クローズ済み

sn_vul_vulnerable_itemテーブルを使用し、OT システム内のすべてのクローズ済み脆弱性一致アイテムを含みます。

OTRT.アクティブ

sn_vul_vulnerabilityテーブルを使用し、OT システム内のすべてのアクティブな修復タスクを含めます。

インジケーター

オペレーショナルテクノロジー脆弱性対応 アプリケーションの脆弱性修復の進捗状況を測定および追跡するために、いくつかのインジケーターが使用されます。

インジケーターの レコード収集 オプションは、オペレーショナルテクノロジー脆弱性対応 アプリケーションではデフォルトで無効になっています。このオプションは、各インジケーターの大量のデータを収集するときに発生する可能性のあるパフォーマンスの問題を回避するためにオフになっています。

OT 脆弱性一致アイテム

データソース OTVI の OT 脆弱性一致アイテムの数。アクティブ:sn_vul_vulnerable_itemテーブルを使用します。目標は、システム内の脆弱性一致アイテムの数を最小限に抑えることです。

重大な OT 脆弱性一致アイテム

データソース OTVI 上の OT の重大な脆弱性一致アイテムの数。アクティブ:sn_vul_vulnerable_itemテーブルを使用します。目標は、システム内の重大な脆弱性一致アイテムの数を最小限に抑えることです。

未アサインの OT 脆弱性一致アイテム

[アサイン先グループ] フィールドと [アサイン先] フィールドの両方が空であるすべてのアクティブな OT 脆弱性一致アイテム。目標は、未アサインの脆弱性一致アイテムの数を最小限に抑えることです。

クローズ済み OT 脆弱性一致アイテム

クローズ済み OT 脆弱性一致アイテムインジケータは、単位番号で毎日測定されます。目標は、システム内のクローズされた脆弱性一致アイテムの数を最大化することです。

保留された OT 脆弱性一致アイテム

データソース OTVI で保留された OT 脆弱性一致アイテムの数。アクティブ:sn_vul_vulnerable_itemテーブルを使用します。目標は、システム内で保留される脆弱性一致アイテムの数を最小限に抑えることです。

保留された重大な OT 脆弱性一致アイテム

データソース OTVI で保留された重大な OT 脆弱性一致アイテムの数。アクティブ:sn_vul_vulnerable_itemテーブルを使用します。目標は、保留される重大な脆弱性一致アイテムの数を最小限に抑えることです。

保留されていない期限切れの重大な OT 脆弱性一致アイテム

データソース OTVI の保留されていない期限切れの重大な脆弱性一致アイテムの数。アクティブ:sn_vul_vulnerable_itemテーブルを使用します。目標は、システム内の保留されていない期限切れの重大な脆弱性一致アイテムの数を最小限に抑えることです。

OT 修復タスク

データソース OTRT の OT 修復タスクの数。アクティブ:sn_vul_vulnerabilityテーブルを使用します。目標は、システム内の修復タスクの数を最小限に抑えることです。

保留されていない期限切れの重大な OT 修復タスク

データソース OTRT の保留されていない期限切れの重大な修復タスクの数。アクティブ:sn_vul_vulnerabilityテーブルを使用します。目標は、システム内の保留されていない期限切れの重大な修復タスクの数を最小限に抑えることです。

保留されていない OT 修復タスク

データソース OTRT の保留されていない OT 修復タスクの数。アクティブ:sn_vul_vulnerabilityテーブルを使用します。目標は、システム内の保留されていない修復タスクの数を最小限に抑えることです。

保留されていない重大な OT 修復タスク

データソース OTRT の保留されていない重大な OT 修復タスクの数。アクティブ:sn_vul_vulnerabilityテーブルを使用します。目標は、システム内の保留されていない重大な修復タスクの数を最小限に抑えることです。

未アサインの OT 修復タスク

[アサイン先グループ] と [アサイン先] フィールドの両方が空であるすべてのアクティブな修復タスク。目標は、システム内の未アサインの修復タスクの数を最小限に抑えることです。

