検証済みプロファイル：製造(非ファブリック) 業界

2025 年 2 月 12 日

© 2025 Cisco and/or its affiliates. All rights reserved.

注記

製造業（SD-Access）におけるシスコの検証済みプロファイルについては、『Validated Profile: Manufacturing (SD-Access Vertical)』で詳細を確認してください。

© 2025 Cisco and/or its affiliates. All rights reserved.

ソリューションの概要

このガイドでは、製造業の実稼働ネットワーク用にシスコが推奨する展開プロファイルについて説明します。Cisco Catalyst Center を使用した一般的な非ファブリック展開のガイダンスを提供し、デプロイエンジニアの検証リソースとして機能します。理論的な情報と実用的な情報を組み合わせて、不可欠なサービスのインサイトをエンジニアに提供し、展開および設定中の情報に基づいた判断を支援します。このガイドは、シスコの産業用自動化および Converged Plant-wide Ethernet（CPwE）のシスコ検証済み設計（CVD）の設計および導入ガイダンスに準拠しており、一般的にこれらに従っています。

このガイドの対象読者は、製造生産ネットワークを導入または管理する IT および運用技術（OT）の専門家です。このガイドは、実稼働システムの設計、導入、または運用に携わるベンダー、パートナー、システム実装者、顧客、およびサービスプロバイダー用の検証リファレンスとして機能します。

実稼働環境は、過去 15 年間で大幅に進化し、独自のニッチ ネットワーキング テクノロジーから標準のネットワーキング テクノロジーとプラクティスに移行しました。実稼働ネットワークは通常、IT チームと OT チームが混在して導入および管理されます。このような実稼働環境には、運用を開始して継続するために、大規模なネットワークを一貫して展開するためのネットワーク自動化の必要性、サイバーセキュリティがほとんどない環境向けのネットワークセキュリティの強化、重要な運用をサポートする可用性の高いレジリエンスのあるネットワーク インフラストラクチャ、IT 以外のオペレータ向けのシンプルなモニタリング、効率的なトラブルシューティングなどの、独自の一連の要件があります。以降の項では、現代的な工場、生産施設、および倉庫の開発の基礎となるこれらの重要な領域について詳しく説明します。

高可用性

製造業務は継続的に実行されることが多く、ネットワークの中断が発生すると生産のダウンタイムが発生し、重大な財務的損失が発生する可能性があります。高可用性（HA）により、ハードウェア障害、ソフトウェアの問題、接続の問題、またはその他の中断が発生した場合にネットワークの動作が確保され、生産のダウンタイムが最小限に抑えられます。製造ネットワーク内の産業オートメーションおよび制御システムの稼働時間を確保するには、堅牢で復元力のあるネットワークが必要です。

このガイドで採用されているネットワークアーキテクチャでは、ネットワーク、管理、およびアクセス制御システムの信頼性とフォールトトレランスが強化されます。このアーキテクチャでは、関連する場合、OT ネットワーク全体でサポートされている Cisco Catalyst スイッチにスイッチスタック（物理または仮想）を導入することで、ハードウェアの単一障害点が削減されます。複数のネットワークパスとともに、必要なレイヤ 3 ルーティングプロトコルと、レイヤ 2 ネットワークでの迅速なリカバリを実現するように設計されたレジリエンスプロトコルを組み込むことで、ネットワークのレジリエンスが実現されます。ネットワークのセットアップは高速コンバージェンス用に設計されています。これは、製造ネットワークの厳格な遅延と最小パケット損失の要件を考えると重要です。ネットワーク インフラストラクチャに加えて、ネットワークデバイスを管理および設定するシステムが冗長モードで展開されます。Catalyst Center には、3 つのノードを使用した HA 設定が含まれています。さらに、ネットワークポリシーを制御する Cisco ISE が、ポリシー管理ノード（PAN）、ポリシーサービスノード（PSN）、Platform Exchange Grid（pxGrid）、モニタリングおよびトラブルシューティング ノード（MnT）などの冗長性を備えたマルチノードクラスタとして展開されます。

© 2025 Cisco and/or its affiliates. All rights reserved.

ネットワーク自動化

製造設備には、多くの場合、多数のデバイスと設定を持つ大規模で複雑なネットワークがあります。自動化により、ネットワークのプロビジョニング、設定の変更、およびメンテナンスタスクが合理化され、ダウンタイム、ワークロード、および人的エラーのリスクが削減されます。拡張性は、多数のネットワークデバイスを含む製造ネットワークを自動化するために不可欠な要素です。Catalyst Center では、プラグ アンド プレイ アプローチを使用して、初期設定（Day 0 設定）のためにネットワークデバイスを大規模かつシームレスにオンボードできます。これにより、Catalyst Center は複雑な製造ネットワークを自動化するための重要なツールとなっています。さらに、設定変更（Day n 設定）の自動プロビジョニングがサポートされ、すべてのネットワークデバイスで設定の一貫性が保たれます。ソフトウェアのアップグレードは、特にさまざまなイメージとバージョンを実行している多数のネットワークデバイスを処理する場合には、困難で時間がかかることがあります。Catalyst Center のソフトウェアイメージ管理（SWIM）機能により、ソフトウェアのアップグレードプロセスが簡素化され、アップグレードにかかる時間が短縮されます。Catalyst Center は、ネットワーク自動化機能を一元化することで、シスコ製品ポートフォリオの使用可能なさまざまなセキュリティ プラットフォームと統合しながら、有線およびワイヤレスの接続を含む IT と OT の両方のネットワーキング要件に対応します。

ネットワーク セキュリティ

ネットワークセキュリティは、製造ネットワークの重要な要件です。製造ネットワークは、重要なプロセスや機械を制御および監視するための接続を提供するうえで重要な役割を果たします。セキュリティが侵害されると、生産が中断され、財務上の損失や潜在的な安全上のリスクが生じる可能性があります。ネットワークセキュリティの侵害、マルウェアの侵入、またはサイバー攻撃は、生産の大幅なダウンタイムにつながり、出荷の遅延、生産目標の未達成、および収益の減少の原因となる可能性があります。不正アクセスやデータ漏洩により、製造業者が知的財産の窃取や産業スパイ活動にさらされる可能性があります。

このドキュメントで説明するセキュリティアーキテクチャには、『Industrial Automation Security Design Guide』に詳述されている以下のようなセキュリティ対策の全領域が統合されています。

- Cisco Trustworthy 技術によるセキュアなネットワーク インフラストラクチャ。
- 実稼働システムを保護する産業用緩衝地帯（IDMZ）を確立するための次世代ファイアウォール。
- Cisco Cyber Vision を使用した、製造工場フロア上のさまざまな設備の拡張ビュー。
- Cisco ISE での Cisco TrustSec を使用したセキュリティポリシーの展開とセグメンテーション。
- Cisco Extended Detection and Response（Cisco XDR）による問題の検出と対応の向上。
- Cisco Secure Network Analytics と Cisco Cyber Vision を使用した異常とマルウェアの脅威の特定。

ネットワークのモニタリングとトラブルシューティング

製造プロセスのネットワークシステムへの依存度が高まるにつれて、効果的なネットワーク管理が不可欠になります。ネットワーク管理によって、運用の継続性、リソース効率、およびセキュリティが確保され、製造設備の成功と競争力のために役立てることができます。ネットワーク輻輳、ハードウェア障害、セキュリティ侵害などの問題を特定するには、迅速な異常検出が重要です。ネットワーク管理ツールにより、問題を迅速に特定し、解決にかかる時間を短縮できます。ネットワーク管理ツールではネットワークパフォーマンスとトラフィックパターンに関する有益なインサイトが提供され、プロセスの最適化、予知保全、および情報に基づいた判断のために使用することができます。

© 2025 Cisco and/or its affiliates. All rights reserved.

Catalyst Center は、ネットワークのモニタリングとトラブルシューティングの領域に優れた、包括的なネットワーク管理プラットフォームを提供します。ネットワークの可視性を確保し、デバイス、アプリケーション、サービスステータス、およびパフォーマンスのモニタリングを容易にします。Catalyst Center は、スイッチ、ルータ、アクセスポイント、エンドポイントなどのさまざまなネットワークデバイスの正常性を追跡するために役立ち、それらの動作ステータスに関する有益なインサイトを提供します。また、このプラットフォームではトラフィック分析用のツールも提供され、ネットワーク トラフィック パターンの特性評価、逸脱検知、およびネットワークパフォーマンスに影響を与える可能性のある潜在的な問題のアラート生成を行うことができます。さらに、Catalyst Center は事前定義された基準またはネットワークイベントに基づいてアラートと通知を提供できるため、ネットワーク管理者は迅速に問題に対応できます。Catalyst Center には、デバイスの相互接続を示すネットワークトポロジマップが表示されます。これは、ネットワークアーキテクチャを理解し、潜在的な障害点を特定するために役立ちます。

ネットワークの問題が発生すると、Catalyst Center はデバイスとトラフィックの動作に関する詳細なインサイトを提供することで、根本原因の特定を支援します。Catalyst Center は、ネットワークパスを追跡し、アプリケーション パフォーマンスに影響を与える可能性のあるブロックまたは接続の問題を特定するためのパス分析ツールを提供します。このプラットフォームでは履歴データも保持されるため、管理者は過去のネットワークイベントやパフォーマンスの傾向を確認して、繰り返されている問題を特定できます。

© 2025 Cisco and/or its affiliates. All rights reserved.

ハードウェアとソフトウェアの仕様

ソリューションは、次の表に示すハードウェアとソフトウェアで検証されています。

ロール	モデル名	ハードウェア プラットフォーム	ソフトウェア バージョン
Catalyst Center コントローラ	DN2-HW-APL-XL	Catalyst Center アプライアンス 3 ノードクラスタ	2.3.7.7
アイデンティティ管理、RADIUS サーバー	ISE-VM-K9	Cisco Identity Services Engine 仮想アプライアンス	3.3 パッチ 4
ネットワーク検出、可視性、逸脱検知	CV-A-250	Cisco Cyber Vision	4.2.2、5.0.1
セキュリティモニタリング、逸脱検知、脅威検出	L-ST-SMC-VE-K9 L-ST-FC-VE-K9	Cisco Secure Network Analytics Manager、Cisco Secure Network Analytics Flow Collector	7.4.2
ファイアウォールマネージャ	FMCv25	Cisco Secure Firewall Management Center	7.2.8
ファイアウォール IDMZ	FPR-2140	Cisco Firepower	7.2.8
Cisco アクセススイッチ	IE3100-18T2C IE3105-18T2C IE3200-8P2S IE3200-8T2S IE3300-8P2S IE3300-8T2S IE3300-8T2X IE3300-8U2X IE-3400-8P2S IE3400-8T2S IE3400H-24FT	Cisco Catalyst IE3100、3200、3300、3400、9320	17.9.5、17.12.4
Cisco ディストリビューション スイッチ	C9300-24T C9300-48T C9300X-24Y C9300X-12Y	Cisco Catalyst 9300 シリーズ スイッチ	17.9.5、17.12.4
Cisco コアスイッチ	C9500-12Q C9500-24Q	Cisco Catalyst 9500 シリーズ スイッチ	17.9.5、17.12.4
シスコ ワイヤレス コントローラ	C9800-40-K9	Cisco Catalyst 9800 ワイヤレスコント	17.9.6、17.12.4

© 2025 Cisco and/or its affiliates. All rights reserved.

ロール	モデル名	ハードウェア プラットフォーム	ソフトウェア バージョン
		ローラ	
Cisco アクセス ポイント	IW-6300H-AC-X-K9 9124AXI	Cisco Catalyst アクセスポイント	17.12.4

© 2025 Cisco and/or its affiliates. All rights reserved.

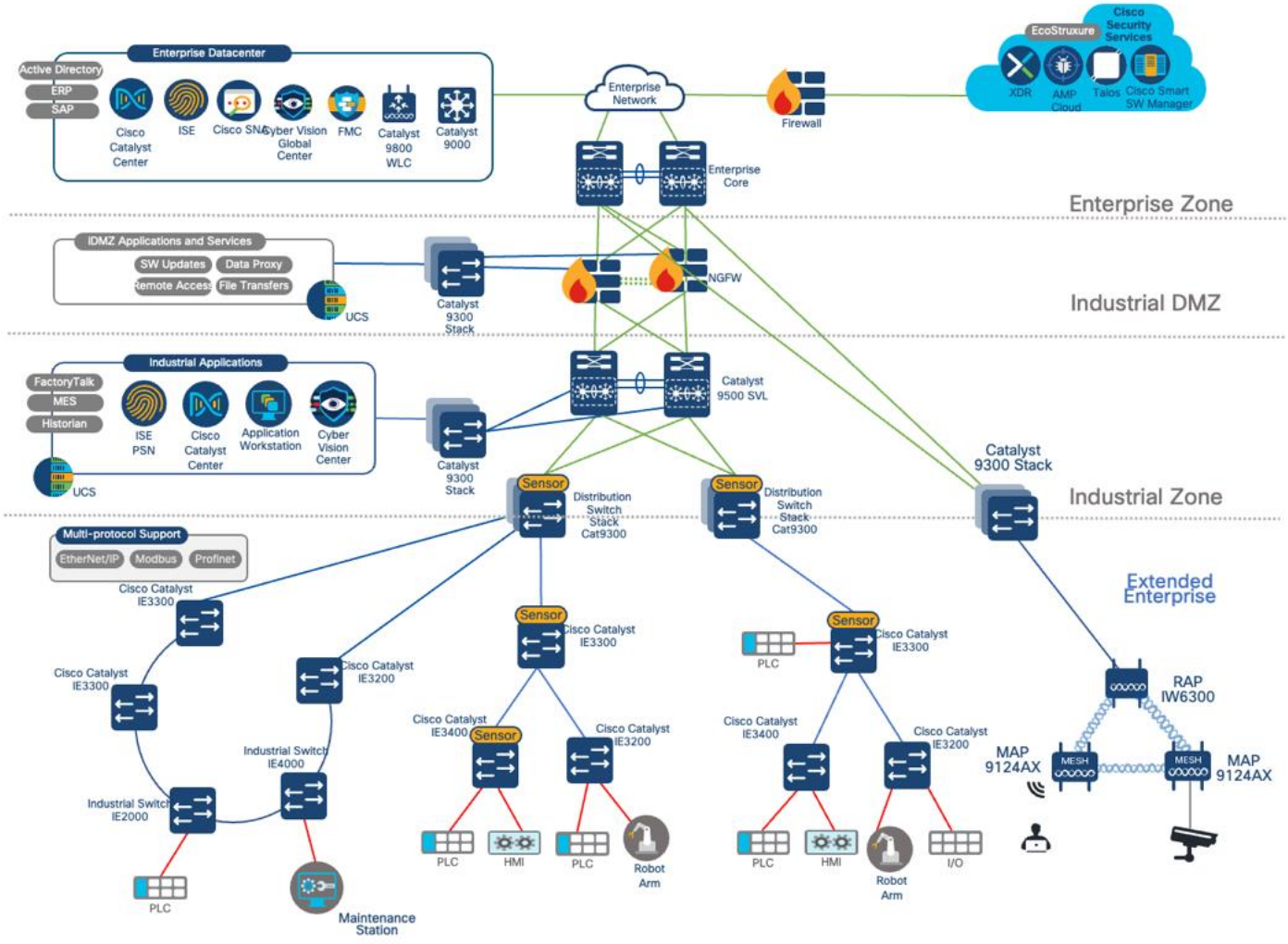
テストトポロジには、次の産業用自動化/制御システム（IACS）デバイスが含まれます。

メーカー	ロール	モデル
Rockwell Automation	コントローラ	LOGIX5318ER LOGIX5336ER LOGIX5336ER M LOGIX 5573 Safety LOGIX 5575
	I/O デバイス	A-B 1791ES-IB8XOBV4 IP20 8/
	管理ソフトウェア	FactoryTalk アプリケーション
Siemens	コントローラ	S7 300 S7 1500 S7 414F-3 S7 400
	I/O デバイス	ET200M
	ハードウェア モジュール インターフェイス（HMI）	TP 1200
	管理ソフトウェア	TIA エンジニアリング ワークステーション
Schneider Electric	コントローラ	BMEP583020 BMEP582020
	I/O デバイス	STBNIC2212 BMECRA31210
	管理ソフトウェア	EcoStruxure Control Expert

© 2025 Cisco and/or its affiliates. All rights reserved.

ソリューション トポロジ

図 1. ソリューション トポロジ



© 2025 Cisco and/or its affiliates. All rights reserved.

