

Ask the Experts

【臨時開催】
ISEアップグレード + バージョン3.3機能紹介

2024 年 6月 19日



Disclaimer

This document is Cisco Confidential information provided for your internal business use in connection with the Cisco Services purchased by you or your authorized reseller on your behalf. This document contains guidance based on Cisco's recommended practices.

You remain responsible for determining whether to employ this guidance, whether it fits your network design, business needs, and whether the guidance complies with laws, including any regulatory, security, or privacy requirements applicable to your business.

免責

この文書は、お客様またはお客様の代理人である認定リセラーが購入したシスコサービスに関連して、お客様が社内業務において使用することを目的としてシスコが提供するシスコの機密情報です。この文書にはシスコが推奨するプラクティスに基づく手引きが記載されています。

お客様は、この手引きを使用するか否かやお客様のネットワーク設計および業務上のニーズにこの手引きが適合しているか否か、さらにはこの手引きが法律（お客様の業務に適用される規制上の要件、セキュリティ上の要件およびプライバシーに関する要件を含みます）に準拠しているか否かを判断する責任を引き続き負います。

本日の トピック

1

アップグレードする理由

2

アップグレードの計画と準備

3

アップグレードの実行

4

アップグレード後の作業

5

3.3の新機能について

アップグレード する理由



近年リリースされたISEバージョンの主な新機能

ISE 3.1新機能

- ・ AWS上でのISEの展開
- ・ ランダムMACアドレスの処理
- ・ OpenAPI サービス
- ・ Linuxポスチャー
- ・ ゼロタッチプロビジョニング

[3.1 リリースノート](#)

ISE 3.2新機能

- ・ クラウドサポート (Azure、Oracle)
- ・ Data Connect
- ・ システム 360
- ・ ダークモード
- ・ ポスチャ条件スクリプトのサポート

[3.2 リリースノート](#)

ISE 3.3新機能

- ・ GUIナビゲーションの改善
- ・ IPv6対応の拡大
- ・ 新しいスプリットアップグレード
- ・ エンドポイントプロファイリングのためのCisco AI-ML ルール提案
- ・ 多要素分類による拡張エンドポイントの可視化
- ・ 多要素認証のための Cisco Duo の統合

[3.3 リリースノート](#)

ISE リリースサイクル – 新しいモデル

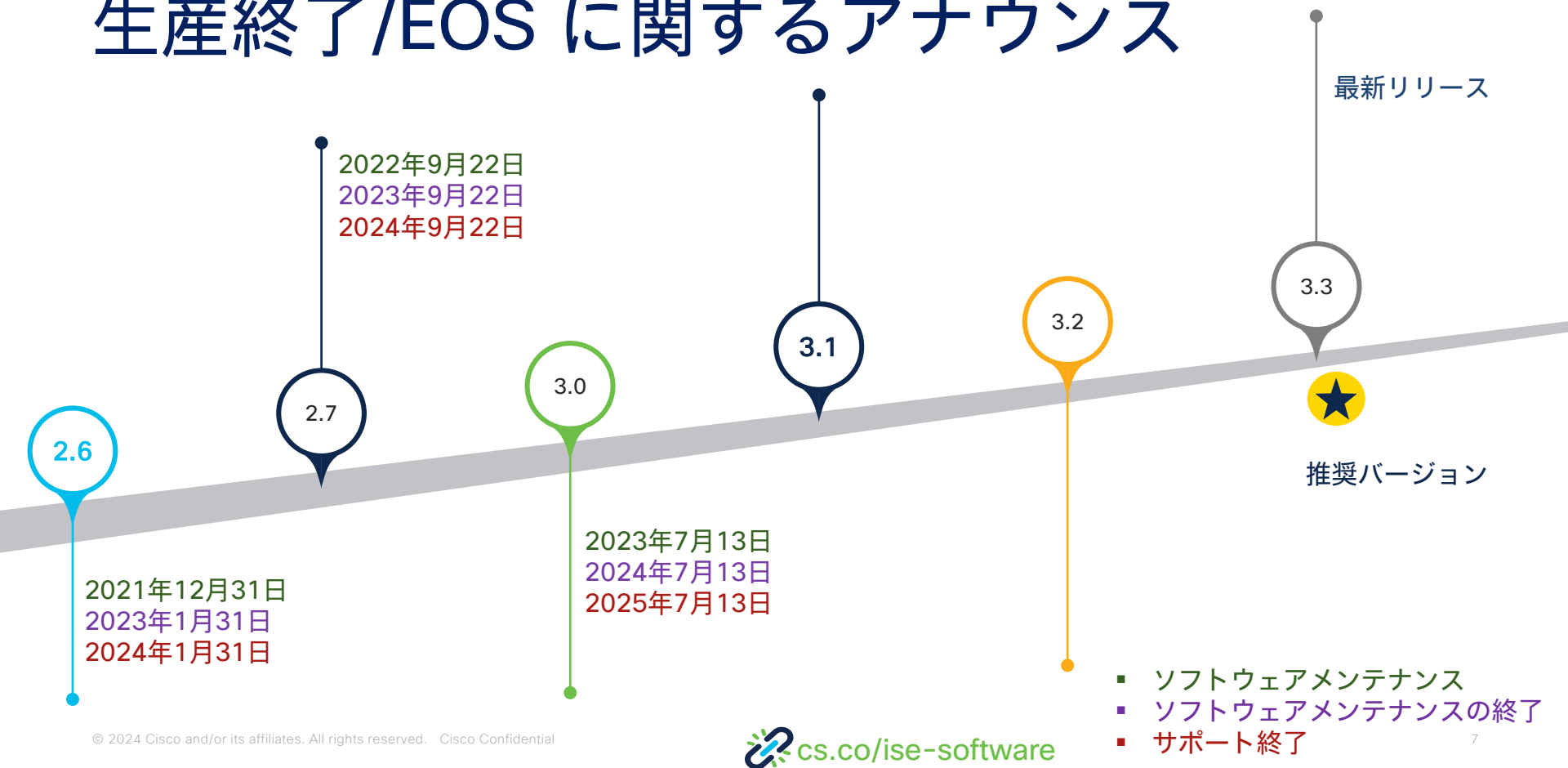
2.7 以降、ショートタームリリースとロングタームリリースは廃止
新しいリリースサイクルを適用