修復ターゲットを満たした脆弱なアイテムの割合

$$\frac{([\text{クローズされた脆弱なアイテム} > \text{修正ターゲット} = \text{ターゲット達成}] / [\text{クローズされた脆弱なアイテム}]) * 100}{}$$

目標は、システム内の修復ターゲットを満たす脆弱性一致アイテムの割合を最大化することです。

OT 脆弱性一致アイテム平均修復時間

$$\frac{[\text{クローズされた脆弱なアイテムの所要時間合計}]}{[\text{クローズされた脆弱なアイテム}]}$$

クローズ済み脆弱性一致アイテムの OT 合計期間

データソース OTVI のクローズ済み脆弱性一致アイテムの OT 合計期間の数。クローズ済み:sn_vul_vulnerable_itemテーブルを使用します。目標は、システム内のクローズされた脆弱性一致アイテムの合計期間を最小化することです。

オペレーショナルテクノロジー脆弱性対応 (PA) ダッシュボードのブレイクダウン

オペレーショナルテクノロジー脆弱性対応はブレイクダウンを使用して、収集されたレコードをフィルタリングしてグループ化します。

ダッシュボードのインジケータは、次のブレイクダウンに適用されます。

経過時間

日/時間/分の形式で表示される脆弱性一致アイテムの経過時間。

クローズした経過時間

ステータスが [クローズ済み] に変更された場合の脆弱性一致アイテムの経過時間。

アサイン先グループ

脆弱性一致アイテムまたは修復タスクのアサイン先グループ。

CI マネージャー

脆弱な構成アイテム (CI) のマネージャー。

保留の理由

脆弱性一致アイテムが修復のために保留される理由。

エクスプロイト攻撃ベクトル

脆弱性エクスプロイトの最も脆弱な攻撃ベクトル。

エクスプロイト有無

脆弱性に関連付けられているエクスプロイト。

エクスプロイトスキルレベル

脆弱性を利用するために必要な最低のスキルレベル。

修復ターゲットルール

脆弱性一致アイテムの修正予定期間。

修復ターゲットステータス

修復ターゲット日の脆弱性一致アイテムのステータスが更新されました。

修正ターゲットステータス (クローズ済み)

修復ターゲット日に達したときに脆弱性一致アイテムのステータスを更新します。

リスク評価

脆弱性一致アイテムを [重大]、[高]、[中]、[低]、および [なし] に分類する数値化されたリスクスコア。

重大度

脆弱性の重大度を正規化したもの。

状況

脆弱性一致アイテムまたは修復タスクのステータス。

次のブレイクダウンソースは、脆弱性一致アイテムレポート、修復タスクレポート、またはその両方のタイプのレポートのダッシュボードのインジケータに適用されます。

アサイン先グループ

脆弱性一致アイテムと修復タスクのレポート。

Deferred.Reason.Non.Closed

脆弱性一致アイテムレポート。

エクスプロイト攻撃ベクトル

脆弱性一致アイテムレポート。

エクスプロイト有無

脆弱性一致アイテムレポート。

エクスプロイトスキルレベル

脆弱性一致アイテムレポート。

OT 経過時間範囲

脆弱性一致アイテムレポート。

修復ターゲットステータス

脆弱性一致アイテムと修復タスクのレポート。

修復ターゲットステータス (クローズ済み)

脆弱性一致アイテムと修復タスクのレポート。

Remediation.Target.Rule

脆弱性一致アイテムと修復タスクのレポート。

リスク評価

脆弱性一致アイテムと修復タスクのレポート。

過酷

脆弱性一致アイテムおよび修復タスクレポート。

状態

脆弱性一致アイテムと修復タスクのレポート。

Vulnerable.Item.CI.Manager

脆弱性一致アイテムレポート。

オペレーショナルテクノロジー脆弱性対応 (PA) ダッシュボード収集ジョブ

オペレーショナルテクノロジー脆弱性対応 (PA) ダッシュボードは、収集ジョブを使用して、ダッシュボードに表示されるデータを収集します。

次の収集ジョブは、オペレーショナルテクノロジー脆弱性対応 (PA) ダッシュボードに表示されるデータを収集します。

[PA OT VR]履歴脆弱性データの収集

既存のレコードの履歴データの収集ジョブ。

i 注: 履歴脆弱性データ収集は、一度だけ実行する必要があるオンデマンドジョブです。履歴データが収集された後、日次データコレクションジョブは毎日スケジュールされた時刻に実行されます。詳細については、「[履歴データの収集](#)」を参照してください。