ソリューションのユースケース

カテゴリ	機能	使用例
ネットワーク自動化	Day 0 および Day n のプロビジョニング	• Catalyst Center のプラグアンドプレイ（PnP）機能を使用した IE スイッチの Day 0 オンボーディング。 • ディストリビューション ゾーンの Cisco Catalyst スイッチと、セルゾーンまたはエリアゾーンの Cisco Catalyst IE デバイスの、Day n のプロビジョニング。
	Resilient Ethernet Protocol（REP）のプロビジョニング	• Catalyst Center を使用した非ファブリック REP リングのプロビジョニング。 • Catalyst Center を使用した REP リングに対する Day n の IE デバイスの追加または削除。 • Catalyst Center を PnP サーバーとして REP-ZTP を使用した REP リングのプロビジョニングとセグメンテーション。
	インベントリ管理	• Catalyst Center を使用した、IP アドレスによるネットワークデバイスの検出。 • Catalyst Center を使用した OT および IT ネットワーク デバイス ソフトウェアのアップグレード。 • Catalyst Center を使用した IE スイッチのデバイス交換。 • OT ネットワークのトポロジビュー。
	Extended Enterprise（ワイヤレス）	• Catalyst Center を使用したワイヤレスネットワークの管理およびプロビジョニング。 • ワイヤレスネットワークでの Day n の変更の実行。 • Catalyst Center を使用した、工場フロアでのワイヤレス メッシュ ネットワークの立ち上げ。 • IP カメラなどの重要ではない有線デバイスまでワイヤレスメッシュを拡張するための、Catalyst Center を使用した CLI テンプレートの展開。
セキュリティ	基本的なセキュリティ（産業用 DMZ）	• Cisco NGFW Firepower デバイスによる、産業用 DMZ を使用した IT と OT の分離。
	Cisco Cyber Vision	• Cisco Cyber Vision とセンサーによる産業の可視性。 • Cisco Cyber Vision を使用した逸脱検知と脅威検出。 • Cisco Secure Network Analytics と、Cisco Cyber Vision によって拡充されたホストグループ情報を使用した、フローベースの逸脱検知。
	Cisco TrustSec	• Cisco TrustSec と、Catalyst Center からオーケストレーションされたポリシー制御による、セグメンテーション。 • Cisco Cyber Vision と Cisco TrustSec を使用した、工場フロアでの産業用デバイスの検疫。
ネットワークのモニタリングとトラブルシューティング	グループベースポリシーの分析	• さまざまなセキュリティグループ間のトラフィックフローのモニターと、トラフィックパターンに基づいたポリシーの改善。
	保証	• Catalyst Center Assurance を使用した、デバイス、クライアント、およびネットワークの正常性のモニター。 • Catalyst Center によって提供されるガイド付き手順を使用した、問題のトラブルシューティング。 • 関心のあるイベントのアシュアランスアラートのカスタマイズ。
	AI エンドポイント分析	• Cisco Cyber Vision によって産業用コンテキストが拡充された、IT および OT エンドポイントの統合ビュー。
	コンプライアンス	• ネットワークデバイスのコンプライアンスの追跡と、コンプライア

© 2025 Cisco and/or its affiliates. All rights reserved.

カテゴリ	機能	使用例
		ンスの問題を修正するための適切なアクションの実施。
	監査ログ	• 監査ログ機能を使用した、Catalyst Center への不正アクセスの試みとプロビジョニングの変更の追跡。
高可用性	ネットワークとデバイスのレジリエンス	• Cisco Catalyst スタックスイッチおよび StackWise Virtual リンク（SVL）対応スイッチによるデバイスレベルの SSO。 • レイヤ 2 およびレイヤ 3 の冗長リンクフェールオーバー。 • Catalyst Center 3 ノード HA フェールオーバーと Cisco ISE PAN または PSN フェールオーバーの併用。

© 2025 Cisco and/or its affiliates. All rights reserved.

スケールマトリックス

ソリューションでは、次の表に示すスケールの数値について確認しました。Catalyst Center アプライアンスのスケールの数値を確認するには、Cisco Catalyst Center のデータシートを参照してください。

変数	スケール
コントローラ デバイス インベントリ	2000
サイトごとのネットワークデバイス	500
ゾーン（エリア）	1000
VLAN	2000
セキュリティ グループ タグ（SGT）	1000
セキュリティグループ ACL（SGACL）	500
セキュリティ	20,000（有線が 15,000、ワイヤレスが 5,000）

次の表に、セル/エリアゾーンの検証済みスケールプロファイルを示します。

変数	スケール
エンドポイント	500
マルチキャスト グループ	200
REP リングサイズ	18
Cisco Catalyst IE3400/IE3300 スイッチでの Cisco Cyber Vision フロー	9,600 pps
Cisco Catalyst 9300 スイッチでの Cisco Cyber Vision フロー	12,000 pps

© 2025 Cisco and/or its affiliates. All rights reserved.

ソリューションの重要事項

以下のセクションでは、ソリューションの展開に役立つテクニカルノートについて説明します。

ネットワーク自動化

以降の項では、ネットワーク自動化に関連した機能の導入について説明します。

シスコのプラグアンドプレイを使用した新しいスイッチのオンボーディング

製造工場では、新しいスイッチの迅速なオンボーディングがシームレスな運用にとって重要です。オンボーディングプロセスには、次の重要な特性が必要です。

- 迅速：新しいスイッチは迅速にオンボードされ、数分以内に運用の準備が整うようにする必要があります。
- シンプル：ネットワーキングに関するバックグラウンドを持たないオペレータでもオンボーディングプロセスを実行できる必要があります。
- スケーラブル：プロセスは、何百ものスイッチ間で複製できる必要があります。
- 一貫性：プロセスは、所定のワークフローに従うことで、均一な構成を確保し、人的エラーを防ぐ必要があります。

Catalyst Center のオンボーディングプロセスでは、PnP によるゼロタッチ展開を使用します。PnP は、サイトのネットワークプロファイルを使用して、ネットワーク内の新しい未設定のデバイスの自動設定を容易にします。サイトは、ネットワーク内の物理的な場所、機能、またはその両方に基づいてデバイスをグループ化します。

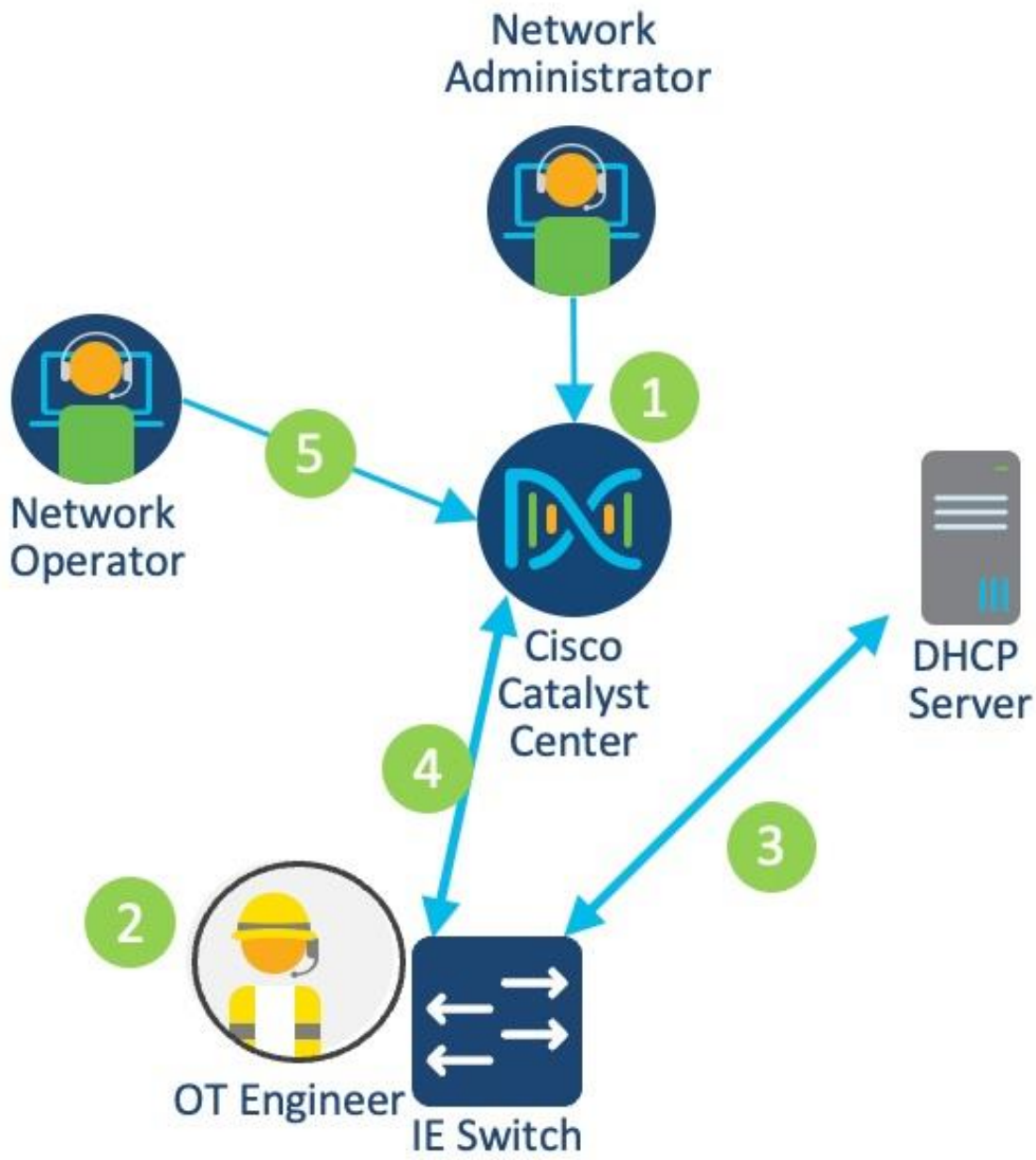
IOS または IOS-XE ソフトウェアを実行しているシスコの産業用スイッチの場合、組み込みの PnP エージェントは PnP 導入サーバーと通信します。この PnP エージェントは、新しく電源が投入されたデバイスや工場出荷時のデフォルトにリセットされたデバイスなど、スタートアップ コンフィギュレーションのないデバイスで動作します。これは、Catalyst Center の DHCP または DNS を介して PnP 展開サーバーを検出します。PnP エージェントは、PnP サーバーとの通信を開始し、重要なソフトウェアとデバイスの設定をダウンロードします。

未設定のデバイスがネットワークに接続し、Catalyst Center に接続すると、Catalyst Center によってデバイスのエントリが作成され、管理者が要求するまで要求元不明状態になります。または、インストール前にシリアル番号とデバイスファミリを入力して、デバイスを Catalyst Center に追加することもできます。接続後、デバイスは指定されたサイトに要求され、サイトの設定に基づいて事前に定義されたソフトウェアイメージと設定を使用して設定できます。

次の図は、PnP プロビジョニング ワークフローを示しています。

© 2025 Cisco and/or its affiliates. All rights reserved.

図 2.　PnP プロビジョニング ワークフロー



このワークフローには、次の主要なステップが含まれています。

1. ネットワーク管理者が、Catalyst Center でサイト階層を作成し、サイトプロパティを設定し、プロビジョニング テンプレートを追加し、ゴールデンイメージを定義します。
2. OT エンジニアが産業用スイッチをネットワークに接続し、デバイスの電源を入れます。
3. スイッチは DHCP を使用して IP アドレスを取得し、PnP サーバーの IP アドレスを検出します（Catalyst Center）。
4. スイッチは Catalyst Center に接続します。

© 2025 Cisco and/or its affiliates. All rights reserved.

5. オペレータが Catalyst Center でデバイスを要求します。要求プロセス中に、Catalyst Center は次のアクションを実行します。
    - ゴールデンイメージをインストールします。
    - ライセンスを含む設定を発行します。
    - Cisco ISE および Catalyst Center のインベントリにデバイスを追加します。

Catalyst Center への設定済みデバイスの追加

PnP プロセスはスイッチのオンボーディングに対する効率的なアプローチを提供しますが、シナリオによっては別の方法が必要になる場合があります。次に例を示します。

- オフラインの新しいスイッチのプロビジョニング：特定の状況では、スイッチをネットワークに接続する前にプロビジョニングすることが必要です。これは、ネットワーク接続を確立する前にスイッチを設定する必要がある産業オートメーション環境に特に関連します。PnP プロセスは設定をネットワーク接続に依存しているため、オフラインでプロビジョニングされたスイッチには別のアプローチが必要です。
- 製造設備外で設定されたスイッチ：場合によっては、製造設備にスイッチが到着する前に、システムインテグレータがスイッチを設定します。この方法では、スイッチは事前設定されて到着し、すぐに導入できるため、オンボーディングプロセスが合理化されます。
- ブラウンフィールド展開：ブラウンフィールドとは、設定が確立された既存のサイトに統合されたデバイスを指します。ブラウンフィールド展開を扱う場合、ネットワークデバイスは検出機能を使用して Catalyst Center に追加されます。

検出プロセス

前の項で説明したシナリオでは、Catalyst Center は検出機能を使用してネットワークデバイスを追加します。検出機能は、ネットワーク内のデバイスのスキャンを実行し、検出されたデバイスのリストを送信し、デバイスインベントリにシームレスに統合します。

検出には、IP アドレス範囲、Cisco Discovery Protocol（CDP）、Link Layer Discovery Protocol（LLDP）など、さまざまな方法を使用できます。この CVP では、IP アドレスの範囲が使用されました。検出タスク中に、Catalyst Center で CLI および SNMP 読み取りクレデンシャルを設定する必要があります。

サイトの割り当てとネットワークアシュアランス

デバイスの検出中に、Catalyst Center でデバイスを特定のサイトに割り当てるオプションを使用できます。デバイスをサイトに割り当てると、Catalyst Center はテレメトリ設定をプッシュして、新しく追加されたデバイスにネットワークアシュアランスを提供します。

REP リングのプロビジョニング

産業用自動化プロセスは、IACS アプリケーションの可用性と稼働時間に大きく依存しています。これらのシステムの継続性を確保するには、復元力があり堅牢なネットワーク設計が不可欠です。標準イーサネットおよび IP コンバージド IACS ネットワーキング テクノロジーのレジリエンスと堅牢さを強化する LAN アーキテクチャを導入することで、総合設備効率（OEE）を向上させ、障害の影響を最小限に抑え、平均修復時間（MTTR）を短縮できます。

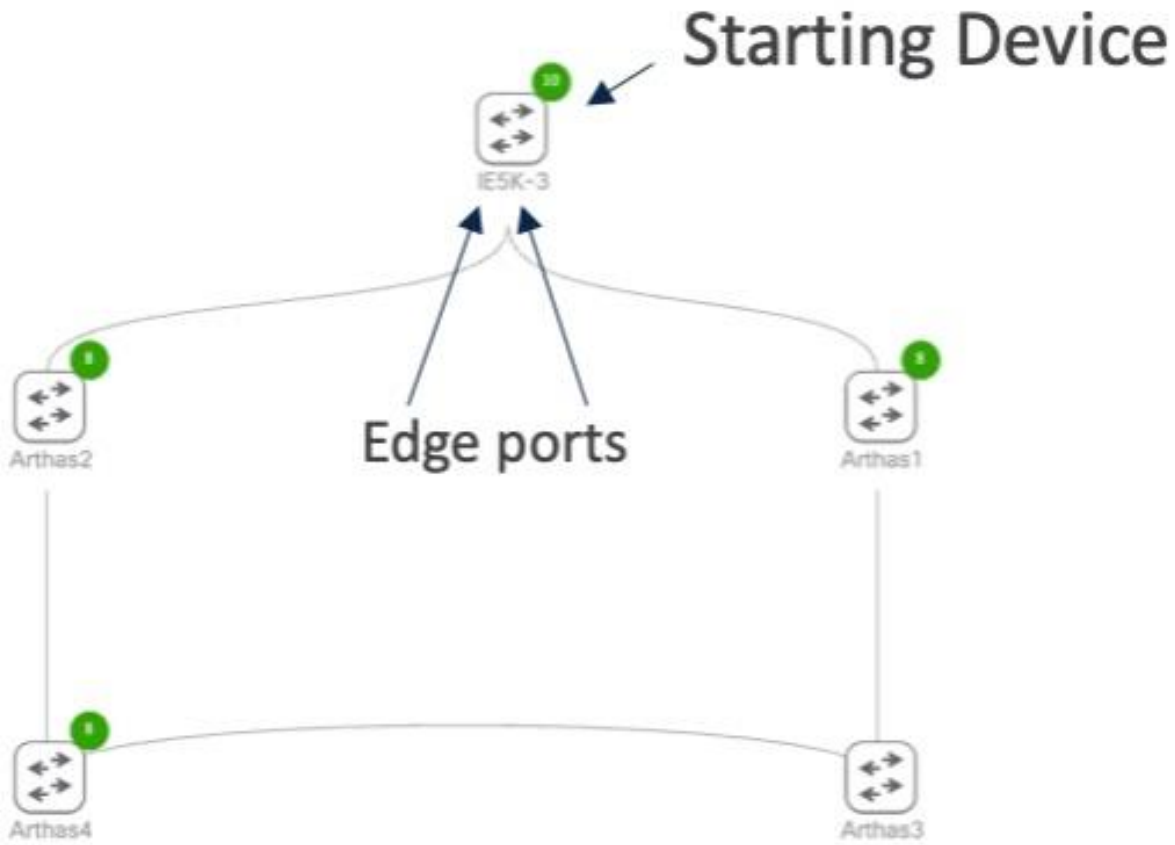
復元力のある設計により、機器やリンクに障害が発生した場合に代替パスが提供されます。セル/エリアゾーン内では、スタートポロジまたはリングトポロジを使用して、エッジ スイッチング プラットフォームからのアップリンクで、ネットワーク冗長性が提供されます。冗長リンク内のループを防止するには、レジリエンスプロトコルを展開する必要があります。Resilient Ethernet Protocol（REP）は、リングトポロジ内のループを防止するプロトコルの例です。

© 2025 Cisco and/or its affiliates. All rights reserved.