ISE 2.7 はさらに 6 ヶ月間の改修を実施
お客様の導入実例に基づき安定性とパフォーマンスの向上を目的とした改修
2.7 以降のすべてのバージョンに適用

2.7 以降のすべてのバージョンは、標準化されたライフサイクルに準拠
推奨ソフトウェアバージョンを常時確認することを推奨

ISE ライフサイクルの詳細については
この[リンク](#) [英語] をクリック

生産終了/EOS に関するアナウンス



アップグレード の準備



計画と準備

01 | 互換性チェックとアップグレードパス

02 | アップグレード前のアクティビティ

03 | アップグレード準備ツール

04 | メンテナンスウィンドウ

互換性チェック

サポート対象の ハードウェア



Cisco SNS-3615-K9 (小規模)
Cisco SNS-3655-K9 (中規模)
Cisco SNS-3695-K9 (大規模)
Cisco SNS-3715-K9 (小規模)
Cisco SNS-3755-K9 (中規模)
Cisco SNS-3795-K9 (大規模)
Cisco ISE-VM-K9**

サポート対象の 仮想環境



- VMware Cloud または AWS Marketplace Web サービスおよび Azure VMware における ISE
- ESXi 6.7+ (RHEL 8.4 における KVM)
- Microsoft Windows Server 2012 R2 以降の Microsoft Hyper-V

Microsoft Active Directory のサポート



Microsoft Active Directory Server:

- 2012、2012 R2
- 2016
- 2019

Cisco Catalyst Center との 互換性

Cisco Catalyst Center :

- Cisco Catalyst Center 2.3.3.7 から ISE 3.3を 対応

**仮想マシンが ISE のインストール要件を満たしていることを確認

cisco.com の ISE リリースノートで
最新の互換性ガイダンスを定期的に確認

ISE ライセンスモデル-機能

2.x モデル

Plus (コンテキスト)

- プロファイリング
- BYOD (+CA、+MDP)
- コンテキスト共有 (pxGrid アウト/イン)
- Rapid Threat Containment (適応型ネットワーク制御を使用)

Apex (コンプライアンス)

- ポスチャ
- モバイルデバイス管理コンプライアンス
- 脅威中心型NAC (TC-NAC)

Base (ネットワークオンボーディング)

- AAA と 802.1X
- ゲスト (ホットスポット、自己登録、スポンサー承認)
- TrustSec (グループベースのポリシー)
- Easy Connect (パッシブID)

3.x モデル

Premier (Advantage + ポスチャとコンプライアンス)

- ポスチャ
- MDM コンプライアンス
- TC-NAC

Advantage(Essentials+コンテキストとクラウド)

- プロファイリング
- ボイド (+CA、+MDP)
- コンテキスト共有 (pxGrid アウト/イン)
- ユーザー定義ネットワーク (クラウド)
- ロケーションサービス
- TrustSec (グループベースのポリシー)
- エンドポイント分析の可視化と適用
- Rapid Threat Containment (適応型ネットワーク制御)

Essentials (ユーザーの可視化と適用)

- AAA と 802.1X
- ゲスト (ホットスポット、自己登録、スポンサー承認)
- Easy Connect (パッシブID)

ISE 3.3 へのアップグレードパス



2 段階アップグレード

シングルステップアップグレード

アップグレード

アップグレード前の確認 (to-do リスト)

ベストプラクティス

バックアップ

- Configuration、Operational、Endpoints.csv
- ロードバランサ
- 証明書および秘密キーのエクスポート
- CLI から内部 CA 証明書をエクスポート

メモを取る

- AD クレデンシャル : トークンクレデンシャル (RSA)
- MDM クレデンシャル
- 各 PSN のプロファイラ設定

クリーン

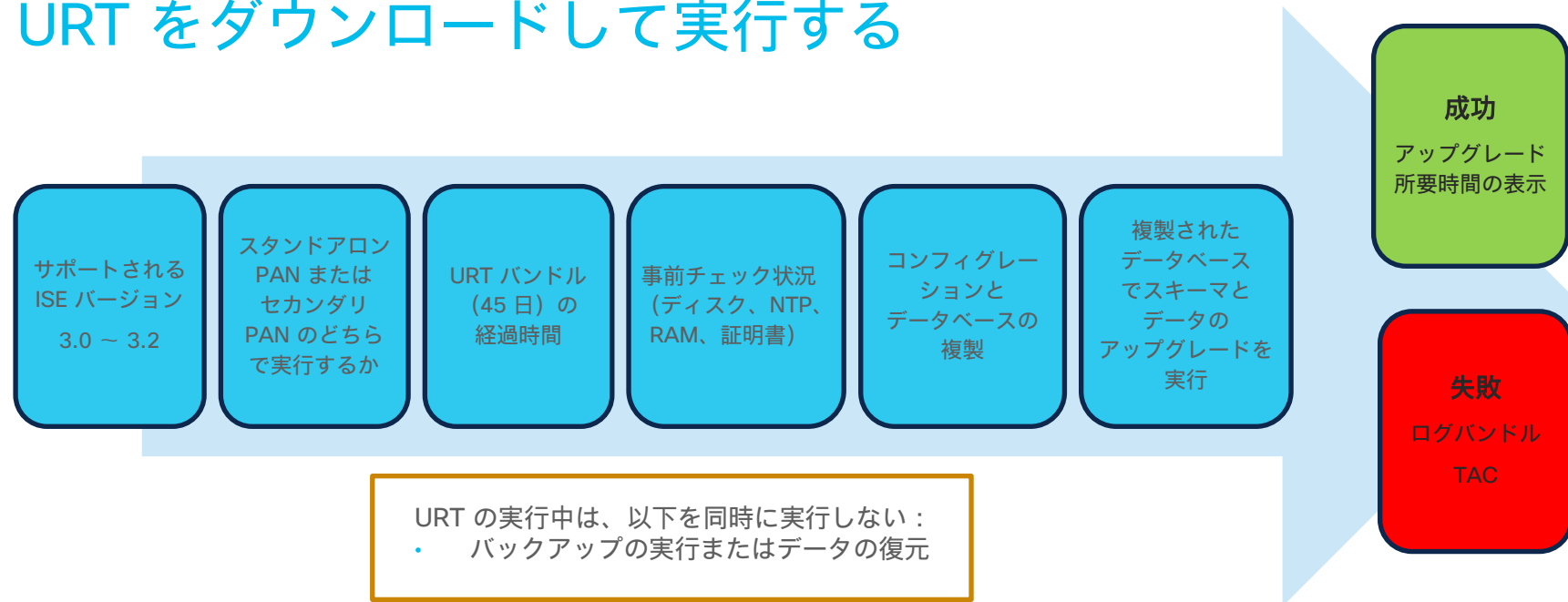
- 期限切れ証明書の削除
- 過剰な運用データ、非アクティブなエンドポイント、ゲストアカウントを消去