[PA OT VR]修復タスクの日次収集

毎日行われる修復タスクデータの収集ジョブ。

[PA OT VR]脆弱性一致アイテム 1 の日次収集

保留されていない期限切れの重大な脆弱性一致アイテム、保留された脆弱性一致アイテム、脆弱性一致アイテム、および重大な脆弱性一致アイテムについて毎日発生する収集ジョブ。

[PA OT VR]脆弱性一致アイテム 2 の日次収集

未アサインの脆弱性一致アイテム、クローズされた脆弱性一致アイテム、クローズされた脆弱性一致アイテムの合計期間、および保留された重大な脆弱性一致アイテムについて毎日発生する収集ジョブ。

オペレーショナルテクノロジー脆弱性対応 (PA) ダッシュボードで使用されるデータの可視化

オペレーショナルテクノロジー脆弱性対応 (PA) ダッシュボードでは、データのビジュアル化を使用して OT 脆弱性データを表示します。

次の表では、オペレーショナルテクノロジー脆弱性対応 (PA) ダッシュボードに表示されるデータの可視化について説明します。

[脆弱性一致アイテム] タブのデータの可視化

名前	タイプ	説明
OT 脆弱性一致アイテムの合計	棒グラフ	アクティブな (クローズされていない) OT 脆弱性一致アイテムをデバイスタイプ別にグループ化して表示する棒グラフ。
新しい OT 脆弱性一致アイテム	円グラフ	システム内で検出された新しい OT 脆弱性一致アイテムをデバイスタイプ別にグループ化して表示する円グラフ。
未アサインの OT 脆弱性一致アイテム	円グラフ	オープンでユーザーにアサインされていないデバイスタイプ別にグループ化された OT 脆弱性一致アイテムを表示する円グラフ。
ステータス別の OT 脆弱性一致アイテム	棒グラフ	すべての脆弱性一致アイテムをステータス別に表示する棒グラフ。対処されている脆弱性の数と、さらに調査が必要な脆弱性の数を解釈できます。たとえば、[調査中] カテゴリが比較的高い場合は、これらの脆弱性一致アイテムに最初に対処することで、これらのアイテムに優先順位を付けることができます。
リスク評価別の OT 脆弱性一致アイテム	棒グラフ	選択した時間スパンにおけるリスク評価によってグループ化されたアクティブな OT 脆弱性一致アイテムの数。
修復ターゲットを満した OT VI	単一スコア	現在の四半期と前の四半期の修正ターゲット日を達成したクローズ済み OT 脆弱性一致アイテムの割合。 修正ターゲットは、最後のオープン日に最後のオープン日からの日数 (24 時間単位として測定) を加算して計算されます。
OT VI 平均修正時間 (MTTR)	単一スコア	OT 脆弱性一致アイテムを修正 (クローズ) する平均時間 (30 日間の実行平均として表示)。

[脆弱性一致アイテム] タブのデータの可視化 (続く)

名前	タイプ	説明
		i 注: [クローズした経過時間] の値は、データの収集時に計算されます。値は、last_opened の日付と収集ジョブの日時の差です。
経過時間別の OT VI	棒グラフ	経過時間 (日数) でグループ化されたアクティブな OT 脆弱性一致アイテムを表示する棒グラフ。
修復ターゲットステータス別のクローズ済み OT 脆弱性一致アイテム	棒グラフ	選択した時間スパンにおける、修復ターゲットステータス別にグループ化されたクローズ済み OT 脆弱性一致アイテムの数。 i 注: [クローズした経過時間] の値は、データの収集時に計算されます。値は、last_opened の日付と収集ジョブの日時の差です。
アサイン先グループ別の重大な OT 脆弱性一致アイテム	インジケータスコアカード	アサイン先グループ別に整理された重要な VI。
アサイン先グループ別の期限切れの重大な脆弱なアイテム	インジケータスコアカード	アサイン先グループ別に整理された期限切れの重要な VI。

