



Cisco Identity Services Engine リリース 2.6 アップグレードガイド

初版：2023年2月21日

最終更新：2023年2月21日

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/>

【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。

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

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)

© 2019 Cisco Systems, Inc. All rights reserved.



目次

第 1 章

Cisco ISE アップグレードの概要 1

アップグレードパス 2

仮想マシンでサポートされるオペレーティングシステム 2

ライセンスの変更 3

その他の参考資料 5

通信、サービス、およびその他の情報 5

Cisco バグ検索ツール 6

マニュアルに関するフィードバック 6

第 2 章

アップグレードの準備 7

アップグレード中の時間を最小限に抑えて効率を最大化するためのガイドライン 8

アップグレードの失敗を防ぐためのデータの検証 10

アップグレード準備ツールのダウンロードと実行 12

リポジトリの作成および URT バンドルのコピー 12

アップグレード準備ツールの実行 13

同じ名前の事前定義済み承認複合条件が存在する場合は、承認単純条件の名前を変更する
13

VMware 仮想マシンのゲスト オペレーティング システムと設定の変更 14

スポンサーグループ名から非 ASCII 文字を削除する 14

通信用に開く必要があるファイアウォールポート 14

プライマリ管理ノードからの Cisco ISE 設定および運用データのバックアップ 15

プライマリ管理ノードからのシステムログのバックアップ 16

CA 証明書チェーン 16

証明書の有効性の確認 16

証明書を削除する	17
証明書および秘密キーのエクスポート	17
	18
アップグレード前の PAN 自動フェールオーバーとスケジュールバックアップの無効化	18
NTP サーバーの設定と可用性の確認	19
仮想マシンのアップグレード	19
プロファイラ設定の記録	19
Active Directory および内部管理者アカウントの資格情報の取得	20
アップグレード前の MDM ベンダーのアクティベート	20
リポジトリの作成およびアップグレードバンドルのコピー	20
利用可能なディスクサイズの確認	21
ロードバランサ構成の確認	21
ログの保持と MnT ハードディスクのサイズ変更	22

第 3 章

ノードのアップグレードの順序	23
アップグレード方法の選択	26
バックアップと復元方法を使用した Cisco ISE 展開のアップグレード (推奨)	30
バックアップと復元によるアップグレード方法の概要	30
バックアップと復元によるアップグレードプロセス	32
セカンダリ PAN およびセカンダリ MnT ノードを、Cisco ISE リリース 2.1、2.2、2.3 または 2.4 にアップグレードします。	32
セカンダリ PAN および MnT ノードの Cisco ISE リリース 2.6 へのアップグレード	32
ポリシーサービスノードの Cisco ISE リリース 2.6 への参加	33
プライマリ PAN および MnT の Cisco ISE リリース 2.6 へのアップグレード	33
GUI からの Cisco ISE 展開のアップグレード	34
GUI からの Cisco ISE 展開のアップグレード	34
リリース 2.1、2.2、2.3、または 2.4 からリリース 2.6 へのアップグレード	34
CLI からの Cisco ISE 展開のアップグレード	36
	36
スタンドアロンノードのアップグレード	36
2 ノード展開のアップグレード	37

	分散展開のアップグレード	39
	アップグレードプロセスの確認	41
	以前のバージョンへのロールバック	42
<hr/>		
第 4 章	Cisco ISE ソフトウェアパッチ	43
	ソフトウェアパッチインストールのガイドライン	44
	ソフトウェアパッチのインストール	44
	ソフトウェアパッチのロールバック	45
	ソフトウェアパッチロールバックのガイドライン	46
	パッチのインストールおよびロールバックの変更の表示	46
<hr/>		
第 5 章	アップグレード後の設定と構成	47
	仮想マシンの設定の確認	47
	ポートが開いていることの確認	48
	ブラウザのセットアップ	48
	Active Directory の再結合	48
	逆引き DNS ルックアップ	50
	証明書の復元	50
	ルート CA チェーンの再生成	51
	脅威中心型 NAC	52
	SMNP 送信元ポリシーサービスノード設定	52
	プロファイラ フィールド サービス	52
	クライアントプロビジョニング	52
	オンライン更新	53
	オフライン更新	53
	暗号スイート	53
	モニタリングおよびトラブルシューティング	54
	Trustsec NAD に対するポリシーの更新	54
	サブリカントプロビジョニング ウィザードの更新	54