重要なポイント

- 自動 PAN フェールオーバーを無効にする
- スケジュールされているバックアップを無効にする
- リポジトリを設定し、最新の URT とアップグレードバンドルをダウンロードする

このリストの前に、ネットワークデバイスのソフトウェア互換性チェックを ISE 互換性マトリックを使用してすべて実行する

アップグレードレディネスツール (Upgrade Readiness Tool (URT)) URT をダウンロードして実行する



デモアップグレードにおける URT の推定所要時間

セカンダリ PAN、1 MNT、PSN - 74 分

PSN（個々またはタンデム） - 57 分

プライマリ PAN、2 MNT、PSN - 67 分

URT 推定所要時間：198 分

GUI 推定所要時間：660 分

```
Running data upgrade for node specific data on cloned database
- Successful

Time estimate for upgrade
=====
(Estimates are calculated based on size of config and mnt data only. Network latency between PAN and
other nodes is not considered in calculating estimates)
Estimated time for each node (in mins):
css-atx-1pan(PRIMARY PAP,MNT,PDP):67
css-atx-2pan(SECONDARY PAP,MNT,PDP):74
Each PSN(2 if in parallel):57

Final cleanup before exiting...

Application successfully installed
```

オンデマンドの ISE ヘルスチェック*

重大なエラーに対して展開を検証

検証対象：

- プラットフォームのサポート (Platform support)
- 展開の検証 (Deployment validation)
- DNS の名前解決が可能か (DNS resolvability)
- 信頼ストア証明書の検証 (Trust store cert validation)
- システム証明書の検証 (System cert validation)
- ディスク容量 (Disk space)
- NTP の到達可能性 (NTP reachability)
- システム負荷の平均値 (Load average)
- MDM の検証 (MDM validation)
- ライセンスの検証 (License validation)

アップグレードの前に検証結果をダウンロードし、重大なエラーがある場合は、修正が可能
これは任意の手順であり、URT の代替ではない。むしろ追加のチェックとしての機能を持つ

メンテナンスウィンドウのスケジュール

メンテナンスウィンドウの採用 アップデートとアップグレード用

通知

予定されるダウンタイムの共有

ダウンタイムの最小化

すべての PSN を一度にアップグレードしない

万が一のために予備の時間を スケジュール

アップグレードにかかる時間に影響する要因

エンドポイントの数
ユーザー数とゲストユーザー数
モニターリングノードまたはスタンドアロンノードの
ログ量
プロファイリングサービス（イネーブルの場合）

推定方法

展開のタイプ	ノードペルソナ	推定所要時間
スタンドアロン	管理、ポリシーサービス、 モニターリング	15 GB のデータごとに 240 分 + 60 分
分散型	セカンダリ管理ノード	240 分
	ポリシーサービスノード	180 分
	モニターリング	15 GB のデータごとに 240 分 + 60 分



デモ： アップグレード準備ツール

アップグレード の実行



ISE の アップグレード

01 | 展開タイプ

02 | アップグレードの種類とプロセス

03 | アップグレードオプション

ISE の展開タイプ



ポリシー管理ノード (PAN)



モニタリングおよびトラブルシューティング ノード (MnT)



ポリシー サービス ノード (PSN)



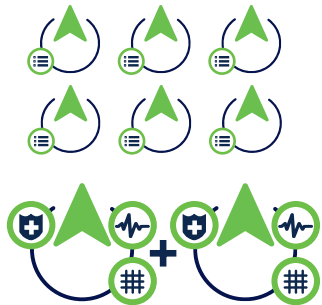
pxGrid コントローラ



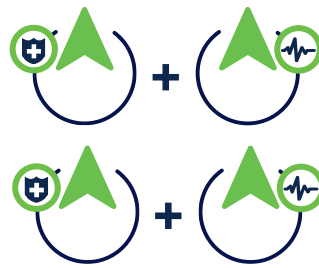
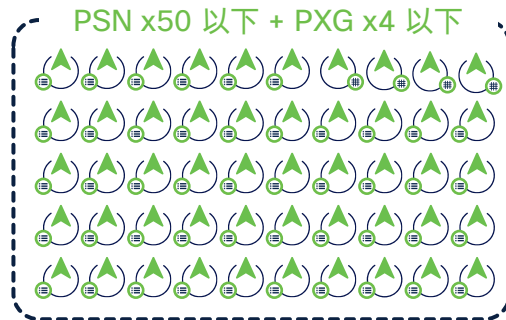
ラボと評価