[修正] タブのデータの可視化

名前	タイプ	説明
OT 修復タスク	単一スコア	アクティブな (クローズされていない) OT 修復タスクの数。
期限間近の重大な OT 修復タスク	単一スコア	修復ターゲット日が近づいているアクティブな OT 修復タスクの数。 OT 修復タスクの修復ターゲット日は、グループ内のアクティブな脆弱性一致アイテムに属する最も近い期日に設定されます。 修正ターゲットは、最後のオープン日に日数 (24 時間単位として測定) を加算して計算されます。

[修正] タブのデータの可視化 (続く)

名前	タイプ	説明
		このレポートでは、保留された OT 修復タスクは除外されます。
リスク評価別の OT 修復タスク	棒グラフ	リスク評価別にグループ化されたアクティブな OT 修復タスクを表示する棒グラフ。
ターゲットステータス別の OT 修復タスク	棒グラフ	修復ターゲットステータス別にグループ化されたアクティブな OT 修復タスクを表示する棒グラフ。 このレポートでは、保留された OT 脆弱性一致アイテムは除外されます。
ステータス別の OT 修復タスク	棒グラフ	すべての修復タスクをステータス別に表示する棒グラフ。修復タスクの進捗状況を解釈できます。
未アサインの OT 修復タスク	単一スコア	アサイン済みまたはアサイン先グループのないアクティブな OT 修復タスクの数。
アサイン先グループ別の OT 重大な修復タスク	インジケータースコアカード	アサイン先グループ別に整理された重大な修復タスク。
アサイン先グループ別の期限切れの重大な OT 修復タスク	インジケータースコアカード	アサイン先グループ別に整理された期限切れの重大な修復タスク。

[例外] タブのデータ可視化

名前	タイプ	説明
理由別の保留された OT 脆弱性一致アイテム	棒グラフ	保留の理由によってグループ化された、保留された OT 脆弱性一致アイテムの数。
アサイン先グループ別の重大な脆弱性一致アイテムの OT 例外	インジケータースコアカード	アサイン先グループ別に整理された重要な VI の例外。