REP はシスコ独自のプロトコルで、スパニングツリープロトコル（STP）に代わるプロトコルとして、ネットワークループの制御、リンクまたはノード障害の処理、コンバージェンス時間の回避を実現します。REP は、セグメントまたは物理リングごとに単一の冗長インスタンスを操作します。REP セグメントは、相互接続されたポートから構成され、固有のセグメント ID があります。各セグメントには、標準セグメントポートと、2 つのユーザー設定のエッジポートが含まれます。ネットワークセグメントは、エッジポートと呼ばれる終端ポートを使用して、隣接する Cisco IE アクセススイッチまたはディストリビューション スイッチで終端します。リング内のループの防止は、セグメント内の 1 つのポート（代替ポートとも呼ばれます）をブロックすることにより行われます。セグメント障害が発生した場合、代替ポートはフォワーディングステートに移行し、トラフィックが代替パスを通過できるようにし、ネットワーク障害をバイパスします。

産業用自動化におけるレジリエンスプロトコルの詳細については、『Networking and Security in Industrial Automation Environments Design and Implementation Guide』を参照してください。

図 3.　Catalyst Center トポロジ図



注：　このワークフローでは、STP から REP への変換中に障害が発生します。

Catalyst Center REP 自動化ワークフローは、完全な REP リングを作成し、オープン REP セグメントの設定をサポートします。ワークフローを開始する前に、リング上のリンクをトランクとして設定する必要があります。デフォルトでは、REP リングワークフローは最大 18 台のデバイスをサポートしています。REP ノードの動的な追加と削除もサポートされています。次の手順は、ワークフローを使用して REP リングを作成した後に、未設定

© 2025 Cisco and/or its affiliates. All rights reserved.

のスイッチを使用して追加のノードをリングに追加する方法を示しています。REP リングのプロビジョニングについては、『Cisco Catalyst Center User Guide』を参照してください。

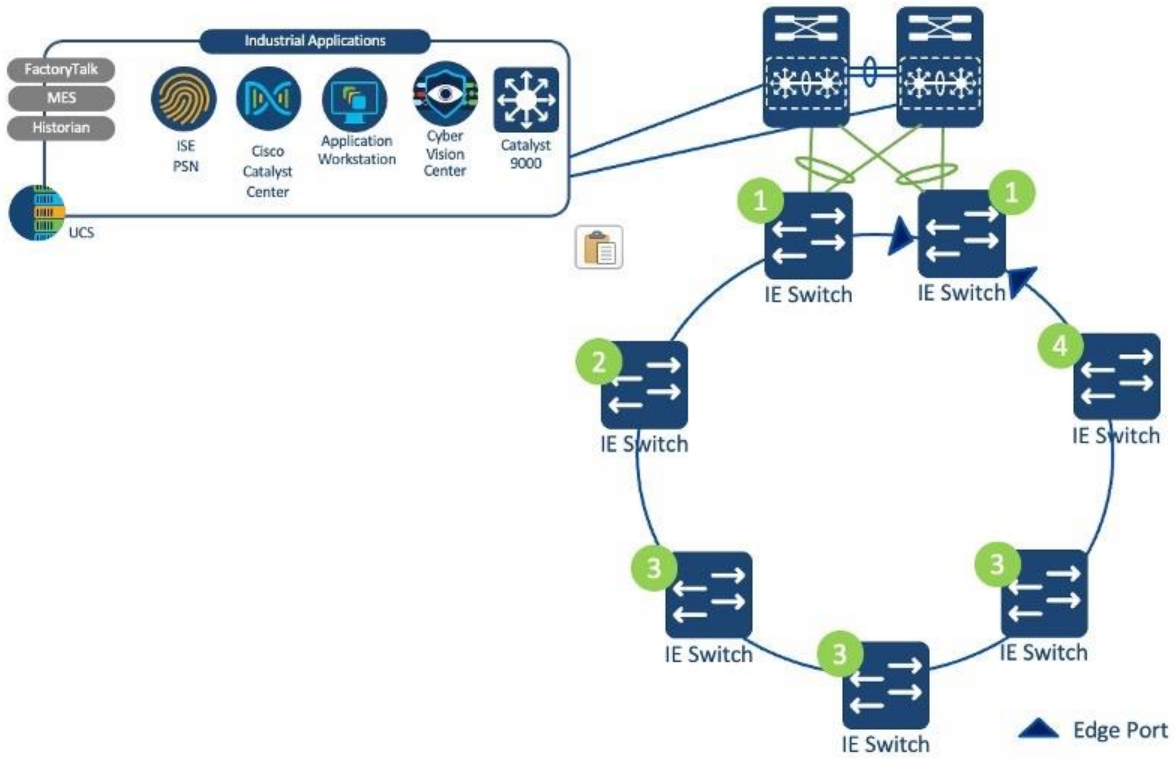
1. 手動で設定するか、Catalyst Center テンプレートを使用して、PnP のスタートアップ VLAN および DHCP プールの設定をリングスイッチにプッシュします。
2. 新しいノードが挿入される隣接インターフェイスをシャットダウンして、rep segment <#> コマンドがインターフェイスに適用されていることを確認し、REP を有効にしてインターフェイスにセグメント ID を割り当てます。
3. 隣接インターフェイスに rep ztp-enable コマンドを設定し、REP ZTP を有効にします。
4. 新しいデバイスを接続し、隣接インターフェイスのシャットダウンを解除します。新しいノードで PnP プロセスが実行されます。
5. 新しいデバイスを要求し、既存の REP リングと同じサイトに追加されたことを確認します。Catalyst Center により、新しいノードで関連インターフェイスに REP が自動的に追加されます。

REP ZTP

Catalyst Center REP ワークフローでは、ワークフローを開始する前に、Catalyst Center によってプロビジョニングおよび管理されるスイッチで構成された STP リングの存在が必須となります。または、産業用スイッチがオプションとして REP ZTP 機能を提供します。REP ZTP は、PnP プロセスを介した REP リングへのスイッチの直接プロビジョニングを容易にします。標準の運用シナリオでは、REP インターフェイスは、隣接スイッチとの REP 隣接関係が確立されるまでトラフィックが非アクティブのままです。しかし、REP ZTP はこの標準から逸脱し、未設定のスイッチに接続された REP インターフェイスを PnP メッセージが通過できるようにします。これにより、未設定のスイッチがポートの REP 設定を含む完全な設定を受信できます。PnP プロセスにより、スイッチは REP セグメントにシームレスに参加し、通常の動作モードに移行できます。

© 2025 Cisco and/or its affiliates. All rights reserved.

図 4.　REP ZTP プロビジョニングのワークフロー



REP ZTP プロビジョニングのワークフローは、次のように進行します。

1. リング内の最初のスイッチ（複数可）がプロビジョニングされ、これらのスイッチには REP リングに含まれないアップリンクがあります。リングインターフェイスは、REP セグメントを使用して設定する必要があります。REP ZTP をグローバルに有効にし、リングインターフェイスで設定する必要があります。
2. 新しい産業用スイッチが REP インターフェイスに接続されます。アップストリームスイッチが DHCP および PnP のフローを許可するため、新しいスイッチを設定できます。デバイスにプッシュされるオンボーディング テンプレートには、REP 設定が含まれています。PnP プロセスが完了すると、スイッチは通常の REP 動作に参加します。
3. 追加のスイッチは、ダウンストリームに一度に 1 つずつ接続されます。すべての新しいスイッチに対してステップ 2 が繰り返されます。
4. 最後のスイッチが接続されると、そのインターフェイスの 1 つだけで PnP プロセスが開始されます。ステップ 2 の説明に従ってスイッチがプロビジョニングされ、REP リングが動作するようになります。

ハードウェアとソフトウェアのサポートを含む REP ZTP 機能の詳細については、『Redundancy Protocol Configuration Guide』を参照してください。

REP ZTP と REP リング（非ファブリック）ワークフローの比較

次の表で、2 つの REP 自動化オプションを比較します。

Catalyst Center REP ワークフロー	REP ZTP
Catalyst Center によって管理される既存の STP リングとス	新しいスイッチまたは未設定のスイッチが必要であり、新しい REP

© 2025 Cisco and/or its affiliates. All rights reserved.

Catalyst Center REP ワークフロー	REP ZTP
イッチが必要であり、変換する必要がある既存のリングに適しています。	セグメントに適しています。
ウィザードベースのアプローチをサポートし、REP 設定用のテンプレートを必要としません。	テンプレートが必要です。
REP リングのみをサポートします（クローズセグメント）。	オープン REP セグメントをサポートします。
ノードの追加と削除をサポートします。	ノードの追加と削除をサポートします。
STP から REP に移行するときに障害が発生します。	デバイスのオンボーディング後に障害が発生することはありません。
Catalyst Center で、[Inventory] > [Device Details] ウィンドウに REP トポロジが表示されます	Catalyst Center で、[Inventory] > [Device Details] ウィンドウに REP トポロジが表示されません。CLI を介してのみ使用できます。

ソフトウェアイメージ管理（SWIM）

Catalyst Center の SWIM 機能により、IT ドメインと OT ドメインの両方で、ネットワークデバイスのソフトウェア管理を集中管理できます。

次の機能により、SWIM は、製造の展開における効率的で信頼性の高いソフトウェアイメージ管理のための有益なツールとなっています。

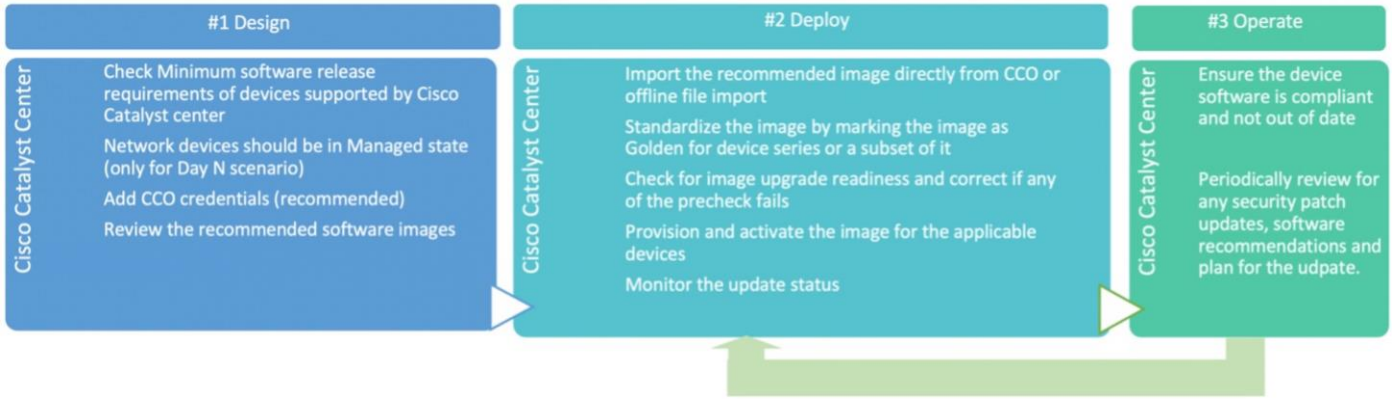
- コンプライアンス：SWIM は、特定のバージョンをゴールデンイメージとして指定できる管理者によって特定された正しいバージョンですべてのデバイスが動作していることを確認して、イメージのコンプライアンスを確保します。Catalyst Center は、優先バージョンを実行していないデバイスにフラグを付けます。イメージのコンプライアンスの確保に加えて、SWIM は使用中のソフトウェアバージョンに関連付けられたセキュリティアドバイザリと、そのセキュリティアドバイザリに対処するためのオプションの特定も支援し、ネットワークセキュリティを強化して潜在的脆弱性を軽減するために役立ちます。
- 大規模なアップグレード：製造の展開で通常見られる、広範なネットワークデバイスに対処する場合に重要な機能です。
- 事前チェックと事後チェック：ソフトウェア アップグレード プロセスには、アップグレードの前後にデバイスの正常性を評価するために、事前チェックと事後チェックの事前定義されたセットが組み込まれています。これらのチェックを製造ネットワークに合わせてカスタマイズして使用し、アップグレード後に悪影響がないことを確認することができます。たとえば、Cyber Vision Sensor のステータスを検証する、カスタマイズされた事後チェックがあります。
- 柔軟なアップグレード：製造の展開では、中断を最小限に抑えるために、ピーク外時間中に更新をスケジュールすることが不可欠です。SWIM により、ユーザーが定義した日時に更新を柔軟に計画して実行することができます。さらに、SWIM は、ソフトウェアイメージの配布とアクティベーションを 2 つの異なる期間に分離する柔軟性を提供します。このアプローチにより、実際のアクティベーションの前にデバイスでのゴールデンイメージのステージングができるため、全体的なアップグレード期間が大幅に削減されます。

Catalyst Center での SWIM 機能の使用方法の詳細については、『Cisco Catalyst Center User Guide』を参照してください。

© 2025 Cisco and/or its affiliates. All rights reserved.

次の図に、一般的な Catalyst Center の SWIM ワークフローの概要を示します。

図 5.　SWIM ワークフロー



注：　SWIM はアップグレードのために内部フラッシュメモリを使用します。SWIM を使用して SD カードから実行されているスイッチをアップグレードするには、内部フラッシュから起動するように再設定します。

Cisco IOS XE リリース 17.9.x 以前を実行しているシスコの産業用イーサネット（IE）スイッチでは、SD フラッシュメモリモジュール（SD カード）が存在する場合、カード上にイメージがないことを確認します。そうでない場合は、ソフトウェアメンテナンスの更新（SMU）と SWIM が機能しません。この場合は、内部フラッシュメモリをプライマリブートデバイスとして使用するようにスイッチを設定します。

ワイヤレス メッシュ ネットワーク

製造設備には、多くの場合、複雑なレイアウトを特徴とする広大なスペースが含まれます。ワイヤレス メッシュ ネットワークは、アクセスポイントの相互接続によってカバレッジを拡大し、施設の離れた場所に堅牢な無線信号強度を提供します。製造工場全体にイーサネットケーブルを設置することは、物理的障壁、機械、およびその他のロジスティクス上の制限により、困難な場合があります。この場合、ワイヤレス メッシュ ネットワークによって広範囲な配線を避け、迅速でより経済的な展開を実現できます。また、メッシュネットワークでは複数のデータ伝送経路が提供されるため、冗長性も実現します。干渉やデバイスの不具合が原因で 1 つのルートにアクセスできなくなった場合、このネットワークは代替の経路を介してトラフィックを適切にリダイレクトするため、一貫性と信頼性のある接続が維持されます。

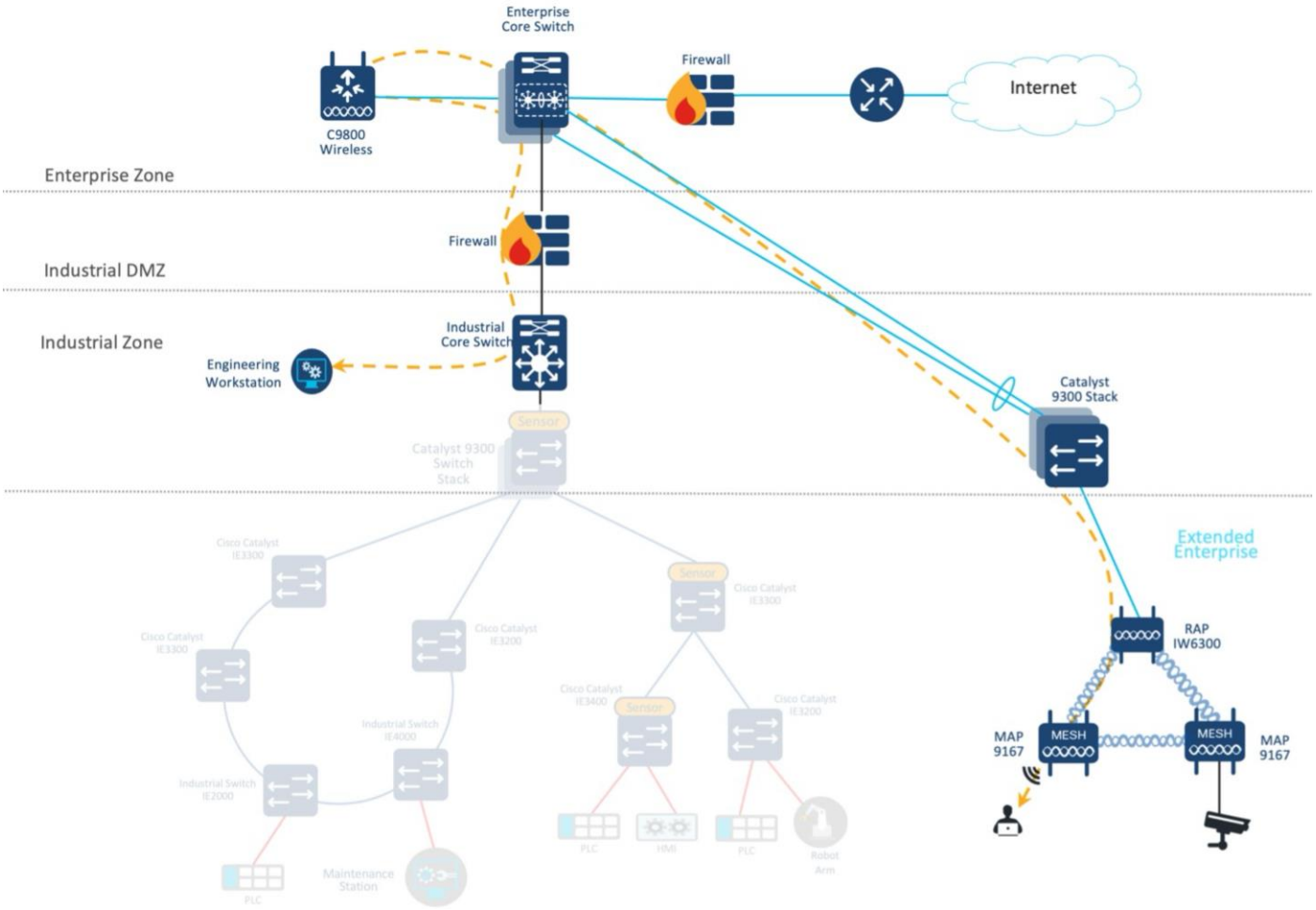
シスコ ワイヤレス メッシュ ネットワーク ソリューションにより、セキュアなワイヤレス LAN のコスト効率と拡張性に優れた展開が容易になります。これにより、固定アプリケーションとモバイルアプリケーションの両方にアクセスできるようになるため、安全性、効率性、生産性、および応答性が向上します。これは Cisco Unified Wireless Network アーキテクチャ内でシームレスに統合できるため、企業 WLAN のカバレッジを製造工場フロアまで拡張することを目標とするお客様にとって、自然な選択肢となっています。

Catalyst Center のネットワーク自動化機能は、ワイヤレス メッシュ ネットワークの完全な機能を実現するために重要な役割を果たします。さらに、Cisco Catalyst Assurance によって提供される高度なモニタリング機能を使用して、ネットワークパフォーマンスを効率的に追跡できます。メッシュアクセスポイント（MAP）には、MAC アドレスリストを利用したセキュアなオンボーディングが行われます。このリストは、CSV アップロードプロセスを介して、Catalyst Center 内の AP 承認リストに簡単に統合できます。Catalyst Center を使用してメッシュネットワークを立ち上げる方法の詳細については、『Cisco Catalyst Center User Guide』を参照してください。

次の図は、フロア オペレーション マネージャが、Extended Enterprise Wi-Fi ネットワークを介して産業ゾーン内のエンジニアリング ワークステーションにどのようにアクセスするかを示しています。

© 2025 Cisco and/or its affiliates. All rights reserved.