小規模 HA 展開
(PAN + MNT + PSN) x2



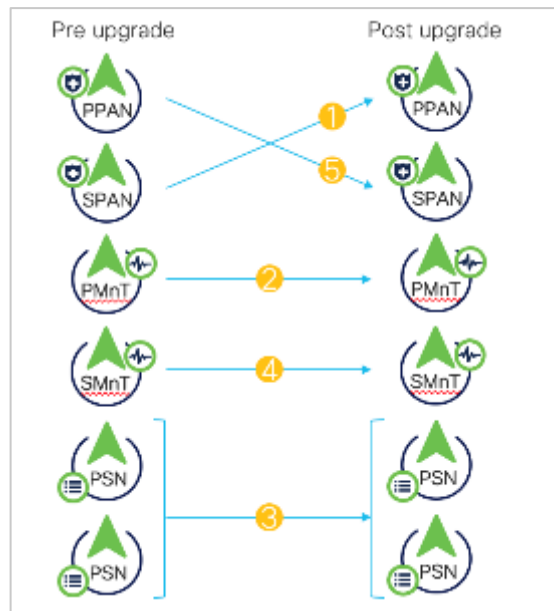
中規模分散展開
(PAN + MNT + PSN) x2、PSN x6 以下



大規模分散展開
PAN x2、MNT x2、PSN x50 以下、PXG x4 以下

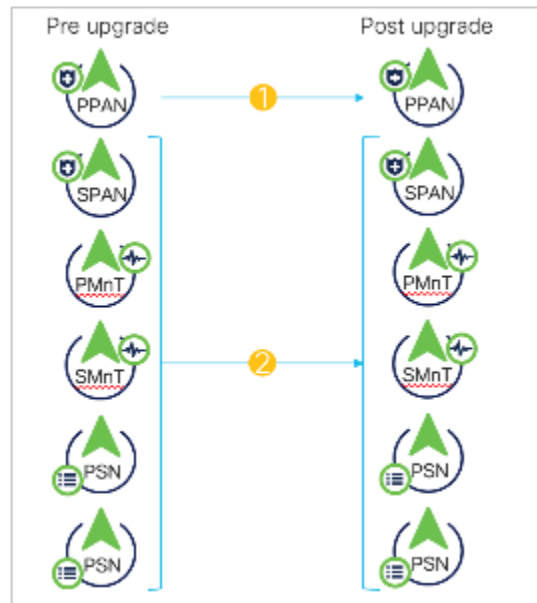
アップグレードの種類

スプリットアップグレードとフルアップグレード



スプリット

- サービスが利用可能な間に展開をアップグレードする、複数ステップのシーケンシャルプロセス
- フルアップグレードより時間がかかる

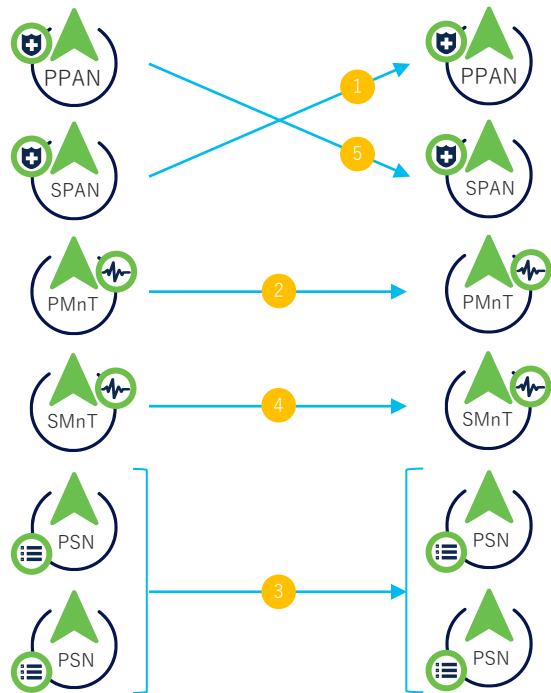


フル

- サービスの停止と並行して、すべてのノードをアップグレードする、2ステッププロセス
- スプリットアップグレードより時間がかからない

スプリットアップグレード

アップグレード前 アップグレード後



ステップ：GUIで実行する場合、以下はすべて自動で実行

1. SPAN：登録解除、設定データのアップグレード、PPAN への昇格
2. PMnT：登録解除、新規展開への登録、データのダウンロードとインポート、運用データのアップグレード
3. PSN：登録解除、新規展開への登録、データのダウンロードとインポート
4. SMnT：登録解除、新規導入への登録、データのダウンロードとインポート、運用データのアップグレード
5. PPAN：データの登録、データのダウンロードとインポート

アップグレード中のダウンタイムの最小化

アップグレードによるダウンタイムを最小化するためには、PSN全てを同時にアップグレードしない

- ✓ 拠点単位などに分割してアップグレード
- ✓ PSN Node Groupを考慮してPSNをアップグレードする。グループ内のいずれかのPSNが処理を続行できるように計画
- ✓ PSN Node Groupのアップグレード中に、RADIUSクライアントが影響を受けないように、NAD側に複数のRADIUS サーバを設定



PSN 群 - 拠点C

シーケンスC



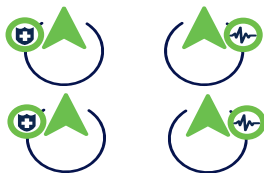
PSN 群 - 拠点B

シーケンス B



PSN 群 - 拠点A

シーケンス A



アップグレードオプション - スプリットアップグレード

CLI、GUI、バックアップ / 復元

CLI



- 最初にすべてのセカンダリノードをアップグレードしてから、PAN をアップグレードする*
- アップグレードバンドルをすべてのノードに手動でアップロードする必要がある

GUI



- ISE はアップグレードバンドルをすべてのノードに自動的にプッシュする
- シングル クリック アップグレード が可能

バックアップ / 復元



- 古いバージョンをバックアップし、新しいバージョンで復元する
- ダウンタイムを最小限に抑えることができ、仮想環境に最適

アップグレード オプション

GUI - スプリットアップグレード

ステップ 1

シングル クリック
アップグレード

ステップ 2

PSN アップグレード 順番の
カスタマイズ オプション

ステップ 3

タンデムまたはグループ
での PSN アップグレード

ステップ 4

完了後、元の PAN と
MNT を昇格

ステップ 5

最新のパッチを
インストール

アップグレードオプション

CLI - スプリットアップグレード

ステップ 1

手動プロセス

ステップ 2

各ノードを
個別にアップグレード

ステップ 3

アップグレードイメージを
各ノードにコピー (9
GB)