オペレーショナルテクノロジー統一マップを表示

デバイスと他の CI との関係を示す 産業用ワークスペース 内の オペレーショナルテクノロジー (OT) 統一マップを表示します。

始める前に

必要なロール：admin

このタスクについて

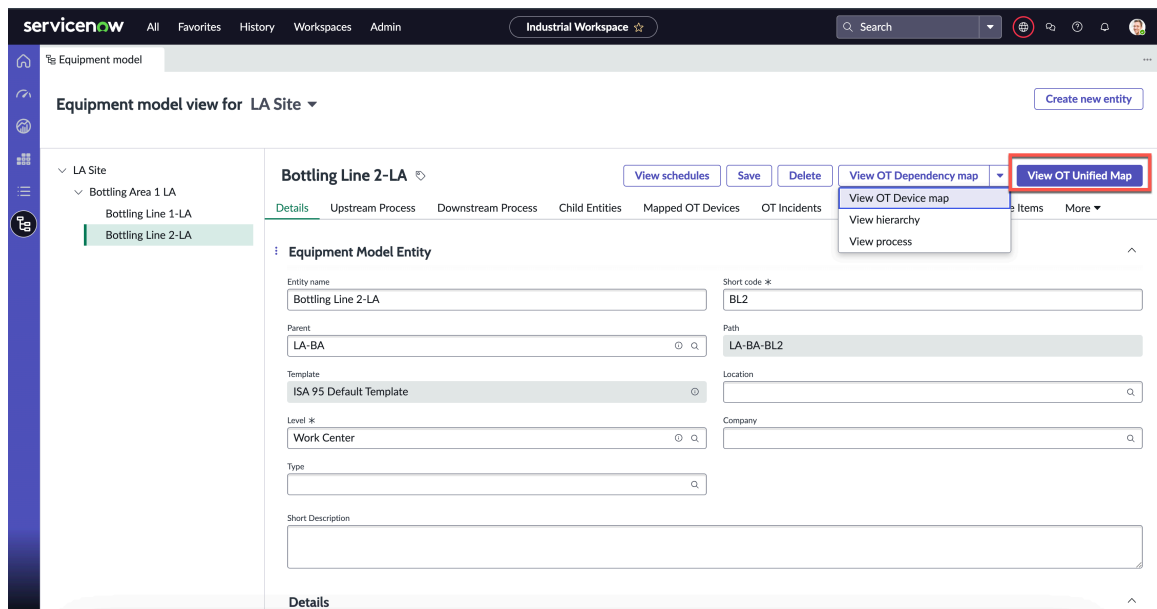
OT 統一マップには、産業用ワークスペース内の次の場所からアクセスできます。

- 機器モデルマネージャーの ISA レコード
- OT インシデントレコード
- OT 変更レコード

手順

1. 移動先 すべて > 産業用ワークスペース.
2. 機器モデルエンティティレコードの OT 統一マップにアクセスするには、次のアクションを完了します。

- a. 機器モデル () アイコンを選択して、機器モデルマネージャーを開きます。
- b. 統一マップを表示する機器モデルエンティティレコードを開きます。
- c. [OT 統一マップを表示] ボタンを選択します。



3. OT インシデントレコードや変更レコードなどの関連レコードの OT 統一マップにアクセスするには、次のアクションを完了します。

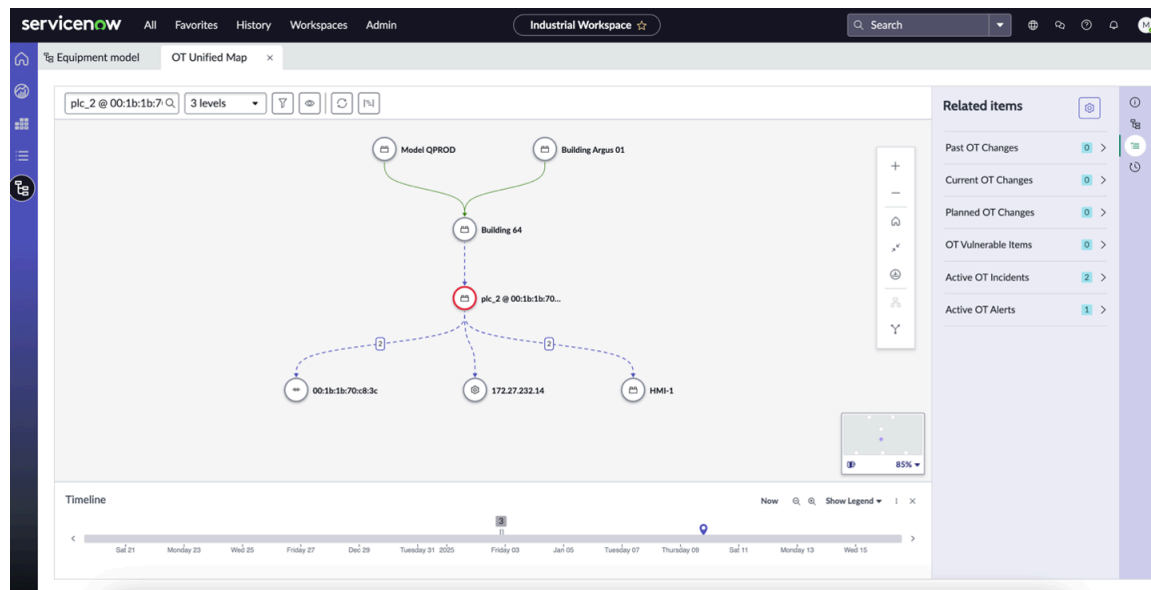
- a. リスト () アイコンを選択して、産業用ワークスペースリストビューを開きます。
- b. 統一マップを表示するレコードを選択します。
たとえば、OT インシデントレコードの統一マップを表示する場合は、[OT インシデント] モジュールで利用可能なリストのいずれかを選択してレコードを開きます。
- c. 新しいウィンドウでマップを開くには、[OT 統一マップを表示] ボタンを選択します。
- d. レコードのサイドパネルでマップを開くには、[OT ヘルプ] () アイコンを選択します。

