



Cisco ISE と Cisco Catalyst Center の再統合

Cisco ISE と Cisco Catalyst Center の再統合 2

前提条件 2

IP アドレスと命名規則 3

既存のセットアップの状態 3

目的 4

ハードウェアとソフトウェアのバージョン 5

再統合フェーズ 5

Cisco ISE と Cisco Catalyst Center の再統合

このガイドは、次の2つのユースケースを対象としています。

- Cisco ISE プラットフォームをハードウェアから、Catalyst Center と統合された仮想ネットワークに置き換える（IP アドレスの変更が含まれます）。
- 既存の Cisco ISE を現在の Catalyst Center から新しい Catalyst Center に移動させる際に既存の Cisco ISE の IP アドレスを変更する。

両方のユースケースで同じ手順を実行できます。Cisco ISE の IP アドレスを変更する場合も、同じ手順を使用できます。Catalyst Center で設定を変更することなく、既存の Cisco ISE を新しい Cisco ISE に移行可能です。

この手順は主に、Catalyst Center : ABC から Catalyst Center : XYZ に Cisco ISE を移動させるために使用されます。



-
- (注) [cisco.com](https://www.cisco.com) でこのガイドを表示している場合は、図のいずれかをクリックすると、フルサイズバージョンが表示されます。
-

前提条件

次の状態を確認してください。

- Catalyst Center と既存の Cisco ISE pxGrid が機能しており、SGT 同期が機能している。
- 既存の Cisco ISE と新しい Cisco ISE が同じソフトウェアバージョンおよびパッチ上に存在する。
- 移行時にライセンスの問題が発生した場合、問題を軽減するためにスマート登録ポータルにアクセスできる。
- 新しい Cisco ISE VM クラスターを解除し、各 Cisco ISE をスタンドアロンノードにする。
- 移行時に問題が発生した場合、問題を回避するために新しい Cisco ISE アプリケーションを工場出荷時のデフォルトにリセットする。
- 新しい Cisco ISE に、DNS サーバーに登録された A レコードと PTR レコードがある。
- 既存の Cisco ISE をバックアップする。
- Cisco ISE の技術的問題やライセンスの問題が発生した場合、問題を軽減するためにプロアクティブ TAC ケースを開く。
- 既存の Cisco ISE ノードと新しい Cisco ISE ノードのライセンスが同じである必要がある。

IP アドレスと命名規則

次の表に、移行に関連する IP アドレスおよび命名規則の例を示します。



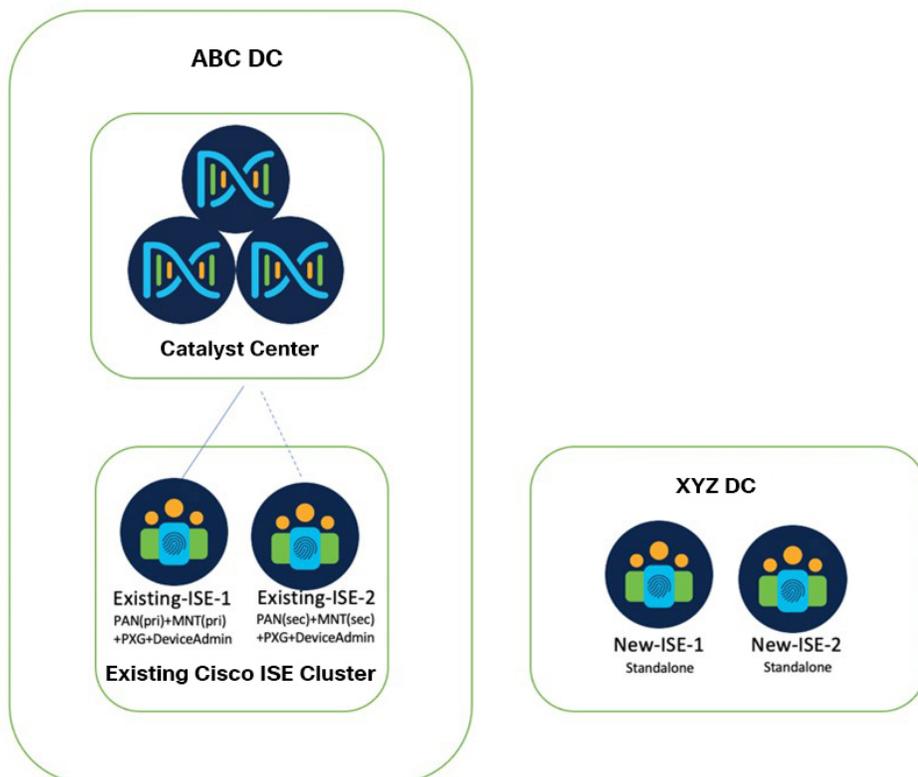
(注) Catalyst Center : XYZ と Catalyst Center : ABC の間のラウンドトリップ時間は、ピーク時で約 20 ～ 30 ミリ秒です。