ステップ 4

アップグレードを準備
および実行

ステップ 5

各ノードを個別に監視

ステップ 6

最新パッチをインストール

アップグレード オプション

バックアップ、再イメージ化（新規作成）、復元

– スプリットアップグレード

ステップ 1

コンフィグレーション
データベースのバックアップ

ステップ 2

ISE 3.3（新しい仮想
マシンまたはハード
ウェア）をインストール、
または既存のノードを
再イメージ化

ステップ 3

バックアップの復元

ステップ 4

新しい展開ヘノードを追加

ステップ 5

最新のパッチを
インストール

ハイブリッドアプローチ

ハイブリッドアプローチ – スプリットアップグレード

ステップ 1

GUI または CLI から
セカンダリ PAN の
登録を解除

ステップ 2

展開内の他すべての
ノードの再イメージ化

ステップ 3

すべてのノードを手動で
PAN に追加し同期

ステップ 4

元のプライマリ PAN を
昇格

ステップ 5

アップグレードされた
単一ノードの再イメージ化

ステップ 6

再イメージ化された
ノードを展開に追加

ステップ 7

最新のパッチを
インストール

最適なオプション

	バックアップ / 復元	GUI	CLI	ハイブリッド
複雑度	中程度	容易	複雑 (手動操作を多く含む)	容易
アプライアンス および仮想マシン へのアクセス	必須	最小限 (主に URT 用)	必須	必須
並列機能	あり	PSN のみ	特定の順序であり	1 つのノードのみ アップグレードが必要
ロールバック	不可能、以前のバージョンへの 再イメージ化が必要	限定的	あり	限定的
以前の アーティファクト	なし、クリーンイメージ	維持 (以前の不具合による ディスクの問題)	維持	なし、 クリーンイメージ
時間	中程度	長時間	中程度、ノードごとのア クティブなモニタリング が必要	長時間
関連資料	スタッフ多数、 追加の仮想マシンリソース	スタッフ少数	スタッフ少数	スタッフ多数、 一時的な仮想マシン リソース
エラー	最小	ベストプラクティスを 使用しない場合に発生	CLI の操作スキルがない 場合に発生	最小

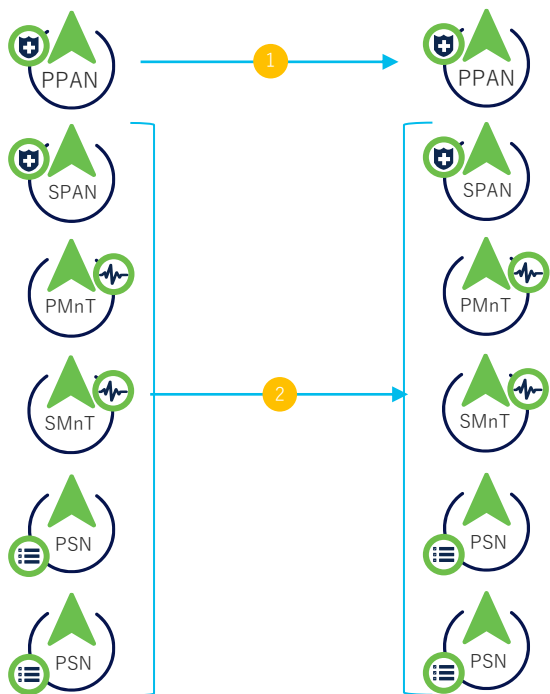


デモ： GUI - スプリット アップグレード

フルアップグレード

アップグレード前

アップグレード後



- フルアップグレードの詳細は[Upgrade ISE with Full Upgrade Method](#)を参照
- フルアップグレード自体は、下記バージョンからサポートされる。アップグレードパスを考慮の上で実行すること
 - ✓ ISE 2.6 patch 10以降
 - ✓ ISE 2.7 patch 4以降
 - ✓ ISE 3.0 patch 3以降

フルアップグレード

事前チェック

すべてのノードに対してリポジトリが
設定されていることを確認

アップグレードバンドルをダウンロード、すべての
ノードに対して DB のアップグレードを準備

PAN またはスタンドアロンで 25%、
他のノードで 1GB のメモリ空き領域を確保

PAN-HA が有効になっているかことを確認

スケジュールされているバックアップが
有効であることを確認

最近（直近 1 週間）のバックアップを確認

1. リポジトリの検証
2. バンドルのダウンロード
3. メモリのチェック
4. PAN のフェールオーバーの検証
5. スケジュールされているバックアップのチェック
6. コンフィグレーションバックアップのチェック
7. コンフィグレーションデータのアップグレード
8. プラットフォームサポート状況のチェック
9. 展開の検証
10. DNS の到達可能性
11. 信頼ストア証明書の検証
12. システム証明書の検証
13. ディスク容量のチェック
14. NTP の到達可能性と時刻源の確認
15. 負荷平均のチェック
16. ライセンスの検証
17. サービスまたはプロセスの失敗



アップグレード後の 作業



アップグレード後の作業

パッチのインストール

- アップグレード後に、最新パッチのインストールを推奨
- パッチはGUIまたはCLIからインストール可能
- GUIで実行する場合、パッチが最初にPANへインストールされ、その後残りのノードへ1台ずつ自動的にパッチがインストールされる
- CLI で実行する場合、並行でパッチをインストールするノードの選択が可能。ただし構成内の全てのISEノードへ、同一バージョンのパッチをインストールするよう注意
- Full UpgradeでISEをアップグレードする場合、オプションとしてアップグレード後にパッチの自動インストールの指定が可能
- Cisco ISE パッチは累積型。例えばパッチ 11には、パッチ 1 からパッチ 10 までの全ての修正内容が包含される
- パッチのインストールによって、ISEは再起動する

アップグレード後の作業

ベストプラクティス

ライセンスの確認

仮想マシンの設定を確認する

連携していた場合、Active DirectoryへRe-Joinする

証明書のリストア

必要に応じてISE ルート CAを再生成



Profiling、Posture、Client Provisioningの
定義ファイル更新

MnT バックアップの復元

Trustsecを使用している場合、NADで
TrustSecポリシーを更新

Client Provisioningのリソースの更新

TC-NAC を使用している場合、アダプター
の再始動

※アップグレード後作業の詳細は[Cisco Identity Services Engine リリース 3.3 アップグレードプロセス](#)のアップグレード後のタスクを参照

アップグレード後の作業

ベストプラクティス

- 基本的な健全性チェックを行うため、オンデマンドヘルスチェックを実施
- 前のアップグレードからのクリーンアップ：CLI から *application upgrade cleanup* を実行する（スプリットアップグレードのみ）
- ユースケースと認証をテストして検証
- バックアップを再構成 - 手動バックアップの実行
- 自動 PAN フェールオーバー（構成されている場合）と PAN 間のハートビートを有効化