第 1 章

Cisco ISE アップグレードの概要

このマニュアルでは、Cisco ISE アプライアンスおよび仮想マシンで Cisco Identity Services Engine (Cisco ISE) ソフトウェアをリリース 2.6 にアップグレードする方法について説明します。
(『Cisco Identity Services Engine リリース 2.6 リリースノート』の「[Cisco ISE リリース 2.6 の新機能](#)」のセクションを参照してください。)



- (注) Cisco ISE リリース 2.3 以降では、すべての既存のネットワーク アクセス ポリシーとポリシー セットを置き換える、新しい拡張された [ポリシーセット (Policy Sets)] ページが用意されています。以前のリリースからリリース 2.3 以降にアップグレードすると、すべてのネットワーク アクセス ポリシーの設定 (認証および認可の条件、ルール、ポリシー、プロファイル、および例外を含む) が Cisco ISE GUI の新しい [ポリシーセット (Policy Sets)] ウィンドウに移行されます。ポリシーモデルの詳細については、『[Cisco Identity Services Engine リリース 2.6 管理者ガイド](#)』の「新規ポリシー モデル」のセクションを参照してください。

Cisco ISE 展開環境のアップグレードは複数段階のプロセスであり、このマニュアルで指定されている順序で実行する必要があります。このマニュアルで示されている推定所要時間を使用して、最小限のダウンタイムでのアップグレードを計画してください。展開環境に含まれる複数のポリシーサービスノード (PSN) が 1 つの PSN グループに属している場合、ダウンタイムは発生しません。アップグレード対象の PSN で認証されるエンドポイントがない場合、要求はノードグループ内の別の PSN で処理されます。エンドポイントは、認証の成功後に再認証されて、ネットワークアクセス権が付与されます。



- 注意** スタンドアロン展開環境または単一の PSN のみの展開環境の場合は、その PSN がアップグレードされている間、すべての認証にダウンタイムが発生する可能性があります。



- (注) Cisco ISE リリース 3.2 以降にアップグレードすると、ルート CA の再生成がアップグレードフローで自動的に行われます。したがって、アップグレード後のルート CA の再生成は必要ありません。

さまざまなタイプの展開

- スタンドアロンノード：管理、ポリシーサービスおよびモニタリングのペルソナを担当する単一の Cisco ISE ノード
- マルチノード展開：複数の ISE ノードによる分散展開。
- アップグレードパス (2 ページ)
- 仮想マシンでサポートされるオペレーティングシステム (2 ページ)
- ライセンスの変更 (3 ページ)
- その他の参考資料 (5 ページ)
- 通信、サービス、およびその他の情報 (5 ページ)

アップグレードパス

シングルステップ アップグレード

次のリリースはすべて、リリース 2.6 に直接アップグレードできます。

- Cisco ISE、リリース 2.1
- Cisco ISE、リリース 2.2
- Cisco ISE、リリース 2.3
- Cisco ISE、リリース 2.4

アップグレードバンドルは [Cisco.com](https://www.cisco.com) からダウンロードすることができます。リリース 2.6 では、次のアップグレードバンドルを使用できます。

[ise-upgradebundle-2.x-to-2.6.0.xxx.SPA.x86_64.tar.gz](https://www.cisco.com/ise-upgradebundle-2.x-to-2.6.0.xxx.SPA.x86_64.tar.gz) : リリース 2.1、2.2、2.3 または 2.4 から 2.6 にアップグレードするには、このバンドルを使用します

2段階のアップグレード

Cisco ISE リリース 2.1 より前のバージョンを現在使用している場合は、はじめに上記のリリースのいずれかにアップグレードしてから、リリース 2.6 にアップグレードする必要があります。

仮想マシンでサポートされるオペレーティングシステム

Cisco ISE は、Red Hat Enterprise Linux (RHEL) に基づく Cisco Application Deployment Engine オペレーティングシステム (ADE-OS) で動作します。Cisco ISE リリース 2.6 では、ADE-OS は RHEL 7.5 に基づいています。