テクノロジー	名前	IP アドレス	ロケーション
既存の Cisco ISE (3955 ハードウェア) : プライマリ (PAN + MNT + PSN + デバイス管理者 + PXG)	Existing-ISE-1	10.0.0.1	ABC
既存の Cisco ISE (3955 ハードウェア) : セカンダリ (SAN + MNT + PSN + デバイス管理者 + PXG)	Existing-ISE-2	10.0.0.2	ABC
新しい Cisco ISE (3615 VM) : プライマリ (SAN + MNT) : 600 GB	New-ISE-1	10.0.0.3	XYZ
新しい Cisco ISE (3615 VM) : プライマリ (SAN + MNT) : 600 GB	New-ISE-2	10.0.0.4	XYZ
新しい Cisco ISE (3615 VM) : PXG : 300 GB	New-ISE-3	10.0.0.5	XYZ
新しい Cisco ISE (3615 VM) : PXG : 300 GB	New-ISE-4	10.0.0.6	XYZ
新しい Cisco ISE (3615 VM) : PSN : 300 GB	New-ISE-5	10.0.0.7	XYZ
新しい Cisco ISE (3615 VM) : PSN : 300 GB	New-ISE-6	10.0.0.8	XYZ
Catalyst Center-1	HQ-SDA-Catalyst-1	10.255.255.250	ABC
Catalyst Center-2	HQ-SDA-Catalyst-2	10.255.255.251	ABC
Catalyst Center-3 ¹	HQ-SDA-Catalyst-3	10.255.255.252	ABC
Catalyst Center VIP	HQ-SDA-Catalyst	10.255.255.253	ABC

¹ この例は、3 ノード Catalyst Center クラスタを示しています。この手順は、Catalyst Center クラスタが、スタンドアロンクラスタ、2 ノードクラスタ、または 3 ノードクラスタのいずれであるかに関係ありません。

既存のセットアップの状態

次の図は、既存のセットアップの例を示しています。



- *Existing-ISE-1* と *Existing-ISE-2* は、デバイス管理を担当するプライマリとして1つのクラスタ内に存在します。
- Catalyst Center は、*Existing-ISE-1*（プライマリ PAN として）および *Existing-ISE-2*（セカンダリ PAN として）と統合され、次の検出が学習されます。
 - プライマリ PAN、PXG、TACACS としての *Existing-ISE-1*。
 - セカンダリ PAN、PXG、TACACS としての *Existing-ISE-2*。
- *Existing-ISE-1* と *Existing-ISE-2* は、TACACS および RADIUS（デバイス管理）用の非 SDA ネットワークデバイスを管理します。
- *New-ISE*（VM）は、工場出荷時のデフォルトにリセットされたスタンドアロンとして更新される別の新しいクラスタ内に存在します。新しいクラスタは、dot1x/MAB（RADIUS）を使用したエンドポイントネットワークアクセスコントロールを担当します。

目的

再統合の目的は、次のとおりです。

- Catalyst Center が、IP アドレスを変更することなく、既存の Cisco ISE から新しい Cisco ISE に透過的に統合されます。

- 新しいCisco ISE VMが、既存のCisco ISE クラスタに追加されます。PAN/MNT、pxGrid、およびPSN ペルソナは、新しいノードに次のように配布されます。