ISE 3.3の新機能について



近年リリースされたISEバージョンの主な新機能 (再掲)

ISE 3.1新機能

- ・ AWS上でのISEの展開
- ・ ランダムMACアドレスの処理
- ・ OpenAPI サービス
- ・ Linuxポスチャー
- ・ ゼロタッチプロビジョニング

[3.1 リリースノート](#)

ISE 3.2新機能

- ・ クラウドサポート (Azure、Oracle)
- ・ Data Connect
- ・ システム 360
- ・ ダークモード
- ・ ポスチャ条件スクリプトのサポート

[3.2 リリースノート](#)

ISE 3.3新機能

- ・ GUIナビゲーションの改善
- ・ IPv6対応の拡大
- ・ 新しいスプリットアップグレード
- ・ エンドポイントプロファイリングのためのCisco AI-ML ルール提案
- ・ 多要素分類による拡張エンドポイントの可視化
- ・ 多要素認証のための Cisco Duo の統合

[3.3 リリースノート](#)

GUIナビゲーションの改善

バージョン3.0~3.2

× Cisco ISE

Q 探しているページは何ですか?

ダッシュボード

最近表示したページ

セキュリティ設定
設定
ネットワークデバイス
クライアントプロビジョ...
診断ツール
ポリシーセット

ショートカット

Ctrl + / - 展開メニュー
esc - 縮小メニュー
Make a wish

コンテキストの可視性

オペレーション

ポリシー

管理

ワークセンター

ネットワーク アクセス

概要
ID
IDグループ
外部IDソース
ネットワークリソース
ポリシー要素
ポリシーセット
トラブルシューティング
レポート
設定
ディクショナリ

ゲストアクセス

概要
ID
IDグループ

TrustSec

概要
コンポーネント
TrustSecポリシー
ポリシーセット
SXP
テスト
トラブルシューティング
レポート
設定

BYOD

概要
ID
IDグループ
ネットワークデバイス
外部IDソース

プロファイラ

概要
外部IDソース
ネットワークデバイス
エンドポイントの分類
ノード設定
フィード
手動スキャン
ポリシー要素
プロファイリングポリシー
ポリシーセット
トラブルシューティング
レポート
設定
ディクショナリ

ボスチャ

デバイス管理

概要
ID
ユーザIDグループ
外部IDソース
ネットワークリソース
ポリシー要素
デバイス管理ポリシーセット
レポート
設定

PassiveID

概要
プロバイダー
サブスクリパー
証明書
トラブルシューティング

GUIナビゲーションの改善 バージョン3.3

The screenshot displays the Cisco Identity Services Engine (ISE) dashboard. The top navigation bar includes the Cisco logo, the text 'Identity Services Engine', and the title 'ダッシュボード'. Below this, a secondary navigation bar contains tabs for 'Summary', 'Endpoints', 'Guests', 'Vulnerability', and 'Threat'. The main content area shows a summary of endpoints with three large numbers: '118' for '合計エンドポイント数' (Total Endpoints), '1' for 'アクティブ エンドポイント (Active Endpoints)', and '0' for '拒否されたエンドポイント' (Rejected Endpoints). A sidebar on the left lists various management options: 'ダッシュボード', 'コンテキストの可視性', 'オペレーション', 'ポリシー', '管理', 'ワークセンター', and 'インタラクティブヘルプ'. A dropdown menu is open under 'ダッシュボード', showing a list of sub-items including 'ネットワーク アクセス', 'ゲストアクセス', 'TrustSec', 'BYOD', '概要', 'ID', 'IDグループ', '外部IDソース', 'ネットワーク リソース', 'ポリシー要素', 'ポリシー セット', 'トラブルシューティング', 'レポート', '設定', and 'ディクショナリ'. At the bottom, a bar chart shows the distribution of endpoints by device type, with 'azure_ad' at 4.76% and 'PassiveID' at 9.09%.