次の表に、Cisco ISE のさまざまなバージョンで使用される RHEL バージョンを示します。

表 1: RHEL リリース

Cisco ISE リリース	RHEL リリース
Cisco ISE 1.3	RHEL 6.4
Cisco ISE 1.4	RHEL 6.4
Cisco ISE 2.0	RHEL 7.0
Cisco ISE 2.1	RHEL 7.0
Cisco ISE 2.2	RHEL 7.0
Cisco ISE 2.3	RHEL 7.0
Cisco ISE 2.4	RHEL 7.3
Cisco ISE 2.6	RHEL 7.5
Cisco ISE 3.2	RHEL 8.4

VMware 仮想マシン (VM) の Cisco ISE ノードをアップグレードする場合は、アップグレード後に、RHEL のサポートされるバージョンにゲスト オペレーティング システムを変更する必要があります。これを行うには、VM の電源をオフにし、サポートされる RHEL バージョンにゲスト オペレーティング システムを変更してから VM の電源をオンにする必要があります。



- (注) [ゲスト OS RHEL 8 (Guest OS RHEL 8)] および [ファームウェア EFI (Firmware EFI)] を選択した場合は、[VM オプション (VM Options)] タブで [UEFI セキュアブートの有効化 (Enable UEFI Secure Boot)] オプションが無効になっていることを確認する必要があります。このオプションは、ゲストオペレーティングシステム RHEL 8 VM ではデフォルトで有効になっていません。Cisco ISE VM の [UEFI セキュアブートの有効化 (Enable UEFI Secure Boot)] オプションが無効であることを確認してください。

RHEL オペレーティング システム アップグレードを使用した Cisco ISE アップグレードは、通常のアップグレードプロセスよりも時間がかかる場合があります。また、Oracle データベースバージョンに変更がある場合は、オペレーティングシステムのアップグレード時に新しい Oracle パッケージがインストールされるため、アップグレードにさらに時間がかかる場合があります。

ライセンスの変更

デバイス管理ライセンス

Cisco ISE リリース 3.0 でライセンスの消費を有効にするには、Cisco Smart Software Manager (CSSM) を使用して既存のスマートライセンスか従来のライセンスを新しいライセンスタイプに変換する必要があります。

Cisco ISE 2.4 以降、デバイス管理ライセンスの数は、展開環境のデバイス管理ノード（デバイス管理サービス用に設定された PSN）の数と同じである必要があります。

現在、デバイス管理ライセンスを使用していてリリース 2.4 以降へのアップグレードを計画している場合、TACACS+ 機能はリリース 2.4 以降で 50 デバイス管理ノードに対しサポートされません。

新しい PID から生成された PAK をインストールすると、PAK ファイルで利用可能な数量に応じてデバイス管理ライセンス数が表示されます。必要なデバイス管理ノード数に基づいて、展開に複数のデバイス管理ライセンスを追加できます。Evaluation ライセンスでは、1 つのデバイス管理ノードをサポートします。

VM ノードのライセンス

Cisco ISE は、仮想アプライアンスとしても提供されています。リリース 2.4 以降では、展開に VM ノードの適切な VM ライセンスをインストールすることをお勧めします。VM ノードの数と CPU やメモリなどの各 VM ノードのリソースに基づいて、VM ライセンスをインストールする必要があります。そうでない場合、リリース 2.4 以降で VM ライセンスキーを調達してインストールする警告と通知が表示されますが、サービスは中断されません。

VM ライセンスは、インフラストラクチャライセンスなので、展開で使用可能なエンドポイントライセンスに関係なく VM ライセンスをインストールできます。展開に Evaluation、Base、Plus、Apex ライセンスのどれもインストールされていない場合でも、VM ライセンスをインストールできます。ただし、Base、Plus、または Apex ライセンスによって有効になる機能を使用するには、適切なライセンスをインストールする必要があります。