- *New-ISE-1* (PAN + MNT) 、プライマリとして
- *New-ISE-2* (PAN + MNT) 、セカンダリとして
- *New-ISE-3* (PXG1)
- *New-ISE-4* (PXG2)
- *New-ISE-5* (RADIUS PSN 1)
- *New-ISE-6* (RADIUS PSN 2)
- *Existing-ISE-1* (TACACS PSN 1)
- *Existing-ISE-2* (TACACS PSN 2)



(注) Cisco ISE の移行中に、SDA および非 SDA コンポーネントの TACACS 機能にリスクが生じる可能性があります。

ハードウェアとソフトウェアのバージョン

次の表に、既存のセットアップで使用されているハードウェアとソフトウェアのバージョンを示します。

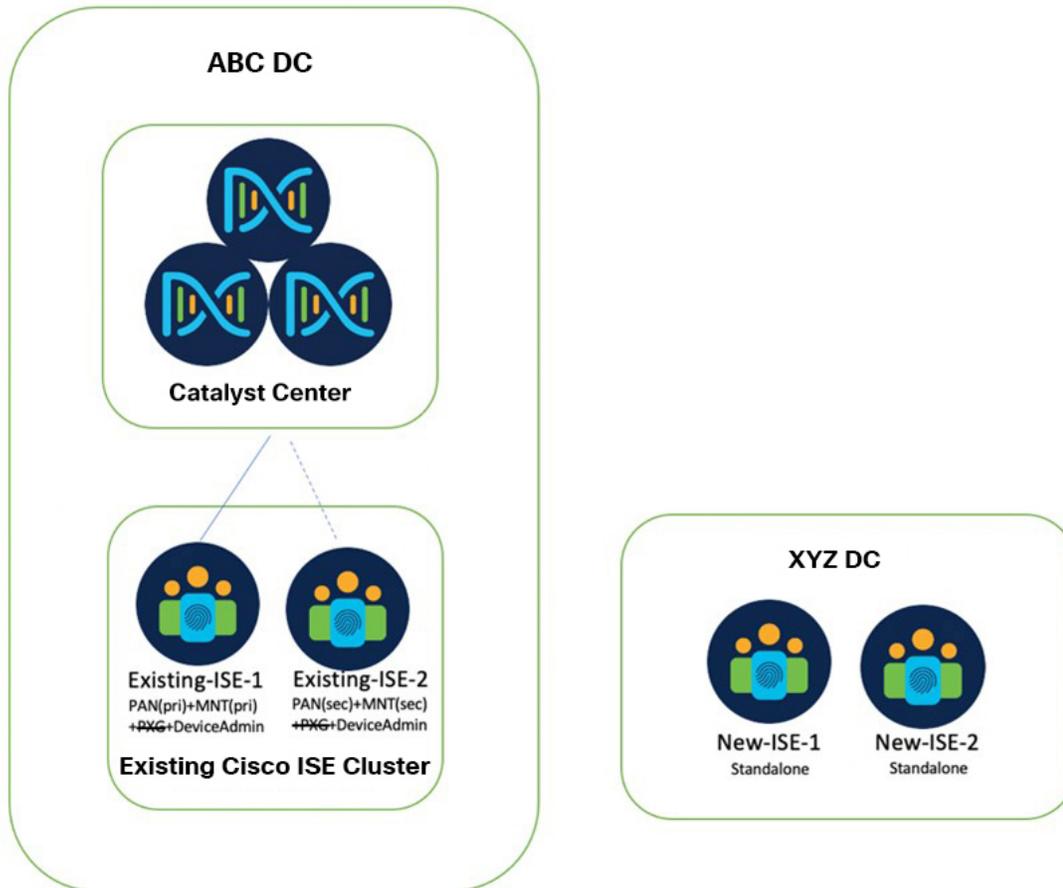
テクノロジー	ハードウェア	Version
既存の Cisco ISE ノード	3955 ハードウェア	2.7 パッチ 3
新しい Cisco ISE ノード	3615 と同等の VM	2.7 パッチ 3
Catalyst Center ノード	DN1-HW-APL	1.3.3.9