ユーザーエクスペリエンス
の向上



ブックマークページ



サイドバーナビゲーション



検索オプション

エージェントレスポスチャ、ポータル、プロファイラ機能の IPv6 サポート

問題

IPv6を採用する顧客が増えて、彼らの環境をサポートするためにISEが必要とされている

ソリューション

ISE 3.3では、エージェントレスポスチャ、ポータル、プロファイラ機能の IPv6 サポートが追加された



2001:0db8:85a3:0000:0000:8a2e:0370:7334



2001:0db8:85a3:0000:0000:8a2e:0370:7334



2001:0db8:85a3:0000:0000:8a2e:0370:7334



2001:0db8:85a3:0000:0000:8a2e:0370:7334



2001:0db8:85a3:0000:0000:8a2e:0370:7334



2001:0db8:85a3:0000:0000:8a2e:0370:7334



2001:0db8:85a3:0000:0000:8a2e:0370:7334

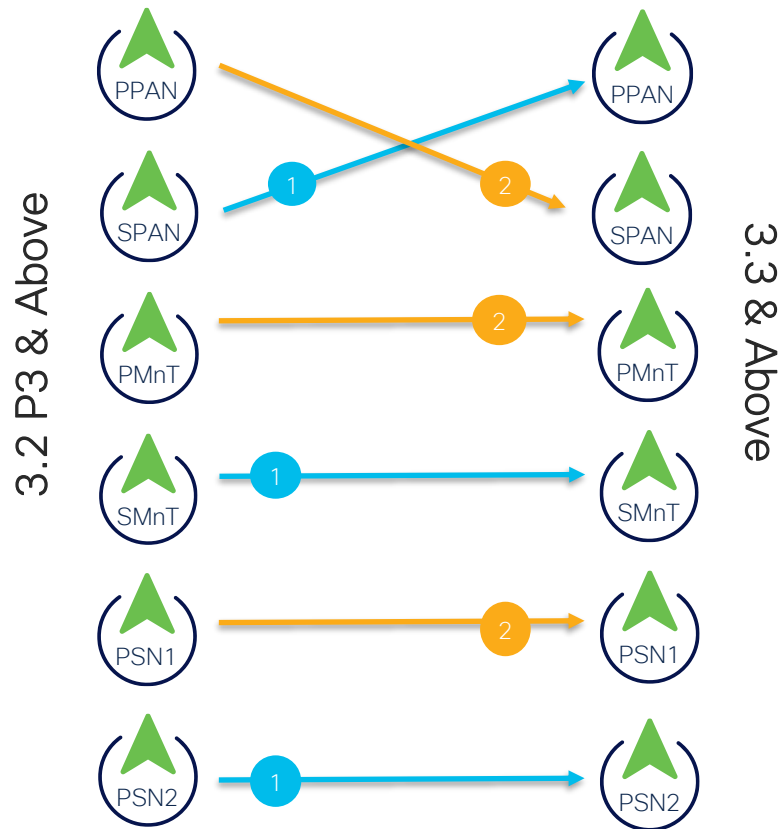


2001:0db8:85a3:0000:0000:8a2e:0370:7334



2001:0db8:85a3:0000:0000:8a2e:0370:7334

新しいスプリットアップグレード



- ✓ ノードはイテレーションに分割できる
- ✓ アップグレード前に事前チェックが行われる
- ✓ データのアップグレードは事前チェックフェーズで行われる
- ✓ SPAN は最初のイテレーションに含める必要がある
- ✓ 古いスプリットアップグレードと比較して全体的な時間が短縮された
- ✓ URTは不要
- ✓ 安定性の向上

エンドポイントプロファイリングのための Cisco AI-ML ルール提案

問題

適切なプロファイリングポリシーの作成は、特にエンドポイントの数が多く、各エンドポイントが固有の属性を持っている場合、困難で時間がかかることがある

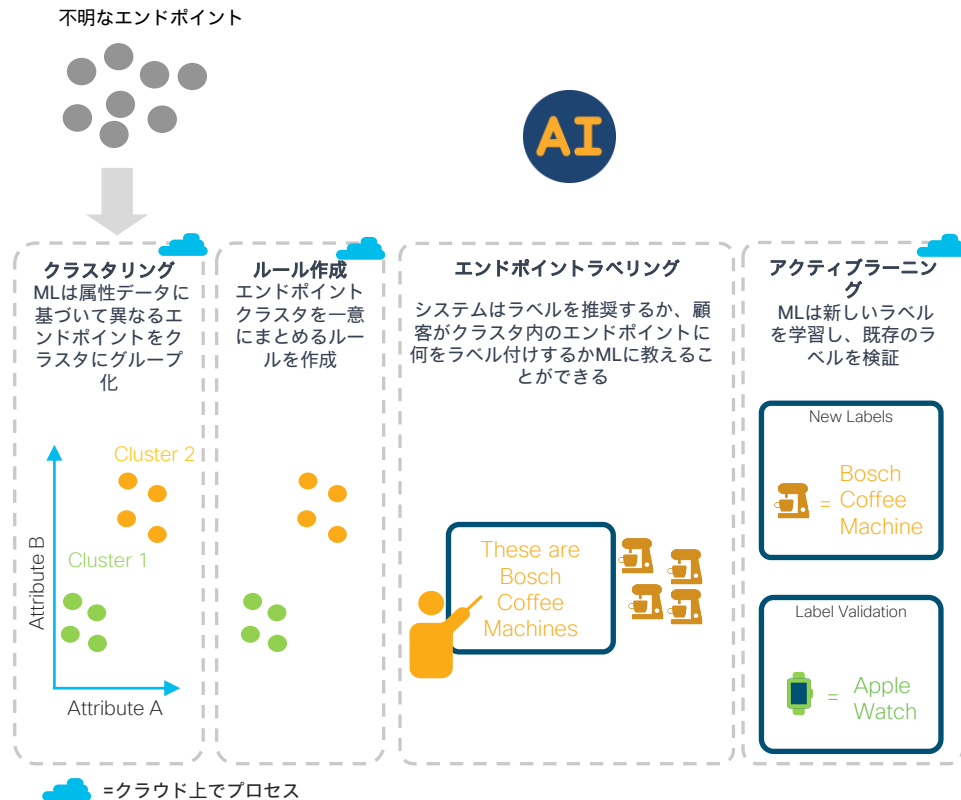
ソリューション

ISEは属性をCiscoのクラウドベースのAI/MLプロファイラーに転送する。プロファイラーは、共通の属性を共有するエンドポイントのユニークなクラスタを作成し、4つのMFCカテゴリーそれぞれにラベルを提案する

ユーザーはこれらのラベルを受け入れるか、自分でラベルを作成するか、またはクラスタ全体を拒否することができる

注意点/前提条件

- スマートライセンスが有効
- 少なくとも 1 つの ISE ノードで pxGrid サービスが有効
- エアギャップ環境はサポートされていない



エンドポイントプロファイリングのための Cisco AI-ML ルール提案 (続き)

The screenshot displays the Cisco Identity Service (Cisco ISE) configuration page for Cisco AI Analytics. The interface is divided into several sections:

- Left Navigation Panel:** Contains links for Bookmarks, ダッシュボード (Dashboard), コンテキストの可視性 (Context Visibility), オペレーション (Operations), ポリシー (Policies), 管理 (Management), ワークセンター (Work Center), and インタラクティブヘルプ (Interactive Help).
- Central Content Area:**
 - Policy Tab:** Includes links for プロファイラ (Profiler), レポート (Reports), カスタム (Custom), and ルール (Rules).
 - Policy Configuration:** Shows the configuration for the Cisco AI Analytics policy, including the NMAPスキャンサブネットの除外 (Exclude NMAP scan subnets) and the Cisco AI Analytics rule.
 - Policy Settings:** Includes checkboxes for MFC Profiling and AI Rules, and End Point Analysis Settings.
 - End Point Analysis Settings:** Contains checkboxes for AI End Point Analysis to publish endpoint attributes and to use the AI End Point Analysis endpoint profile.
- Right Panel:** Contains a warning message about enabling pxGrid Services, the Cisco AI Analytics BETA logo, and the ENDPOINT SMART GROUPING section.

The **設定** (Settings) button is highlighted in the bottom left corner of the central content area.