次のタスク

OT 統一マップを表示できるようになりました。統一マップでは、次の関連アイテムのノードがハイライト表示されているのわかります。

- 過去の OT 変更
- 現在の OT 変更
- 予定されている OT 変更
- アクティブな OT インシデント
- アクティブ OT アラート
- OT 脆弱性一致アイテム

次の画像は、OT 統一マップの例を示しています。



自動翻訳

機器モデルエンティティのオペレーショナルテクノロジー デバイスアクティビティの日次サマリーを表示する

産業用ワークスペースの機器モデルビューで、サイト内のオペレーショナルテクノロジー (OT) デバイスで実行された前日のアクションと変更を表示します。

始める前に

必要なロール:cmdb_ot_isa_viewer

このタスクについて

産業用ワークスペースの [機器モデル] メニューの [日次アクティビティ] タブには、前日にサイト内の OT デバイスで実行されたアクティビティの数が表示されます。[日次アクティビティ] タブには、次のアクティビティが表示されます。

- OT デバイスがサイトに追加されました。
- OT デバイスの詳細が更新されました。
- OT デバイスが新しい機器モデルエンティティにマッピングされました。
- OT デバイスのライフサイクルステータスが [廃止] としてマークされました。

手順

1. 移動先 **すべて > 産業用ワークスペース > [機器モデル] メニュー** () アイコン。 .
2. OT デバイスの日次サマリーを表示する機器モデルエンティティレコードを選択します。

次のタスク

アクティビティの合計数は、[毎日のアクティビティ] タブで確認できます。前日に OT デバイスで実行されたすべてのアクティビティの展開リストを表示する場合は、[日次アクティビティ] タブを選択します。展開されたリストでは、次のようなアクティビティの詳細を表示できます。

- OT デバイスタイプ
- マッピングされた機器モデルエンティティ
- ステータスを変更
- デバイスの重要度
- ディスカバリーソース
- 変更者
- 変更されたフィールド
- フィールドの変更

 **注:** 2 日以上経過した日次アクティビティレコードは自動的に削除されます。

e のハードウェア脆弱性アセスメントメニュー産業用ワークスペース

ハードウェア脆弱性アセスメントメニューを使用して、OT 環境のすべてのファームウェア脆弱性アセスメントを表示および追跡します。また、[HVA] メニューでは、ファームウェア脆弱性アセスメントに基づいて作成された脆弱性一致アイテムを表示できます。

始める前に

必要なロール:sn_otvr.vul_event_manager

このタスクについて

[ハードウェア脆弱性アセスメント] メニューには、脆弱性情報データベース (NVD) に登録されている脆弱性に完全または部分的に一致する、オペレーショナルテクノロジー (OT) インベントリ内のすべての脆弱性に関する情報が表示されます。

手順

1. 移動先 **ワークスペース > 産業用ワークスペース > ハードウェア脆弱性アセスメント**。メニューアイコン () .
2. 必要に応じて、[完全に一致したアセスメント]、[部分的に一致したアセスメント]、[脆弱性一致アイテム]、[無視されたアセスメント]、および [正規化待ち] タブで次のアクションを実行します。
 - a. 追加の列を選択して表示すると、update pdate pカスタマイズlistアイコン () によるを選択すると、アセスメントに関する詳細情報が表示されます。
 - b. 表示されたアセスメントのリストを更新するには、リフレッシュアイコン () を選択します。