再統合フェーズ

再統合は複数のフェーズに分かれます。各フェーズについて、以下のセクションで説明します。

1. 分散 Cisco ISE VM ノードを既存のクラスタに追加します。
2. PAN+MNT ペルソナを新しい Cisco ISE ノードに移動させます。
3. 新しい AAA 設定でスイッチをプロビジョニングします。
4. グローバル認証テンプレートを変更します。

既存のクラスタに分散 Cisco ISE VM ノードを追加する



手順

ステップ 1 *Existing-ISE-1* にログインし、[System] > [Deployment] を選択します。[Existing-ISE-2] から PXG2 ロールの選択を解除します。

ステップ 2 *New-ISE* ノードを次のように登録します。

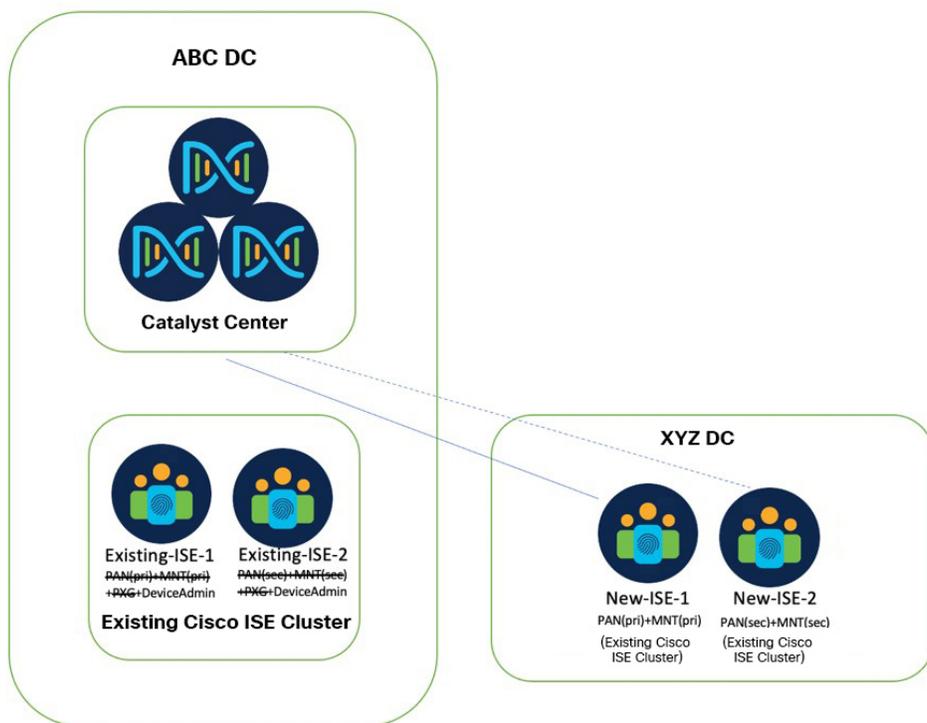
- New-ISE-4* (PXG2) を登録します。
- New-ISE-5* (RADIUS PSN 1) を登録します。
- New-ISE-6* (RADIUS PSN 2) を登録します。
- [Existing-ISE-1] から PXG1 ロールの選択を解除します。
- New-ISE-3* (PXG1) を登録します。
- すべてのノードが同期され、Cisco ISE で緑色のステータスとしてマークされていることを確認します。

この段階では、*Existing-ISE-1* と *Existing-ISE-2* はまだ PAN+MNT+TACACS-PSN として機能しています。

ステップ3 Catalyst Center にログインし、変更を確認します。

ステップ4 Catalyst Center および Cisco ISE pxGrid が機能していることと、SGT/SGT-MATRIX レプリケーションが正しく機能していることを確認します。