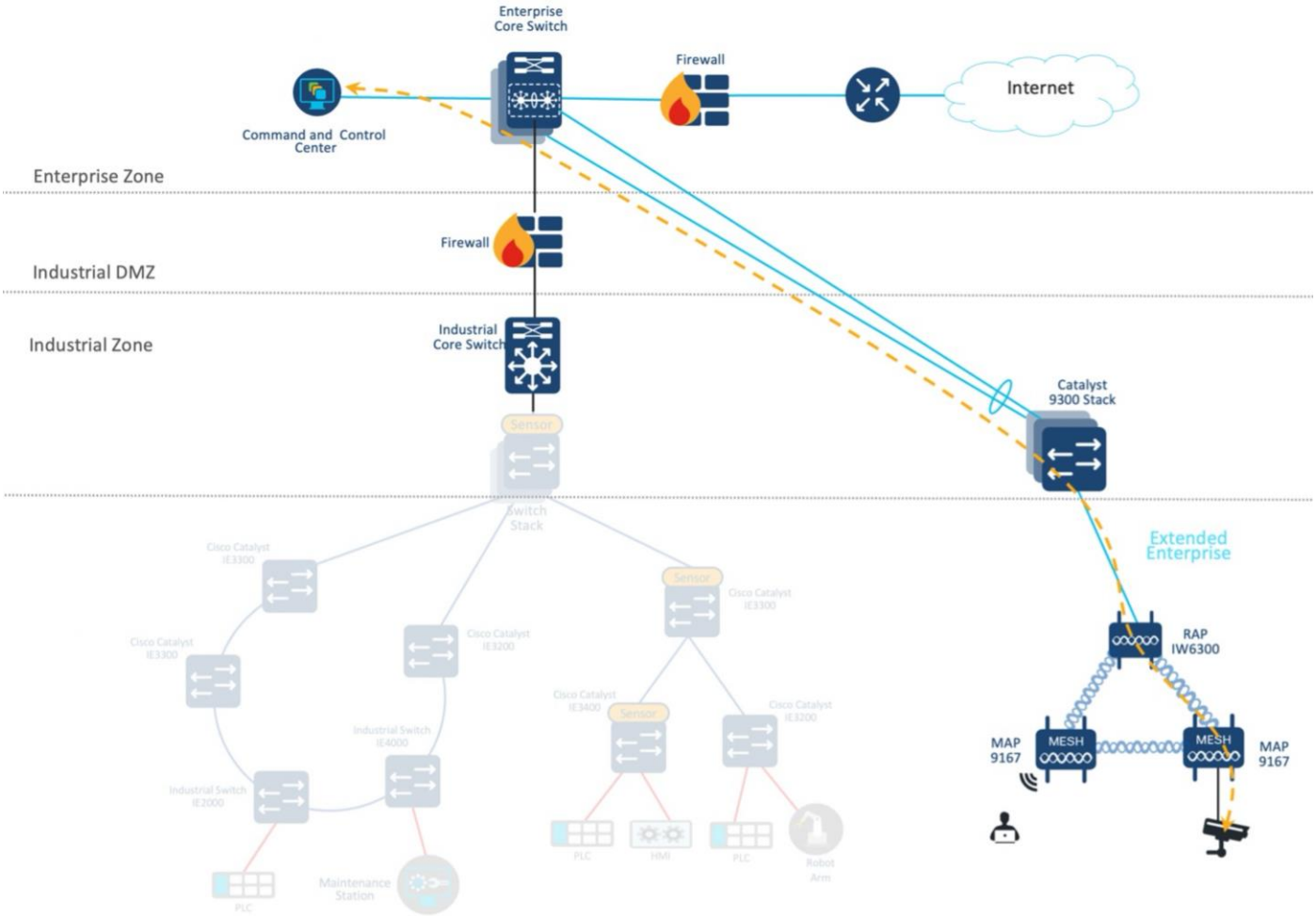
図 6.　Extended Enterprise Wi-Fi ネットワーク



ワイヤレス メッシュ ネットワークは、工場の運用と通信をサポートする他のマルチサービスまで拡張できます。工場フロア内には、重要ではないマルチサービスユニットのカテゴリに分類されるデバイスが存在する場合があります。セキュリティバッジアクセス、監視カメラ、テレフォニーなどのこれらのユニットは、性質的に重要ではありませんが、有線ネットワーク接続を必要とします。幸いなことに、統合用のイーサネット ブリッジング ソリューションを使用すると、ワイヤレス メッシュ ネットワークにこれらのデバイスをスムーズに含めることができます。次の図は、産業ゾーンのコマンド アンド コントロール センターにフィードを送信するメッシュ AP の有線イーサネットポートに IP カメラをどのように接続するかを示しています。

© 2025 Cisco and/or its affiliates. All rights reserved.

図 7.　Extended Enterprise Wi-Fi ネットワークのマルチサービスのサポート



Catalyst Center は、イーサネット ブリッジング ソリューションを実現するためのインテントベースのネットワーク自動化をまだサポートしていません。このプロファイルの検証では、Catalyst Center CLI テンプレートを使用して必要な設定を有効にします。Cisco Catalyst 9800 ワイヤレスコントローラでイーサネット ブリッジング ソリューションを有効にする方法については、『Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide』を参照してください。

セキュリティ

以降の項では、ネットワークセキュリティに関連した機能の導入について説明します。

Cisco Cyber Vision による運用テクノロジーネットワークの可視性

可視性の欠如は、産業用ネットワークの一般的な課題です。これらのネットワークは非常に古く、広範囲に分散していて、多くの請負業者が関与している可能性があるため、多くの場合、運用担当者は、ネットワーク上にどのような機器があるかを正確に管理できていません。

そのため、セキュアな通信アーキテクチャを構築することが困難になっています。可視性が欠如しているということは、どのデバイスが相互に通信しているかを運用担当者が把握していないことが多く、さらには、外部から産業用デバイスに接続している通信さえ認識できていない可能性があるということです。可視性の欠如は、最終的には、セグメンテーションや制御の欠如につながります。

OT の可視性は、OT 環境のすべてのペルソナが使用できるテクノロジーです。OT オペレータは、プロセスレベルの可視性を活用して、製造現場に存在する設備を特定してトラブルシューティングすることができます。IT オ

© 2025 Cisco and/or its affiliates. All rights reserved.

ペレータは、デバイスの通信パターンに関するインサイトを得て、ネットワーク効率を向上させることができます。セキュリティチームは、デバイスの脆弱性とデバイスの通常の動作からの逸脱に関するインサイトを得ることができます。可視性は次の点で重要です。

- すべてのアセットを特定し、それらをゾーンにグループ化します。
- ゾーン間のコンジットを流れるデータを可視化します。
- 外部ネットワークを介して着信するソースデータを明確に把握できます。

Cisco Cyber Vision は、産業用ネットワークの可視性のニーズに対応します。Cisco Cyber Vision は、産業用ネットワーク内のディープ パケット インスペクション、プロトコル分析、および侵入検知を実行する複数のセンサーデバイスで構成される固有のエッジアーキテクチャ上に構築されています。Cyber Vision Center はアグリゲーション プラットフォームとして動作し、センサーからのデータを保存し、ユーザーインターフェイス、分析、振る舞い分析、レポート作成、API などを提供します。産業用自動化ネットワークにおける Cisco Cyber Vision の詳細については、『Industrial Automation Security Design Guide 2.0』を参照してください。

Cisco Cyber Vision Sensor は、Catalyst Center によって管理されるスイッチに展開されます。テンプレートを使用して、Catalyst Center を介してセンサーを設置できるように産業用スイッチを準備することができます。

Cisco TrustSec を使用したセグメンテーション

セグメンテーションは、IACS のネットワークとプロセスを保護するための信頼ゾーンを作成するために重要な役割を果たします。IEC 62443 には、プロセスネットワークまたはサービスの間の不要なデータフローを制限し、制御システムをゾーンおよびコンジットに分割するための制限付きデータフローの推奨事項が提供されています。これは、信頼できないエンティティ間のトラフィックの意図しない相互作用や偶発的な相互作用を防ぐために役立ちます。産業用セキュリティソリューションは、セル/エリアゾーントラフィックをセグメント化するための論理的分離に関する基本的なガイダンスを提供します。

産業用自動化アーキテクチャでのセキュリティプロセスは、企業ネットワークと OT ネットワークのセグメント化から始まります。これは、IDMZ の導入によって実現できます。IDMZ は、企業ネットワークと OT ネットワークの間にセキュアな境界を提供し、制御されたアクセスを実現して重要な設備を保護します。IDMZ の詳細については、『Securely Traversing IACS Data across the IDMZ Using Cisco Firepower Threat Defense』を参照してください。

インテントベースのセキュリティにより、管理者は運用上の意図を示し、IT によって定義された適切なセキュリティポリシーを自動的に選択することができます。特殊なネットワークやセキュリティのスキルは必要ありません。

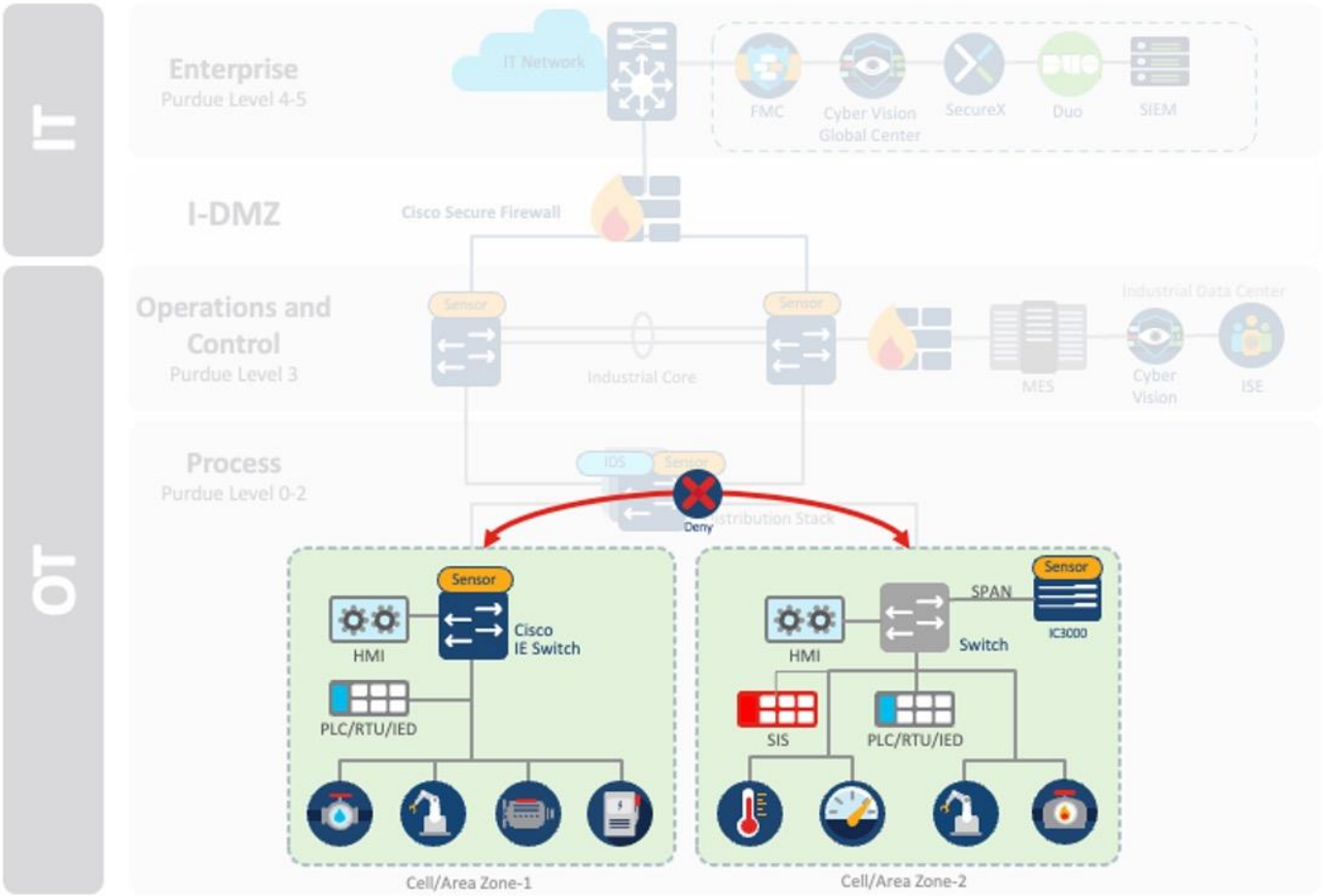
Catalyst Center が Cisco ISE と統合されると、Cisco TrustSec を使用したインテントベースのセキュリティが有効になります。Cisco TrustSec は SGT を使用して、ユーザーまたはデバイスプロファイルのグループにポリシーを適用します。これらのポリシーは、各組織の展開に応じてカスタマイズされます。

産業用ネットワークでは、次のような、セキュアなアクセスを必要とするさまざまな一般的なユースケースとペルソナがあります。

- セル/エリアゾーン：このゾーンは複数のセル/エリアゾーンで構成され、同じゾーン内のデバイスが無制限に通信できる必要があります。ただし、異なるゾーン間の通信は、明示的に許可されていない限り、デフォルトで拒否される必要があります。

© 2025 Cisco and/or its affiliates. All rights reserved.