- c. 追加のフィルター条件に従ってタブでアセスメント情報を表示フィルターリストアイコン () アイコンから選択。
 - d. [フィルターを選択] を選択してアセスメントをすばやくフィルタリングできます。
3. [完全に一致したアセスメント] タブと [部分的に一致したアセスメント] タブを選択して、アセスメントレコードを表示します。
- a. 脆弱性一致アイテムを手動で作成できます 任意のアセスメントレコードに対して選択する 表示されたリストから 1 つ以上のレコードを選択し、[脆弱性一致アイテムを作成] を選択します。
 - b. アセスメント レコード 表示されたリストから 選択) は無視してかまいません。1 つ以上のアセスメントレコードを選択し、[無視] を選択します。無視されたアセスメントは、[無視されたアセスメント] タブで使用できます。
4. [無視されたアセスメント] タブ:
- a. OT デバイス 以前に無視した) でアセスメントを実行する場合は、[元に戻す] を選択します。
 - b. アセスメントの脆弱性一致アイテムを手動で作成する場合 表示されたリストから選択) 場合は、[脆弱性一致アイテムを作成] を選択します。
5. [脆弱性一致アイテム] タブ [完全に一致したアセスメント]、[部分的に一致したアセスメント]、および [無視されたアセスメント] タブで作成されたアセスメントレコードに基づいて作成された脆弱性一致アイテムのリストを表示します。
6. [正規化待ち] タブを選択してアセスメントに使用されていない正規化待ちの OT デバイスデータを表示します。
デバイスデータの正規化ステータスは次のようになります。
- 新規
 - 一致なし
 - 正規化されたパブリッシャー

i 重要: エンタープライズ資産管理 でオプトイン機能を有効にすると、OT デバイスを正規化に使用できるようになります。詳細については、「[エンタープライズ資産管理コンテンツサービスへのオプトイン](#)」を参照してください。

関連トピック

[オペレーショナルテクノロジー ハードウェア脆弱性アセスメント](#)

[ガイド付きセットアップを使用したオペレーショナルテクノロジーデバイスのハードウェア脆弱性アセスメント設定](#)

ドメインセパレーションとオペレーショナルテクノロジー

オペレーショナルテクノロジー ではドメインセパレーションがサポートされています。ドメインセパレーションでは、データ、プロセス、および管理タスクをドメインと呼ばれる論理的なグループに分けることができます。どのユーザーがデータを表示できるか、データにアクセスできるかなど、このアプリケーションのいくつかの側面を制御できます。

サポートレベル：ベーシック

- アプリケーションサービスプロバイダーのユースケースに合わせてデータが適切なドメインに送られるようにするビジネスロジックが存在します。
- このアプリケーションは、ドメインセパレーションを完全にサポートしています。ドメインセパレーションには、ユーザーインターフェイス、キャッシュキー、レポート、ロールアップ、および集計からのドメインの分離が含まれます。
- インスタンスのオーナーは、複数のテナント間で正常に機能するようにアプリケーションをセットアップする必要があります。

サンプルユースケース：サービスプロバイダーがチャットを使用してテナント顧客のメッセージに回答する場合、お客様がサービスプロバイダーの応答を確認できるようにする必要があります。

サポートレベルの詳細については、「[アプリケーションでのドメインセパレーションのサポート](#)」を参照してください。

オペレーショナルテクノロジー ドメインセパレーションの概要

オペレーショナルテクノロジー は、依存関係アプリケーションのドメインセパレーション機能を継承します。各アプリケーションは独自のドメインセパレーション関係を持つことができるため、オペレーショナルテクノロジーに関連付ける特定のサポートレベルはありません。詳細については、「[ドメインセパレーションと ワークフロースタジオ](#)」を参照してください。

次の表に、各 オペレーショナルテクノロジー アプリケーションのドメインセパレーションのサポートレベルとユースケースを示します。

アプリケーションによるサポートレベル

アプリケーション	サポートレベル
オペレーショナルテクノロジー マネージャー	基本
製造業プロセスマネージャー	基本
オペレーショナルテクノロジー 脆弱性対応	基本
オペレーショナルテクノロジー	基本
オペレーショナルテクノロジー 変更管理	基本
オペレーショナルテクノロジー のナレッジ管理	基本
オペレーショナルテクノロジー 要求管理	基本

関連トピック

[サービスプロバイダーのドメインセパレーション](#)