PAN+MNT ペルソナを新しい Cisco ISE ノードに移動させる



次の手順に含まれる各ステップの後に、ノードの変更が同期され、Cisco ISE で緑色のステータスとしてマークされていることを確認してください。

手順

- ステップ1 *Existing-ISE-1* にログインし、[System] > [Deployment] を選択します。*Existing-ISE-2* で、セカンダリ PAN ロールとセカンダリ MNT ロールを削除し、デバイス管理者ロールのみを残します。
- ステップ2 Catalyst Center にログインし、[System] > [System 360] を選択します。Catalyst Center が PAN/MNT の変更を学習することを確認します。
- ステップ3 *Existing-ISE-1* にログインし、[System] > [Deployment] を選択します。*New-ISE-1* をセカンダリ PAN および MNT として登録します。
- ステップ4 Catalyst Center にログインし、[System] > [System 360] を選択します。Catalyst Center が *New-ISE-1* の登録をセカンダリ PAN として学習することを確認します。
- ステップ5 スマート ライセンシング ポータル (Cisco SSM) にアクセスして、*Existing-ISE-2* の登録を解除し、*New-ISE-1* を登録します。

- ステップ 6 Cisco ISE で、**[System]** > **[Licensing]** を選択し、スマートライセンス登録を更新します。再登録後にライセンス警告メッセージが表示されないことを確認します。
- ステップ 7 *Existing-ISE-1* にログインし、**[System]** > **[Deployment]** を選択します。*New-ISE-1* をプライマリにし、*Existing-ISE-1* をセカンダリにします。
- ステップ 8 *New-ISE-1* にログインし、**[System]** > **[Deployment]** を選択します。*Existing-ISE-1* で、セカンダリ PAN ロールとセカンダリ MNT ロールを削除し、デバイス管理者ロールのみを残します。
- ステップ 9 Catalyst Center が変更を再度学習することを確認します。
- ステップ 10 *New-ISE-1* にログインし、**[System]** > **[Deployment]** を選択します。*New-ISE-2* をセカンダリ PAN および MNT として登録します。
- ステップ 11 スマートライセンスポータル (Cisco SSM) にアクセスして、*Existing-ISE-1* の登録を解除し、*New-ISE-2* を登録します。
- ステップ 12 Cisco ISE で、**[System]** > **[Licensing]** を選択し、スマートライセンス登録を更新します。再登録後にライセンス警告メッセージが表示されないことを確認します。
- ステップ 13 Catalyst Center に PAN のプライマリノードとセカンダリノードが正しく表示されていることを確認します。
-

新しい AAA 設定でスイッチをプロビジョニングする

手順

- ステップ 1 Catalyst Center で、ネットワーク設定を更新します。**[Network]** > **[TACACS]** を選択し、既存の Cisco ISE ノード (10.204.0.20 および 10.204.0.21) を指すように設定します。**[Client]** > **[RADIUS]** を選択し、新しい Cisco ISE PSN (10.204.2.124 および 10.204.2.125) を指すように設定します。
- ステップ 2 サンプルスイッチをプロビジョニングします。TACACS および RADIUS がスイッチの設定に正しく反映されていることを確認します。
- ステップ 3 他のスイッチをバッチでプロビジョニングします。
-

グローバル認証テンプレートを変更する

手順

- ステップ 1 Catalyst Center GUI で、メニューアイコンをクリックして、**[Provision]** > **[Fabric]** を選択し、ファブリックを選択します。
- ステップ 2 **[Host Onboarding]** > **[Authentication Template]** を選択し、**[No Authentication]** から **[Closed Authentication]** に変更します。
この手順では、**[No Authentication]** がすでに静的に設定されているポートの設定は変更されません。
- ステップ 3 **[Save]** をクリックします。



Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2023 Cisco Systems, Inc. All rights reserved.

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

©2008 Cisco Systems, Inc. All rights reserved.

Cisco, Cisco Systems, およびCisco Systemsロゴは、Cisco Systems, Inc.またはその関連会社の米国およびその他の一定の国における登録商標または商標です。

本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。

「パートナー」または「partner」という用語の使用はCiscoと他社との間のパートナーシップ関係を意味するものではありません。(0809R)

この資料の記載内容は2008年10月現在のものです。

この資料に記載された仕様は予告なく変更する場合があります。



シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先：シスコ コンタクトセンター

0120-092-255（フリーコール、携帯・PHS含む）

電話受付時間：平日 10:00～12:00、13:00～17:00

<http://www.cisco.com/jp/go/contactcenter/>

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。