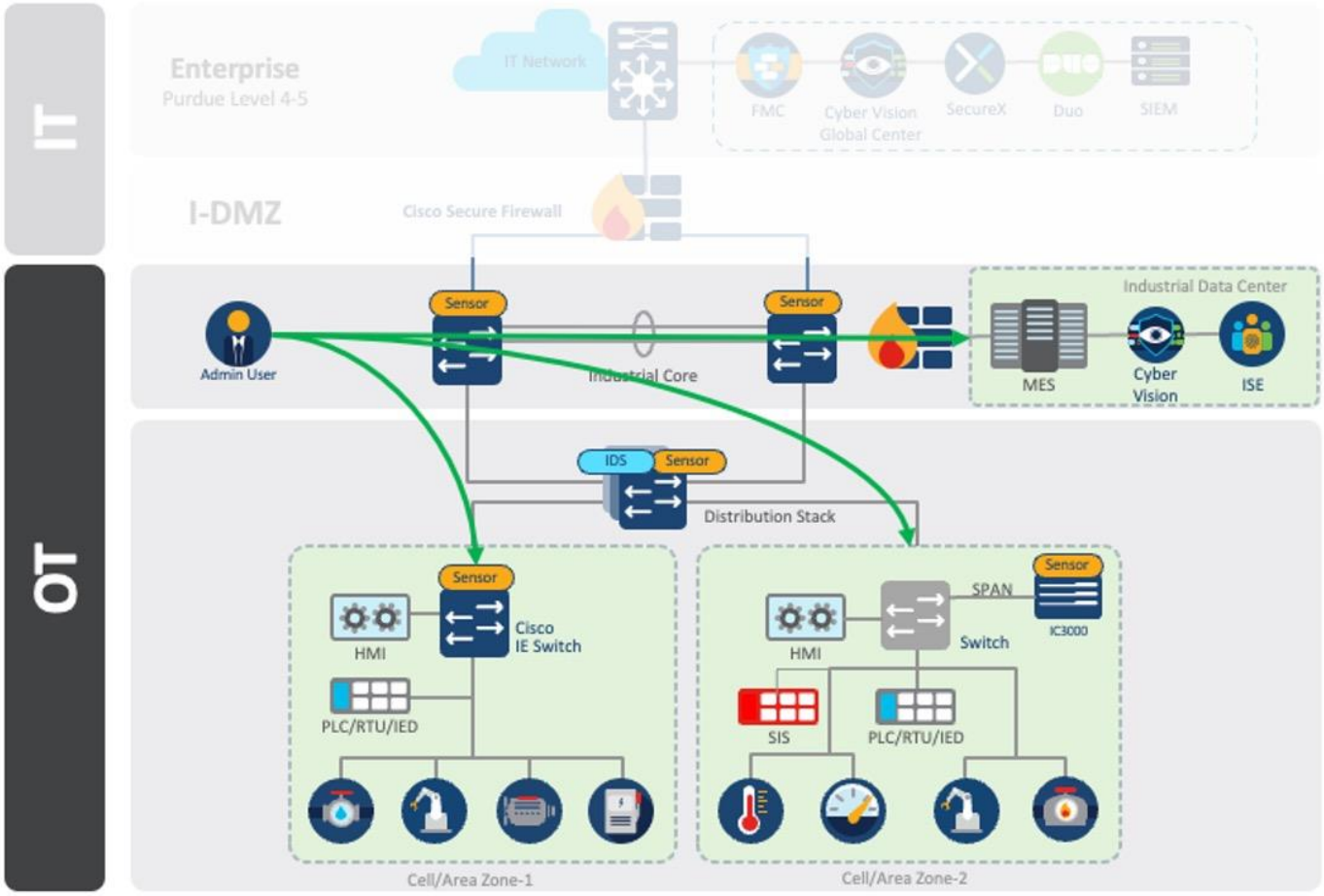
図 8.　セル/エリアゾーン間のセグメンテーション：デフォルトで拒否



- 管理ユーザー: これらのユーザーは、ネットワーク インフラストラクチャの設定や制御ロジックアプリケーションなどのタスクのために、ネットワーク内のすべてのゾーンにアクセスする必要があります。これらのユーザーのアクセスは制限するべきではありませんが、そのデータは保護する必要があります。

© 2025 Cisco and/or its affiliates. All rights reserved.

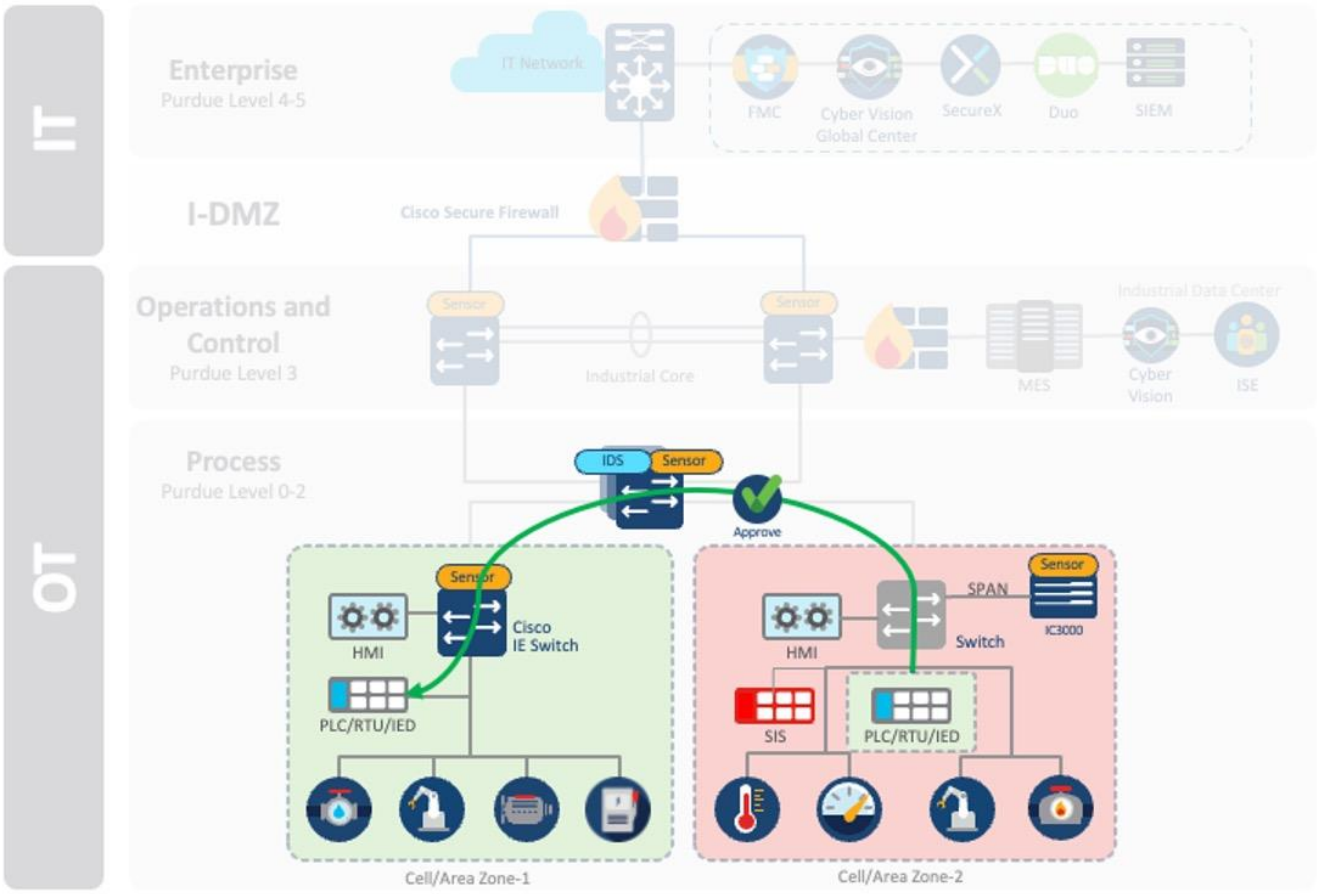
図 9.　セグメンテーションで許可される管理アクセス



- インフラストラクチャ サービス：DHCP、NTP、LDAP サービスなどの、ユーザープレゼンスはないものの、工場の重要な部分にアクセスする必要があるエンドポイント。
- 工場全体でのアプリケーション：工場フロアの機器のモニタリングとメンテナンスのために使用される、分析プラットフォームやベンダーツールなどの、特定のアクセス要件がある産業用データセンター（IDC）内のアプリケーション。
- メンテナンス ワークステーション：これらのワークステーションは、セル/エリアゾーンの外部に存在して特定のゾーンのメンテナンスマシンとして機能するか、セル/エリアゾーン自体の中に存在する場合があります。ただし、ゾーンを離れる場合はより多くの権限を必要とします。
- インターロック プログラマブル ロジック コントローラ（PLC）またはゾーン間通信：一部の産業用通信は、分散型自動化機能のために複数のゾーンを通過する必要がある場合があります。ただし、マルウェアの拡散を防ぐために、厳密な権限ポリシーを適用して有効な通信のみが許可されるようにする必要があります。

© 2025 Cisco and/or its affiliates. All rights reserved.

図 10.　インターロック PLC で許可されるセル/エリアゾーン間通信



- コンビニエンスポート：インフラストラクチャに直接接続するオペレータは、上位のアーキテクチャレイヤで導入されているセキュリティチェックをバイパスする可能性があります。承認されたデバイスポスチャを持つ承認ユーザーのみがネットワークに接続できるようにすることで、このユースケースを保護できます。
- 安全ネットワーク：安全計装システム（SIS）は制御ネットワークにとって重要であり、このゾーンへのデータ漏洩を防ぐために、エアギャップ化されているか論理的にセグメント化されている必要があります。
- リモートユーザー：リモートアクセスは、一般的に、メンテナンス、プロセスの最適化、およびトラブルシューティングのために、従業員、パートナー、およびベンダーに付与されます。限られた時間での工場フロアの特定のデバイスへのアクセスに制限する必要があります。

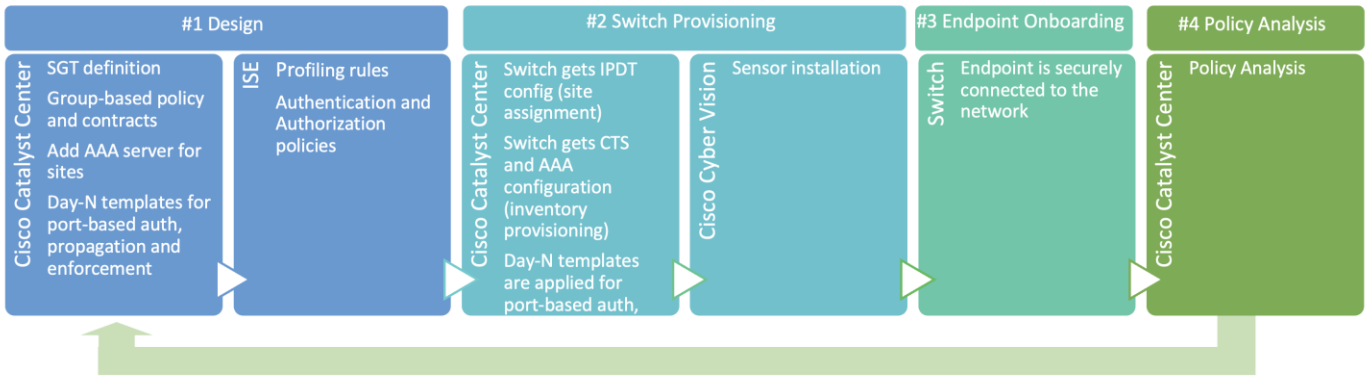
Cisco TrustSec でセグメンテーションを展開するための最初のステップは、タグの伝達方法や適用ポイントなどのセキュリティ設計を定義することです。また、Cisco Cyber Vision Center を使用する場合は、効果的な可視性を確保するためのセンサー配置を事前に決定する必要があります。

設計の詳細については、『Industrial Automation Security Design Guide 2.0』を参照してください。Catalyst Center は、必要なツールと機能を提供することで、ポリシーの適用をサポートします。

次の図に示すセキュリティワークフローは、Cisco TrustSec の展開時に Catalyst Center がどのように重要な役割を果たすかを示しています。

© 2025 Cisco and/or its affiliates. All rights reserved.

図 11.　セキュリティのワークフロー



このセキュリティワークフローは、次の段階を示しています。

ステップ 1.　設計アクティビティとは、セキュリティ設計に基づく設定のことを指します。これらの設定は、ネットワークデバイスまたはエンドポイントがオンボードされる前に実行できます。Catalyst Center は、ネットワークデバイスにプッシュされる Cisco TrustSec のポリシー、設定、およびテンプレートを定義するために使用されます。

ステップ 2.　スイッチのプロビジョニングとは、スイッチをネットワークにオンボードするアクションのことを指します。この段階では、フェーズ 1 で定義されているように、設定がデバイスにプッシュされます。

ステップ 3.　エンドポイントはネットワークにセキュアに接続し、ポリシーで許可されているとおりに通信を開始することができます。

ステップ 4.　ポリシー分析は、通信パターンを理解し、ポリシーを改善するために行われます。ポリシー分析は、エンドポイント、グループ、およびアプリケーション間のアクティビティを検出する Catalyst Center の機能です。ポリシー分析については、「グループベースのポリシー分析」の項で説明しています。

Cisco TrustSec を使用してゾーンにデバイスを検疫するための Cisco Cyber Vision の使用

Cisco Cyber Vision では、Cyber Vision Knowledge Database（DB）に保存されているルールを使用して脆弱性が検出されます。これらのルールは、CERT（コンピュータ緊急対応チーム）、製造業者、パートナー製造業者などの、さまざまな信頼できるエンティティから提供されています。脆弱性の検出は、これらの Knowledge DB ルールと正規化されたデバイスおよびコンポーネントのプロパティを関連付けることで実現されます。デバイスまたはコンポーネントが Knowledge DB 内のルールと一致すると、脆弱性が特定されます。デバイスに重大な脆弱性があることや、何らかの方法で侵害されていることが判明した場合、オペレータはそのデバイスを Cisco Cyber Vision の検疫グループに割り当てることができます。その後、この情報が Cisco ISE に伝達され、デバイスに新しい SGT が割り当てられます。この新しい SGT は、必要なパッチまたは修復措置が適用されるまで、デバイスの通信を制限します。

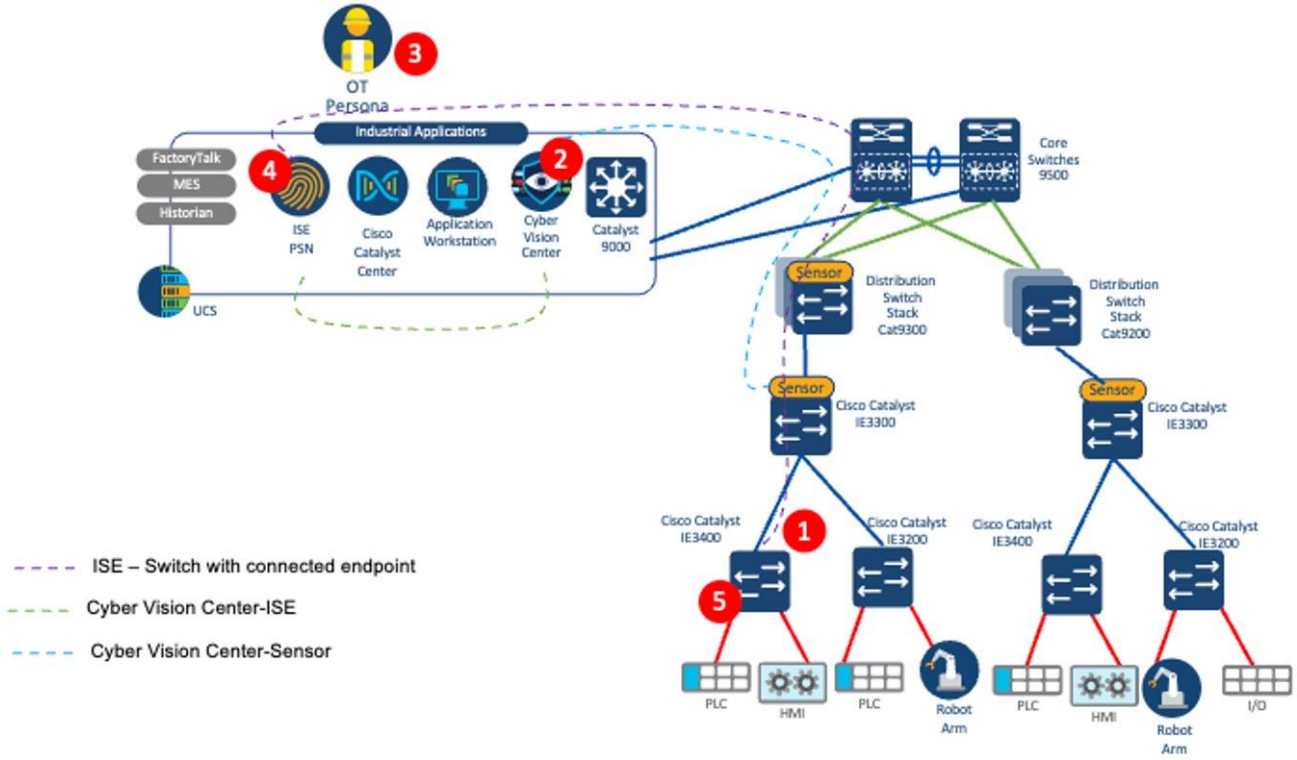
ワークフローは次のようになります。

1. デバイスがネットワークに接続されます。Cisco Cyber Vision Sensor がデバイスを検出し、情報を Cisco Cyber Vision Center に送信します。
2. デバイスの特性がルールに一致する場合、Cisco Cyber Vision Knowledge DB がデバイスの脆弱性アラートを生成します。
3. OT エンジニアが、推奨されるアクションを確認しましたが、ダウンタイムが発生する可能性があるため、すぐには展開できません。OT エンジニアが Cisco Cyber Vision Center の検疫グループにデバイスを割り当てます。

© 2025 Cisco and/or its affiliates. All rights reserved.