多要素分類による拡張エンドポイントの可視化

問題

ISE の現在のエンドポイントプロファイルは単純な文字列であるため、単純な属性でエンドポイントをフィルタリングし、一貫した認可ポリシーを設定することが難しい場合がある

ソリューション

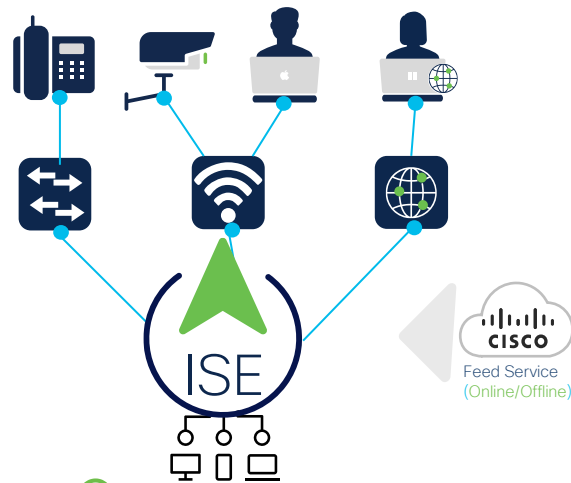
プロファイルは 4 つの要素で構成されるようになった:

- MFC-Manufacturer
- MFC-Model
- MFC-OS
- MFC-Endpoint Type

利点としては、これら 4 つの MFC 属性に基づいてポリシーを簡単に設定できることや、シスコの AI/ML プロファイリングエンジンとの互換性などがある

注意点/前提条件

現在のカスタムプロファイルとは動作しない
Advantageライセンスが必要



Manufacturer



Device Type



Model



OS



Cisco



Arlo



IP-Phone



Camera



IP Phone 7980



Pro wireless Cam



iOS



Linux



Apple



Lenovo



Laptop



Laptop



MacBook Pro



Thinkpad 540



macOS 12.0.1



Windows Enterprise

多要素分類をポリシーに反映する

Identity Services Engine

ポリシー / ポリシー セット

Bookmarks

ダッシュボード

コンテキストの可視性

オペレーション

ポリシー

管理

ワークセンター

インタラクティブヘルプ

結果

条件の属性の選択

ディクショナリ	属性	ID	情報
EndPoints	属性	ID	
EndPoints	MFCInfoEndpointType		
EndPoints	MFCInfoHardwareManufact...		
EndPoints	MFCInfoHardwareModel		
EndPoints	MFCInfoOperatingSystem		

多要素認証のための Cisco Duo の統合

問題

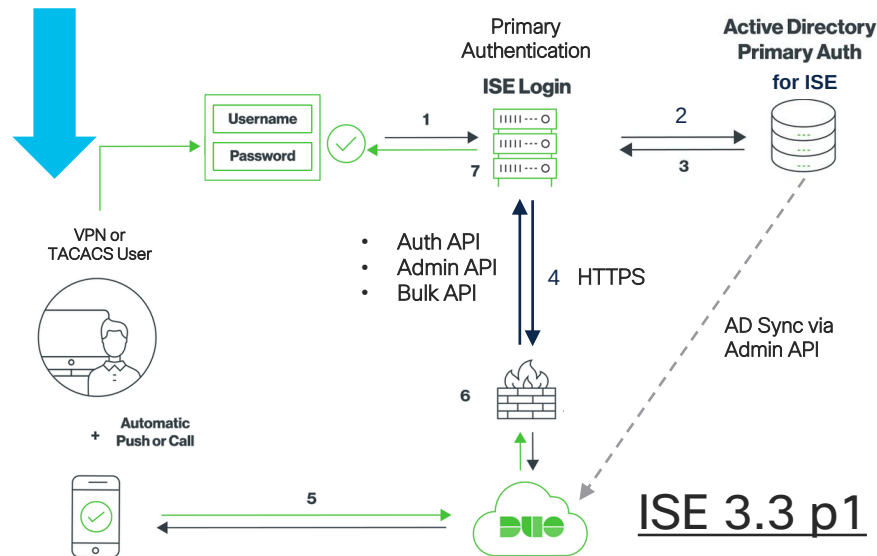
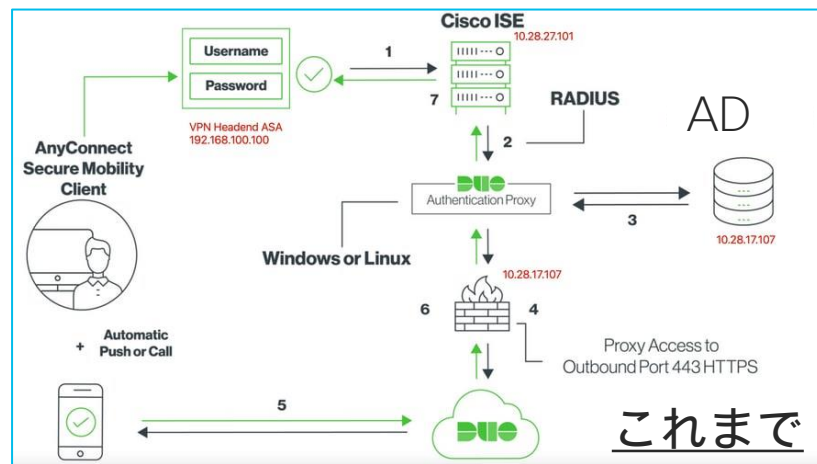
Duo Auth Proxyの設定が複雑で時間がかかる

ソリューション

- DuoをISEに直接統合することで、認証用の外部プロキシサーバーが不要になり、設定とオンボーディングの両方が簡素化される
- ISE と Duo のアイデンティティの同期が可能 (AD Sync)
- 統合のためのワークフローをISEのGUIで提供

前提条件

- 3.3 パッチ 1 以降で使用可能
- ライセンス要件: ISE Advantage、Duo Essentials



キーポイント



- ・ アップグレードパスとアップグレードの種類（スプリットまたはフル）を選択
- ・ システムアップグレードの準備
- ・ アップグレード後の作業を実行
- ・ 3.3の新機能を知る

Resources

- Cisco ISE お役立ちリンク集
- <https://community.cisco.com/t5/-/-/ta-p/4527229>
- ※本日のATXs以外のリソースリンクも確認できます。