4. Cisco Cyber Vision Center が pxGrid を介してこの情報を Cisco ISE に送信します。Cisco ISE が新しいコンテキストでデバイスをプロファイリングします。
5. Cisco ISE がデバイスに接続されているスイッチに認可変更を送信し、新しい SGT が割り当てられます。

図 12.　Cyber Vision から Cisco ISE TrustSec へのワークフロー



産業用ネットワークからのインサイトを利用した統合セキュリティ オペレーション センター

運用ネットワークの相互接続性とサイバー脅威に対する脆弱性の増加を考慮して、産業用ネットワークの管理者は、組織の情報セキュリティチームの専門知識を利用できます。コラボレーション ワークフローを確立することで、これらの攻撃に効果的に対処できます。これに関連して、工場フロアのサイト運用センター（SOC）での異常の特定に関するシナリオを確認できます。これは、Cisco Secure Network Analytics のフローベースの逸脱検知機能によって実現され、Cisco Cyber Vision Center が提供する製造ネットワークに関するコンテキストに基づくインサイトによって補完されます。このコラボレーティブな取り組みにより、セキュリティインシデントを包括的に確認できるようになり、調査と修復のプロセスが合理化されます。

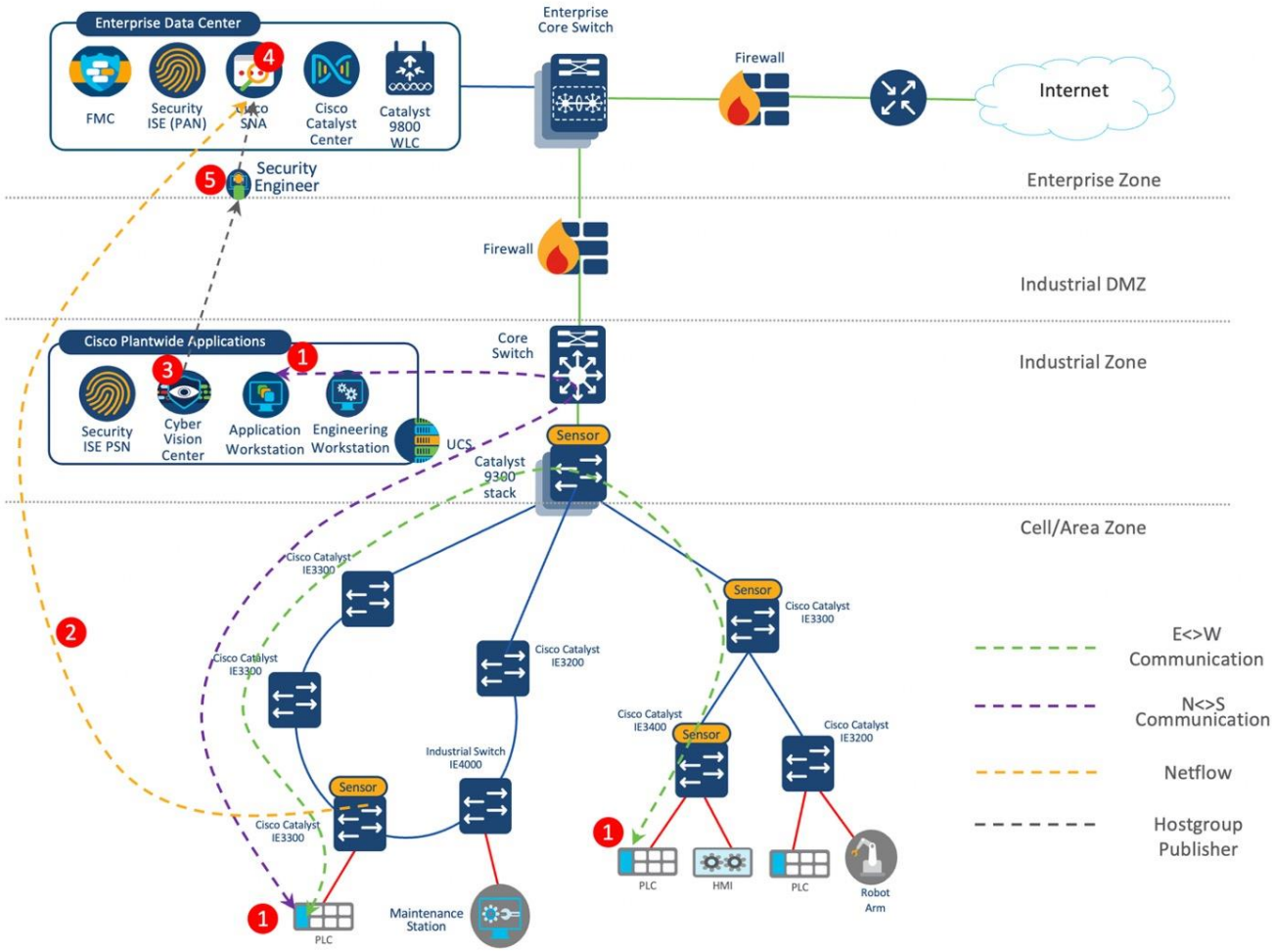
次の手順では、セル/エリアゾーンおよびレベル 3 の動作におけるマルウェア検出のワークフローについて説明します。

1. ゾーン全体の PLC 間の East-West 通信と、サイト運用センターのエンジニアリング ワークステーションとセルエリア内の PLC 間の North-South 通信が、許可されるフローです。
2. IE スイッチは NetFlow が有効にされ、NetFlow レコードを Cisco Secure Network Analytics Flow Collector に送信します。
3. 産業ゾーン内の Cisco Cyber Vision が、さまざまな IE デバイスに展開された Cisco Cyber Vision センサーを使用したパッシブモニタリングに基づいて、産業用プロトコルのディープ パケット インスペクション（DPI）を行います。Cisco Cyber Vision からのこれらのインサイトが、Cisco Secure Network Analytics がモニターするネットワークフローにコンテキストを追加します。

© 2025 Cisco and/or its affiliates. All rights reserved.

4. Cisco Secure Network Analytics マネージャが、フローコレクタからのデータに基づいて構築済みアルゴリズムを実行し、上記のネットワークフローで発生している悪意のあるアクティビティを示すアラームを報告します。
5. IT セキュリティアーキテクトが後続の修復手順を策定してアラートに対応します。これには、より多くの調査を実施する、IACS 設備のアクセスに制限を課すなどの対策が含まれます。

図 13.　Cisco Cyber Vision から Cisco Secure Network Analytics へのマルウェア検出ワークフロー



ネットワークのモニタリングとトラブルシューティング

以降の項では、ネットワークのモニタリングとトラブルシューティングに関連した機能の導入について説明します。

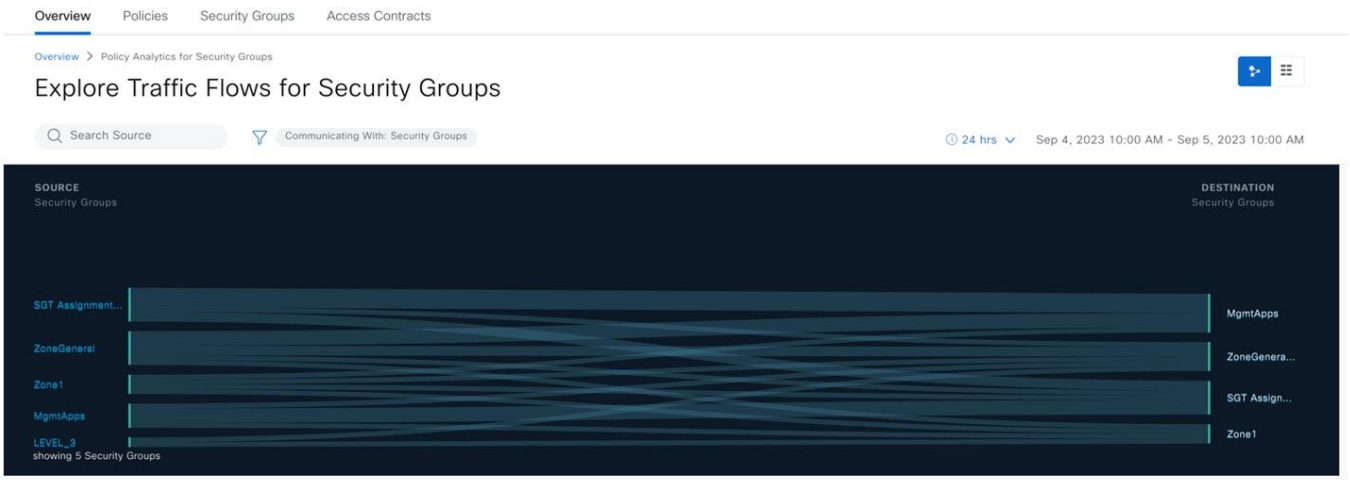
グループベースポリシーの分析

セグメンテーションは信頼ゾーンの確立において重要な役割を果たし、IACS ネットワークと運用の保護を強化します。データの移動を制御して、コントロールシステムを個別のゾーンと経路に分割することは、広く受け入れられている方法です。この分割により、さまざまなプロセスのネットワークまたはサービス間での余分なデータ交換が最小限に抑えられます。信頼できないエンティティ間では、不注意による情報交換または意図的な情報交換を抑制することが不可欠です。Catalyst Center のグループベースのポリシー分析機能が、工場フロアのセル/ゾーンエリア内のさまざまなセキュリティグループ間の通信パターンを可視化するために役立ちます。この可視性の向上は、これらの SGT を制御する適用ルールを改善する際に役立ちます。具体的には、グループベースのポリシー分析により、これらのグループ間のプロトコルおよびポートレベルで、通信の詳細に関する正確なイン

© 2025 Cisco and/or its affiliates. All rights reserved.

サイトを提供できます。この機能は初期アラートメカニズムとして機能し、これらのグループ間で発生している意図しない通信の早期特定のために役立ちます。

図 14.　セキュリティグループのポリシー分析



AI エンドポイント分析

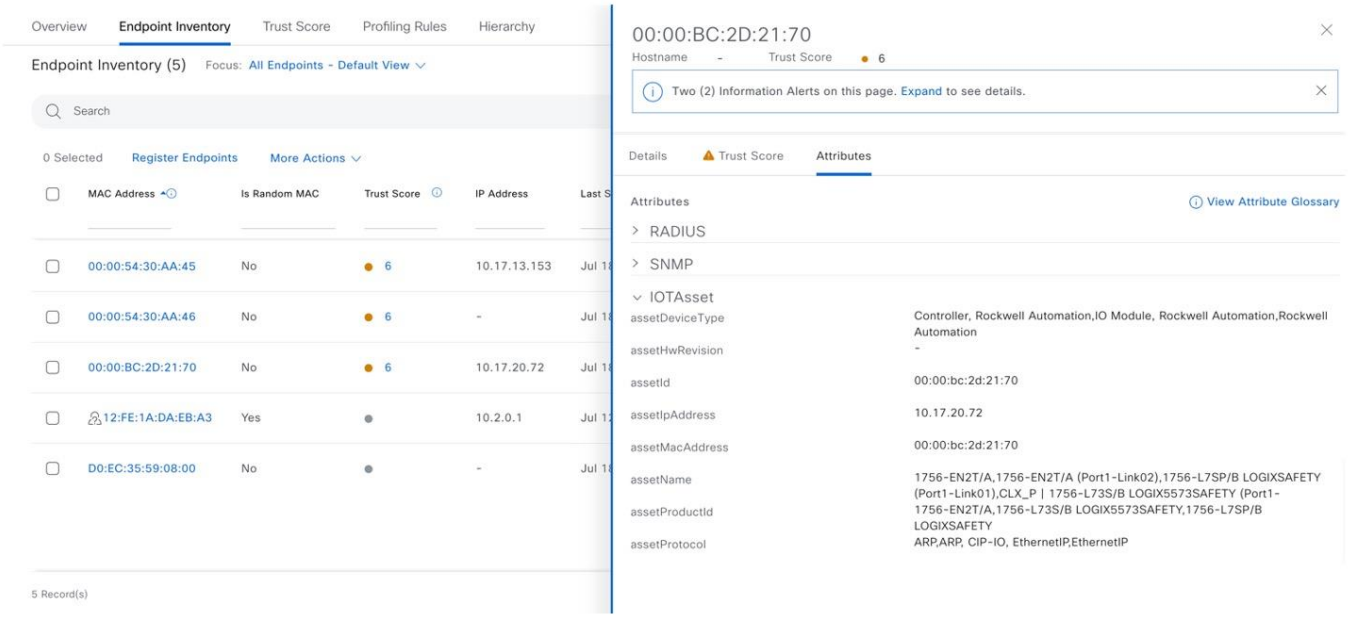
可視性を得ることは、エンドポイントセキュリティを強化するための最初の取り組みとなります。エンドポイントを詳しく調査し、多数の要素によって分類することが重要になります。このプロセスは、エンドポイントをグループ化し、築かれた可視性に基づいて構築された正確なセキュリティポリシーを形成するために役立ちます。

Cisco AI Endpoint Analytics は Catalyst Center 内のアプリケーションであり、個別のラベルの割り当てを通じてエンドポイントを識別および分類するために設計されています。このアプローチは多要素分類（MFC）と呼ばれ、個々のエンドポイントに複数のラベルが割り当てられます。AI 主導のエンドポイント分析エンジンが、Cisco ISE や、Cisco Catalyst 9000 シリーズ スイッチによって実施されるディープ パケット インスペクションなどのソースを含む、さまざまな発信元からエンドポイントメタデータを取得します。このインスペクションでは、Network-Based Application Recognition（NBAR）テクノロジーが活用されます。

製造工場アクセスネットワークでの IE スイッチに対する依存を考慮すると、AI エンドポイント分析のプライマリデータソースは Cisco ISE です。この情報は、Cisco Cyber Vision から発信されたエンドポイントメタデータによって補強されます。後者では、産業用プロトコルでの DPI が実施されてから、エンドポイントに関連ラベルが割り当てられます。これらの拡充された詳細は、後で Cisco ISE から Cisco AI エンドポイント分析エンジンに送信されます。このプロセスにより、Catalyst Center 内に IT エンドポイントと OT エンドポイントの両方を含む、統合されたビューポイントが作成されます。

© 2025 Cisco and/or its affiliates. All rights reserved.

図 15.　AI エンドポイント分析



注：　一般に、エンドポイント分析を使用して、Cisco ISE ではなく Catalyst Center でプロファイリングルールを作成してエンドポイントをプロファイリングすることはできますが、Catalyst Center のプロファイリングルールはプロファイリングの IoT 設備属性をまだサポートしていません。

ネットワークアシュアランス

ネットワークの問題のトラブルシューティング

ネットワークデバイス 360 は、ネットワークの問題が報告されている場合のトラブルシューティングに役立つツールです。オペレータは、Catalyst Center を使用してネットワーク接続の問題を分析および診断することができます。

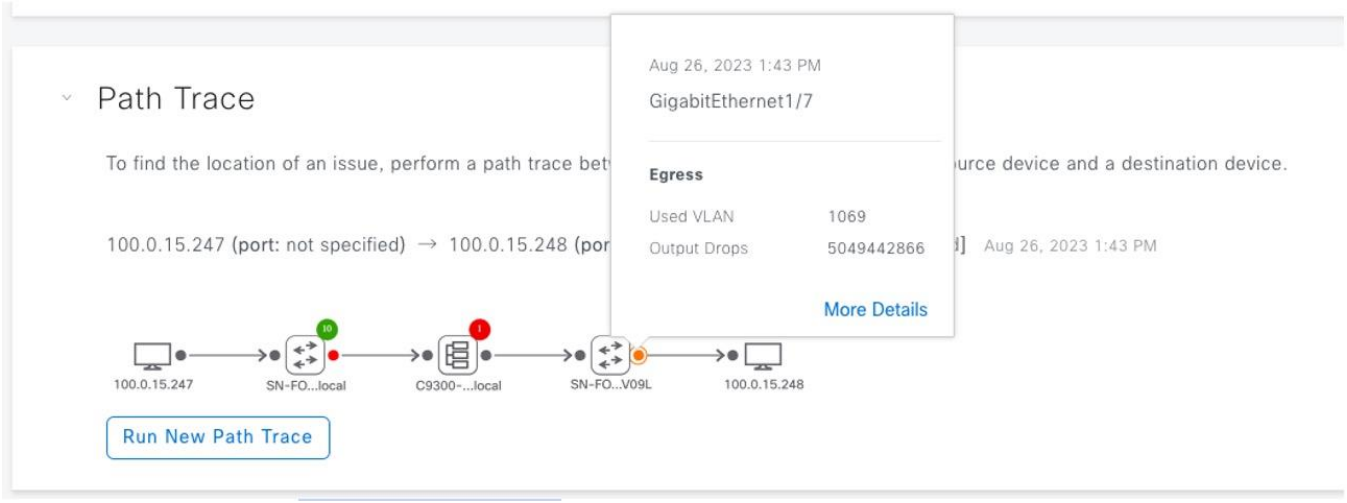
トラブルシューティング プロセスを開始するために、オペレータは Catalyst Center にログインし、パストレース機能を使用します。パストレース機能ではエンドツーエンドのネットワーク接続の包括的なビューが提供され、オペレータが通信パスに沿って潜在的な問題を特定できます。

パストレースでは、通信パスの可用性が確認されるだけでなく、パスに沿ったデバイスの正常性スコアも評価されます。この正常性スコアはクライアント、デバイス、およびネットワークに割り当てられるため、オペレータは潜在的な問題を迅速に特定し、トラブルシューティングの取り組みに優先順位を付けることができます。

次の図は、パストレースの出力を示しています。パス内のデバイスの正常性スコアが表示され、パケットドロップがあるインターフェイスが強調表示されています。オペレータは、パストレースの出力に表示されているネットワークパス内の任意のスイッチから移動して、対応する [Device 360] ウィンドウを開くことができます。この機能により、通信パスに沿って各デバイスの特定の詳細を容易に把握できます。

© 2025 Cisco and/or its affiliates. All rights reserved.

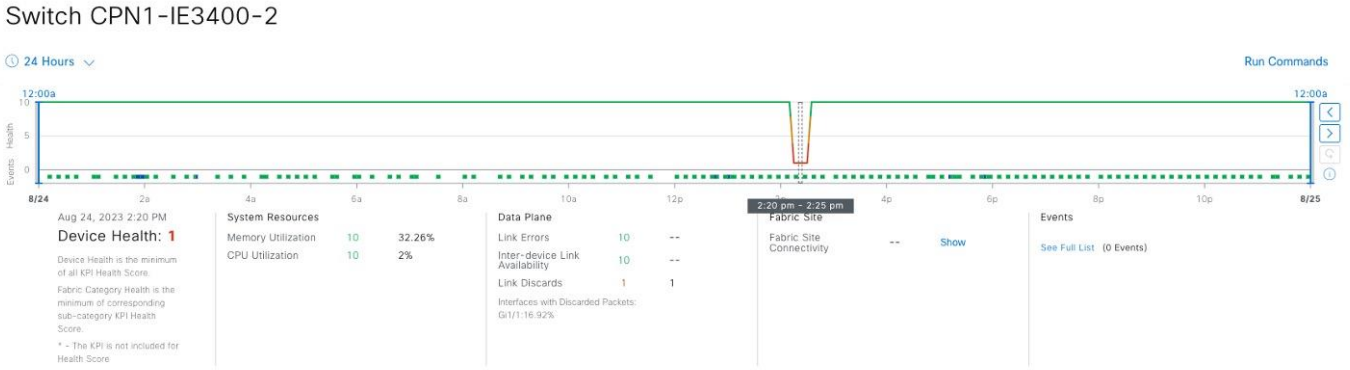
図 16.　アシュアランスのパストレース



[Device 360] ページには各デバイスに関する詳細情報が表示されるため、ユーザーは対処する必要がある潜在的な問題があるかどうかを判断できます。Catalyst Center の [Device 360] ページとその他のアシュアランスページ内で、オペレータはタイムラインを介して過去および現在の重要業績評価指標（KPI）を示すグラフを調べることができます。これらの KPI グラフでネットワークの状態に関する経時的観点が提供されるため、オペレータは任意の時点でのネットワークの正確な状態を把握できます。この情報は、問題の根本原因を特定したり、繰り返されるパターンを特定したりするために非常に役立ちます。

次の図は、特定のインターフェイスでのリンク破棄により、正常性スコアが一時的に低下した例を示しています。

図 17.　アシュアランスの正常性スコア



Catalyst Center のデバイス 360 では、次の情報も提供されます。

- デバイスに関する報告された問題とイベントの可視性。ユーザーは、さらなる分析のために特定の問題に対して簡単にアクセスして調査することができます。
- 物理ネイバートポロジには、クライアントとネイバーのネットワークデバイスが表示されます。リンクまたはデバイスをクリックすると、追加情報が表示されます。
- CPU、メモリ、稼働時間、温度などの詳細なデバイス情報。
- 名前、説明、動作ステータス、リンク速度などのインターフェイス情報。
- インターフェイスの使用率、エラー、および破棄のチャート。

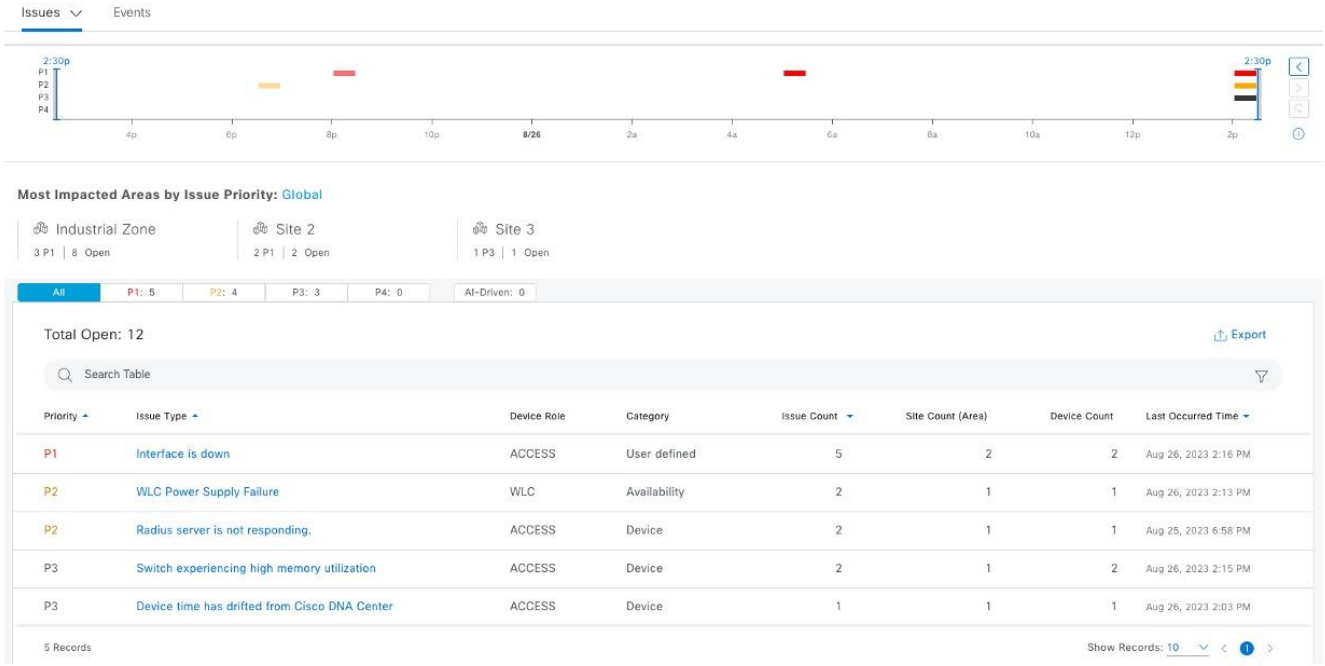
優先順位の高い問題への対処

© 2025 Cisco and/or its affiliates. All rights reserved.

Catalyst Center の [Issues] ダッシュボードでは、ネットワークの対処する必要がある問題が優先順位別に特定されます。時系列に沿って問題が示されているグラフが提供され、カラーコードを使用して優先順位と重大性が示されます。色の明度は、その優先順位レベルで発生した問題数の多寡を示します。

このダッシュボードでは、次の図に示すように、優先順位別に整理された問題のリストが提供されます。そのタイプの問題が発生した回数、影響を受けたサイトの数、影響を受けたデバイスの数、およびその問題が発生した最新の日時が表示されます。

図 18.　アシュアランスの [Issues] および [Events] ダッシュボード

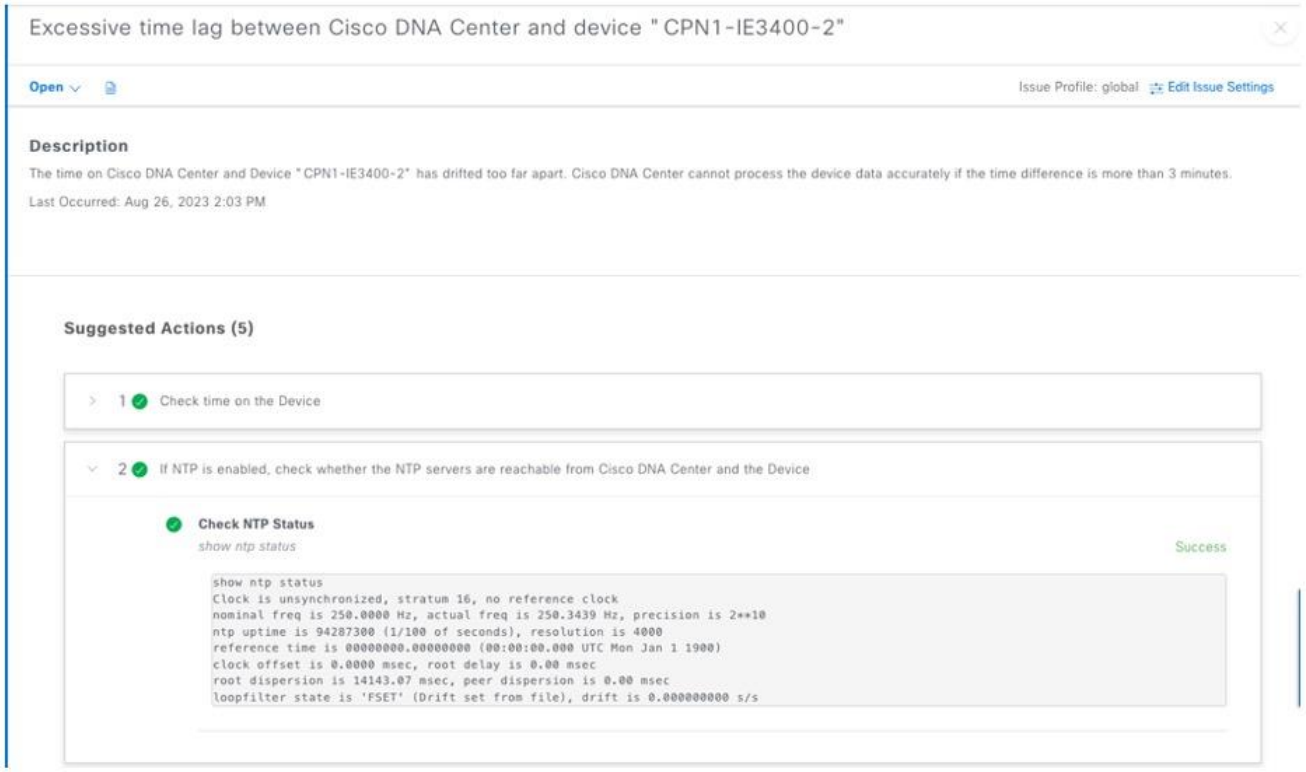


さらに、Catalyst Center Assurance 機能により、トラブルシューティングのためのシステムガイド付きアプローチが提供されます。デバイスログ、ネットワークテレメトリ、ユーザーレポートなどのさまざまなソースからの情報を関連付けて、問題の根本原因を特定します。根本原因が特定されると、アシュアランスで問題を効果的に解決するために可能なアクションがユーザーに提供されます。

次の図は、時間のずれの問題を調査するために Catalyst Center が推奨するアクションの一部を示しています。必要に応じて、Catalyst Center はデバイスに対してコマンドを実行します。このすべての情報を使用して、オペレータが修正措置を講じることができます。

© 2025 Cisco and/or its affiliates. All rights reserved.

図 19.　問題の修復



関心のあるイベントについてアラートを発するためのアシュアランスのカスタマイズ

アシュアランスによって受信されたイベントに基づいて、カスタマイズされた問題を作成できます。次の例は、Catalyst Center によって受信された産業用スイッチでの Cisco IOS XE イベントを示しています。このタイプのイベントに対して問題を作成して、[Issues] ダッシュボードに表示することができます。

図 20.　Syslog イベント

有線クライアントの問題の検出

[Client Health] ダッシュボードには、ネットワークに接続されているすべてのクライアントの集約ビューが表示されます。このダッシュボードには、各クライアントの接続状態、正常性スコア、接続されたリンクのステータスなどの情報が表示されます。オペレータは、ダッシュボードにフィルタを適用して、エリア、使用率、正常性スコアなどの基準に基づいてクライアントを並べ替えて表示することもできます。

アシュアランス内の [Event] ダッシュボードは、有線クライアントに関連するネットワークイベントをモニターするためのもう 1 つの重要なツールです。リンクダウン、リンクアップ、認証イベントなどのイベントをオペレータが簡単に追跡でき、ネットワークアクティビティの包括的なビューが提供されます。

© 2025 Cisco and/or its affiliates. All rights reserved.

特定のデバイスの詳細な分析のために、オペレータは [Client 360] ウィンドウにアクセスして焦点を絞ることができます。次の図に示すように、このページにはデバイスの正常性スコアとイベントが経時的にグラフィカルに表示されるため、オペレータはパターンと潜在的な問題を特定できます。また、クライアント 360 は関連する問題とイベントに関する情報も提供し、デバイスのパフォーマンスの包括的なビューを提供します。

図 21.　クライアント 360 の正常性タイムライン

クライアント 360 は、特定のエンドポイントのネイバースイッチ情報、リンクステータス、および使用状況に関するインサイトもオペレータに提供します。次の図は、選択した期間でのエンドポイントのリンク使用率を示しています。これは、ネットワーク キャパシティ プランニングと最適化のために役立ちます。

図 22.　クライアント 360 の接続タイムライン

コンプライアンスと設定のばらつき

コンプライアンス管理は、産業用自動化におけるネットワークのセキュリティとガバナンスの重要な側面です。これにより、産業用ネットワーク内のスイッチが、業界標準、規制要件、および内部ポリシーに準拠するようにします。

© 2025 Cisco and/or its affiliates. All rights reserved.

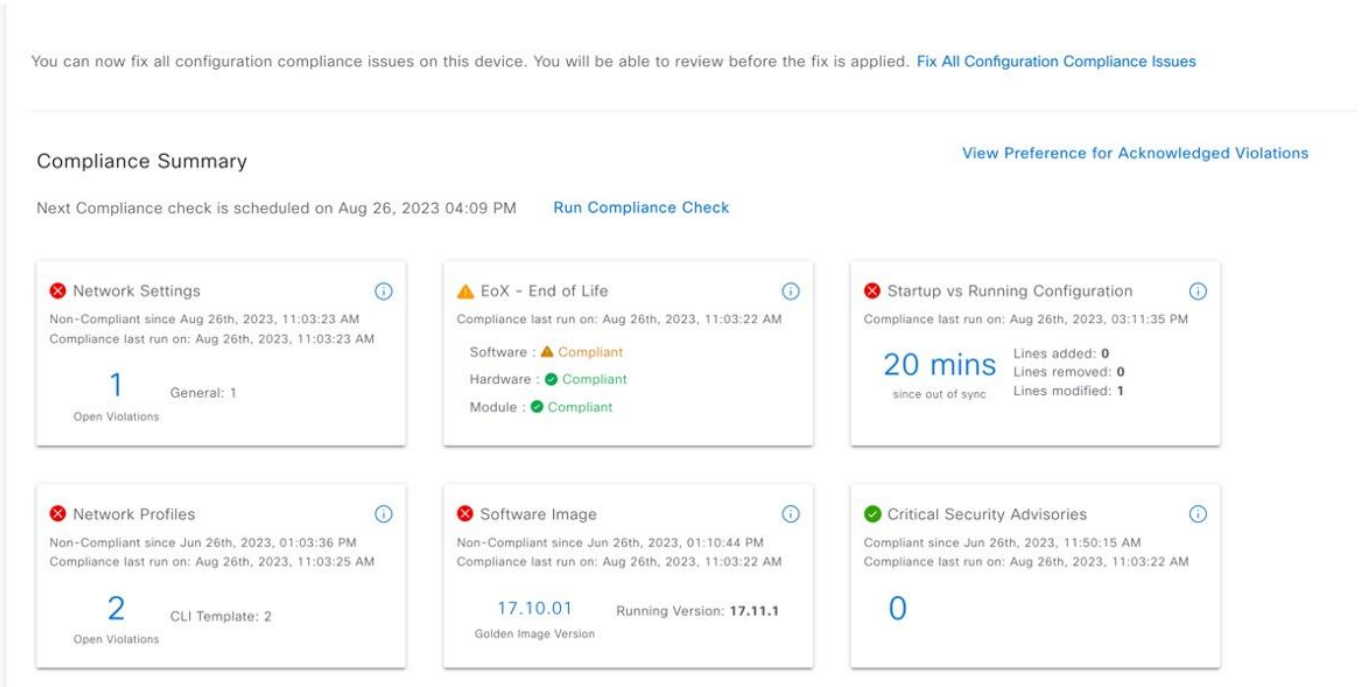
Catalyst Center のコンプライアンス機能により、産業用自動化部門のネットワーク管理者は、一元化および自動化されたアプローチを使用して、スイッチ インフラストラクチャ全体のコンプライアンスをモニター、評価、および適用することができます。この機能により、一貫性のある効率的なコンプライアンスポリシーの管理が可能になり、セキュリティ侵害のリスクが軽減され、産業用ネットワークの信頼性が確保されます。

さらに、コンプライアンス機能により、継続的なモニタリングとレポートの機能が提供されるため、管理者は産業用スイッチのコンプライアンスステータスについて常に最新の情報を入手できます。産業用ネットワークのセキュリティと完全性を確保するために、管理者は次のことを簡単に行うことができます。

- コンプライアンス違反の追跡および分析。
- 非適合のエリアの特定。
- 問題を修正するための適切なアクションの実施。

自動化されたコンプライアンスのチェックとアセスメントにより、コンプライアンス管理プロセスが合理化され、手作業の労力や人的エラーの可能性が大幅に削減されます。次の図は、産業用スイッチの [Compliance Summary] ウィンドウを示しています。

図 23.　Compliance Summary

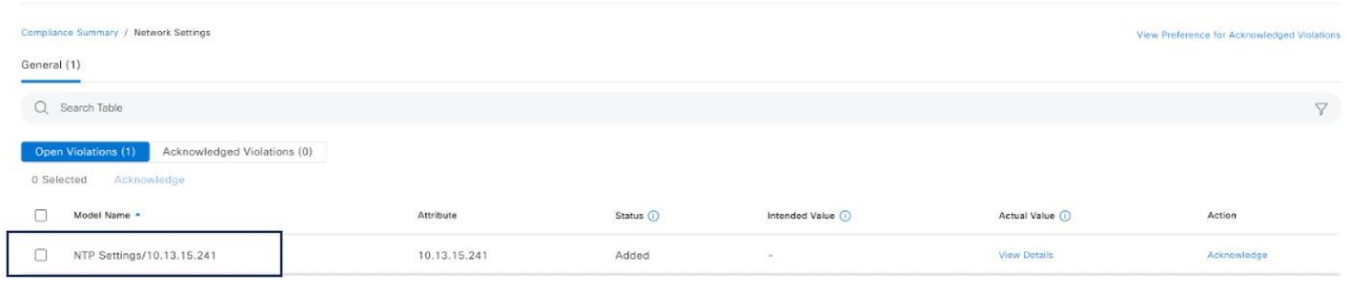


産業用スイッチの [Compliance Summary] ウィンドウでは、管理者が次の領域のコンプライアンスチェックを実行できます。

- **[Network Settings]**：Catalyst Center では、管理者がサイトの構成設定を定義し、そのゾーン内のスイッチにプッシュすることができます。例として、NTP、AAA、および DNS の設定があります。コンプライアンスチェックは、アウトオブバンドの変更またはその他の要因が原因で発生する可能性のある違反を特定してフラグを立てます。

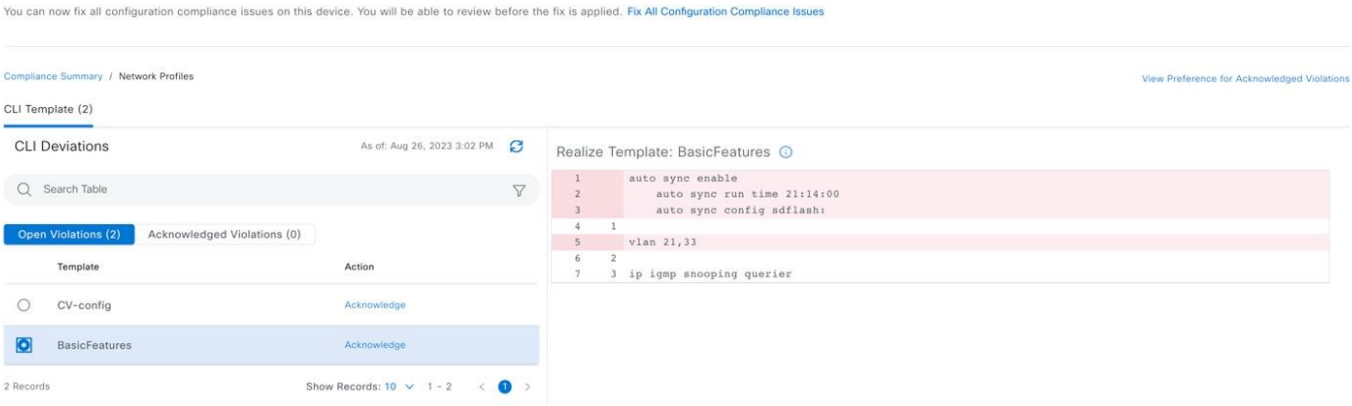
© 2025 Cisco and/or its affiliates. All rights reserved.

図 24.　コンプライアンスのネットワーク設定



- **[Network Profiles]**：管理者が、ネットワークプロファイルを使用してインテント設定を定義し、デバイスに適用することができます。産業用スイッチの場合、このセクションでは、デバイスに適用された Day n テンプレートからの逸脱にフラグが付けられます。修復を支援するために、Catalyst Center では、設定を変更してデバイスを準拠させる機能が提供されています。

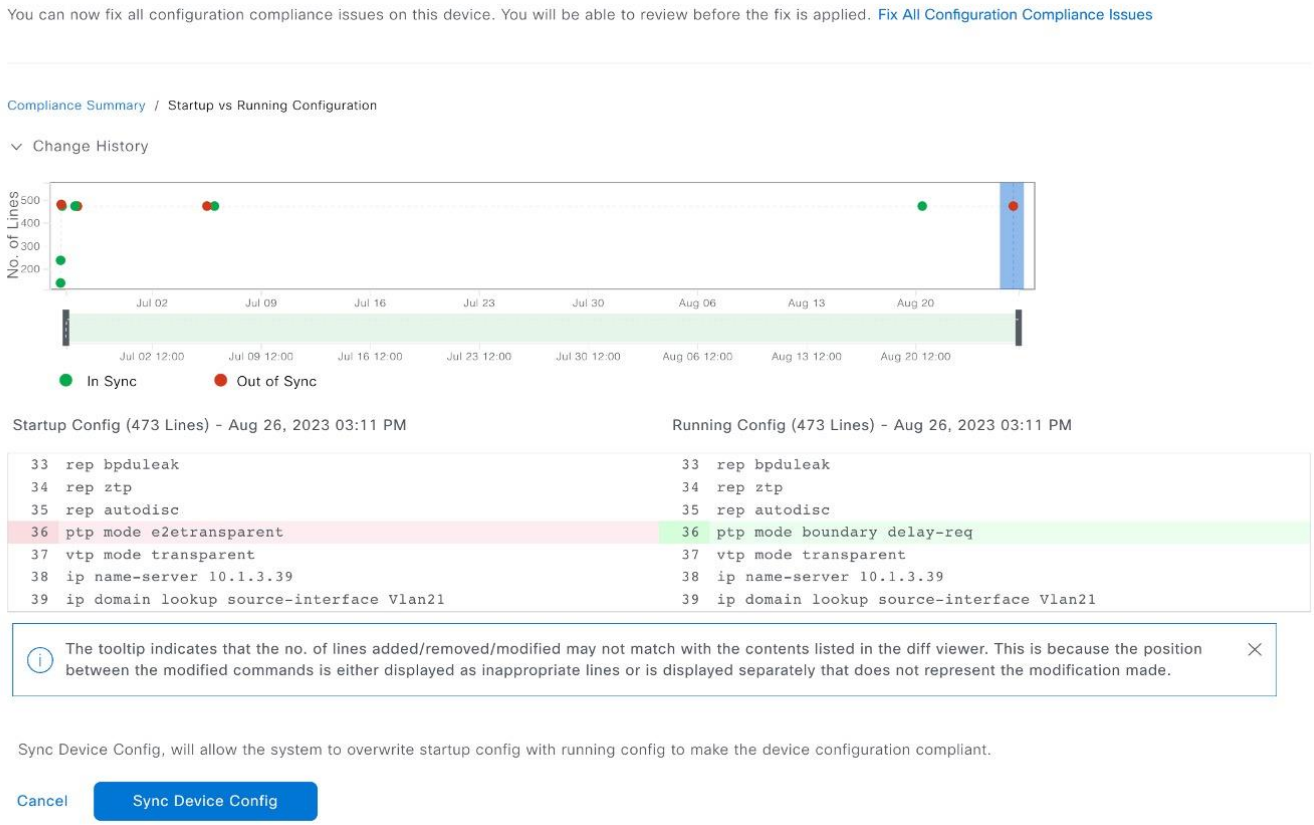
図 25.　コンプライアンスのネットワークプロファイル



- **[EoX - End of Life]**：このコンプライアンスチェックでは、管理者が、サポート終了が近づいているデバイスのハードウェアとソフトウェアモジュールのコンプライアンスステータスを確認できます。
- **[Software Image]**：このコンプライアンスチェックでは、管理者が、Catalyst Center のゴールデンタグが付けられたイメージを、デバイスで実行されているイメージと比較できます。2 つの違いが強調表示されるため、管理者は一貫性を確保できます。
- **[Startup vs. Running Configuration]**：このコンプライアンスチェックは、デバイスのスタートアップ設定と実行中の設定が同期しているかどうかを識別するために役立ちます。2 つの設定間の不一致には、注意のためのフラグが付けられます。スイッチがリロードまたはリブート後に同じ設定を保持するようにするには、変更を修正することが重要です。

© 2025 Cisco and/or its affiliates. All rights reserved.

図 26.　コンプライアンスの設定の比較



- **[Critical Security Advisories]**：このコンプライアンスチェックでは、管理者が、ネットワークデバイスに重大なセキュリティの脆弱性がないかどうかを確認できます。

監査ログ

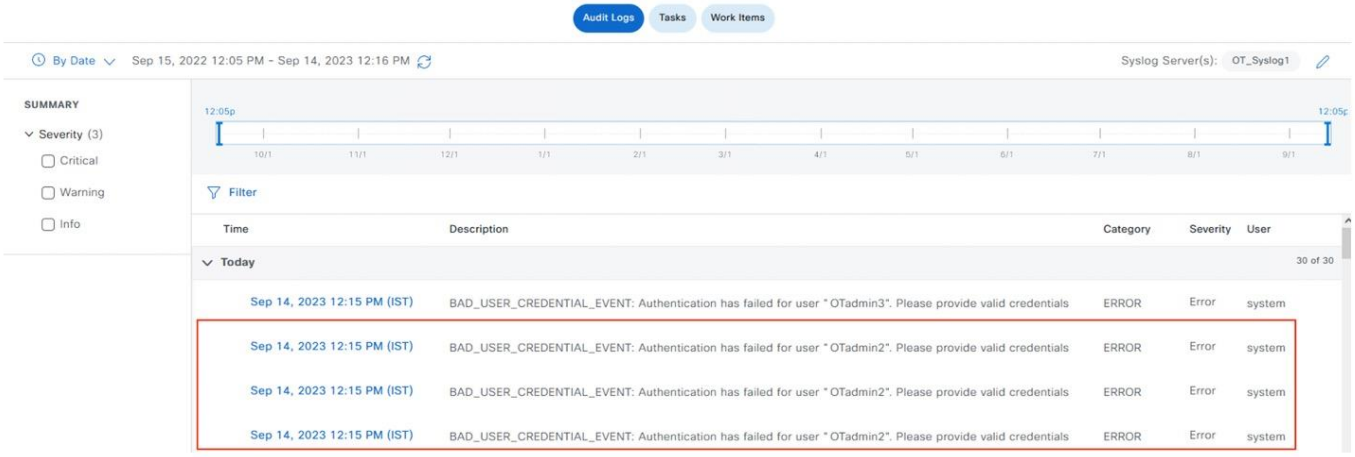
監査ログの目的は、要求された設定変更のタイミング、これらの変更の実行、および関連するエラーの検出などの、重要なアクティビティをキャプチャすることです。また、システムイベント、そのタイムスタンプ、場所、および関連するユーザーも記録されます。Catalyst Center の監査ロギングは、ログイン試行、ネットワークリソースへのアクセス、および設定変更をモニターするための便利な方法を提供します。これにより、製造ネットワーク内の不正なアクティビティや不審なアクティビティを検出して対応することができます。これは、機密データと知的財産を保護するために重要な役割を果たします。

ネットワークの問題が発生した際は、特にその問題が設定不備によって引き起こされた可能性がある場合、根本原因を特定するために監査ログが不可欠になります。問題に関与した可能性がある変更またはアクションを追跡できるため、ネットワーク関連の問題の診断と解決が容易になります。さらに、Catalyst Center の監査ログ機能により、これらのログを定期的にレビューおよび分析して、セキュリティ脅威、運用上の課題、または最適化の機会を示す可能性のある傾向、異常、またはパターンを特定することが容易になります。ユーザー補助と中央管理を強化するために、これらの監査ログを syslog サーバーに簡単にエクスポートできます。これにより、ネットワーク内の複数のシステムからの統合ビューを使用できます。

次の図は、ユーザー OTadmin2 による一連の失敗したログイン試行を監視する能力がネットワーク管理者にあるというシナリオを示しています。これらの繰り返される失敗が潜在的な侵入またはセキュリティ侵害を示している場合、Catalyst Center の監査ログからのインサイトを利用して、セキュリティ対策として、このユーザーのシステムへのアクセスをブロックするなどのプロアクティブな措置を講じる権限がネットワーク管理者にあります。

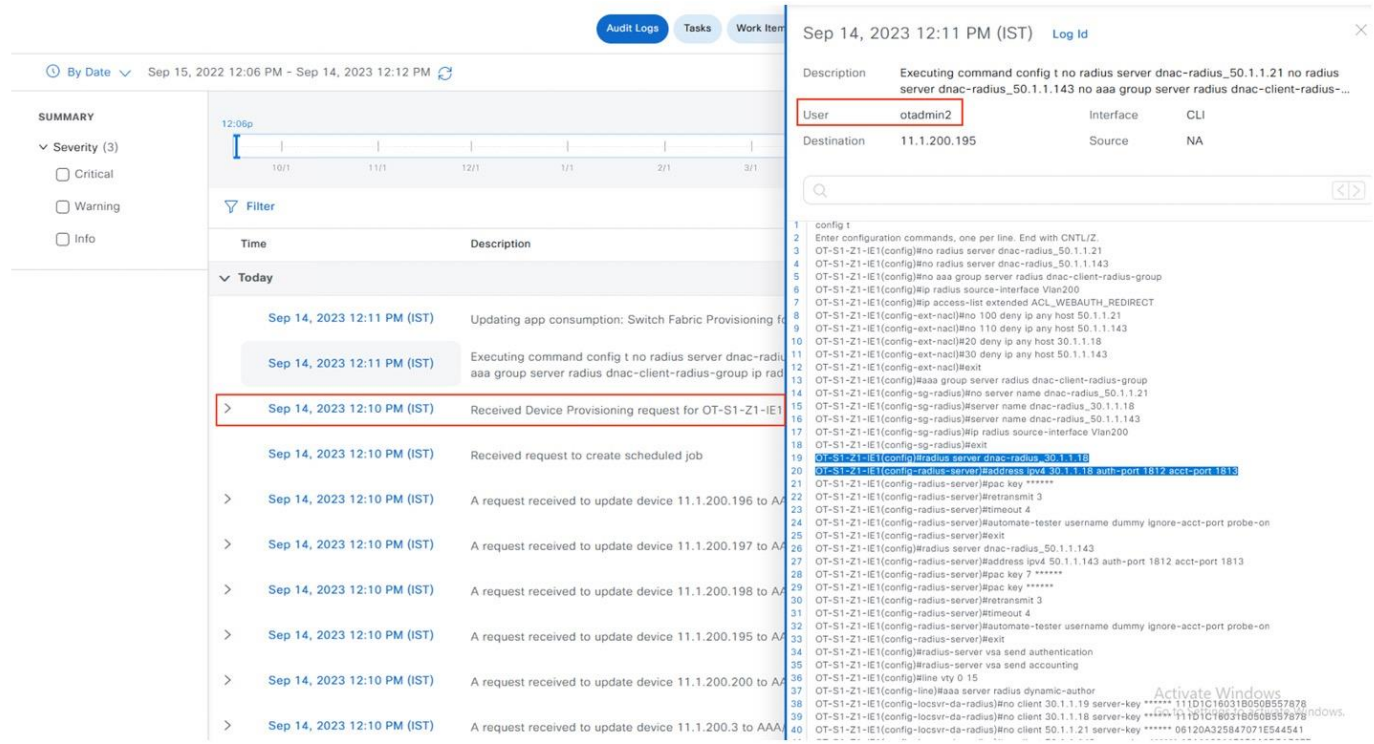
© 2025 Cisco and/or its affiliates. All rights reserved.

図 27.　監査ログ



別のシナリオでは、OT 管理者が OT-S1-Z1-IE1 という名前の特定のデバイスにリンクされている工場フロアでのエンドポイント認証の問題を特定した場合に、監査ログを効率的にフィルタリングしてこの特定のデバイス名に焦点を当てて、設定変更を追跡できます。このプロセスにより、管理者は問題の根本原因として、ユーザー otadmin2 によってプロビジョニングされた認証、許可、およびアカウンティング（AAA）サーバー設定の変更を特定できます。その後、管理者は問題に対処して修正するための修復措置を講じることができます。

図 28.　監査ログの詳細



通知

製造フロアのオペレータは絶えず移動しているため、固定されたダッシュボードにアクセスできないことがよくあります。そのため、情報を提供し続けるために通知が重要な役割を果たします。Catalyst Center の通知により、管理者とオペレータは、自動化ネットワークのパフォーマンスまたは可用性に影響を与える可能性のあるアシュアランスの問題やイベントに関するリアルタイムの最新情報を受け取ることができます。これにより、潜在的な

© 2025 Cisco and/or its affiliates. All rights reserved.

問題に迅速に対処し、ダウンタイムを最小限に抑え、中断のない運用を実現できます。Catalyst Center の通知を使用すると、産業用自動化ネットワークに可視性の向上、プロアクティブなモニタリング、および効率的なトラブルシューティングのメリットがもたらされ、最終的にはネットワーク全体の信頼性と生産性が向上します。通知用にサポートされているアシュアランスチャネルは、REST、PagerDuty、Syslog、Webex、および電子メールです。

次の図は、ネットワーク インターフェイスでの高い使用率の Webex 通知を示しています。オペレータはメッセージを受け取ったときに、問題を修正するために必要なアクションを行うことができます。

図 29.　Webex 通知

© 2025 Cisco and/or its affiliates. All rights reserved.

テクニカル リファレンス

Cisco Catalyst Center User Guide

Cisco Validated Designs for Digital Manufacturing

Cisco Catalyst Center for Industrial Automation Design Guide

Cisco Catalyst Center for Industrial Automation Implementation Guide

Networking and Security in Industrial Automation Environments Design and Implementation Guide

Cisco Catalyst Center User Guide for Non-Fabric REP Provision

REP Zero Touch Provisioning

Industrial Automation Security Design Guide 2.0

Securely Traversing IACS Data across the IDMZ Using Cisco Firepower Threat Defense

Cisco Catalyst Center User Guide for Wireless Mesh Network

Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide for Ethernet Bridging

© 2025 Cisco and/or its affiliates. All rights reserved.

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。