リリース 2.4 以降のインストールまたはアップグレードの後、展開済みの VM ノードの数とインストール済みの VM ライセンスの数の間に不一致がある場合、アラームが 14 日ごとに [アラーム (Alarms)] ダッシュレットに表示されます。アラームは、VM ノードのリソースに変化がある場合や、VM ノードが登録または登録解除されるたびにとも表示されます。

VM ライセンスは永続ライセンスです。VM ライセンスの変更は、Cisco ISE GUI にログインするたびに表示され、通知ダイアログボックスで [このメッセージを再度表示しない (Do not show this message again)] チェックボックスをオンにすると表示されなくなります。

以前に ISE VM ライセンスのいずれも購入していない場合は、『[Cisco Identity Services Engine 発注ガイド](#)』を参照して購入する適切な VM ライセンスを選択します。製品認証キー (PAK) が関連付けられていない ISE VM ライセンスを購入済みの場合、licensing@cisco.com で ISE VM 購入を反映する販売注文番号を使用して VM PAK を要求することができます。この要求は、過去に購入した ISE VM ごとに 1 つの中規模 VM ライセンスキーを提供するように処理されます。

VM ライセンスのカテゴリ

VM ライセンスは、小、中、大の 3 つのカテゴリで提供されます。これらのカテゴリは、ハードウェアアプライアンス、RAM 容量、CPU 数などのリソースによって異なります。たとえば、8 コアと 64 GB RAM を搭載した 3595 相当の VM ノードを使用している場合に、その VM で同じ機能をレプリケートするには、中カテゴリの VM ライセンスが必要になります。展開の要件に応じて、VM とそのリソースの数に基づいて、複数の VM ライセンスをインストールする必要があります。

次の表は、VM カテゴリに必要な VM 最小リソースを示しています。

VM カテゴリ	VM ライセンス仕様
小	<ul style="list-style-type: none">• 最小 16GB RAM および CPU 12 コア (SNS-3515 相当)。• 最小 32GB RAM および CPU 16 コア (SNS-3615 相当)。
中	<ul style="list-style-type: none">• 最小 64GB RAM および CPU 16 コア (SNS-3595 相当)。• 最小 96GB RAM および CPU 24 コア (SNS-3655 相当)。
大	<ul style="list-style-type: none">• 最小 256GB RAM および CPU 16 コア (500,000 を超える同時セッションをサポートするクラスターの MnT)。• 最小 256GB RAM および CPU 24 コア (SNS-3695 相当)。

ライセンスの詳細については、『[Cisco Identity Services Engine 管理者ガイド](#)』の「Cisco ISE ライセンス」の章を参照してください。

その他の参考資料

次のリンクには、Cisco ISE で作業するときを使用できる追加のリソースが含まれています。

https://www.cisco.com/c/en/us/td/docs/security/ise/end-user-documentation/Cisco_ISE_End_User_Documentation.html

通信、サービス、およびその他の情報

- シスコからタイムリーな関連情報を受け取るには、[Cisco Profile Manager](#) でサインアップしてください。
- 重要な技術によりビジネスに必要な影響を与えるには、[シスコサービス](#)にアクセスしてください。
- サービス リクエストを送信するには、[シスコサポート](#)にアクセスしてください。
- 安全で検証済みのエンタープライズクラスのアプリケーション、製品、ソリューション、およびサービスを探して参照するには、[Cisco DevNet](#)にアクセスしてください。
- 一般的なネットワーク、トレーニング、認定関連の出版物を入手するには、[Cisco Press](#)にアクセスしてください。
- 特定の製品または製品ファミリの保証情報を探すには、[Cisco Warranty Finder](#)にアクセスしてください。

Cisco バグ検索ツール

Cisco バグ検索ツール (BST) は、シスコ製品とソフトウェアの障害と脆弱性の包括的なリストを管理するシスコバグ追跡システムへのゲートウェイです。BSTは、製品とソフトウェアに関する詳細な障害情報を提供します。

マニュアルに関するフィードバック

シスコのテクニカルドキュメントに関するフィードバックを提供するには、それぞれのオンラインドキュメントの右側のペインにあるフィードバックフォームを使用してください。



第 2 章

アップグレードの準備

アップグレードプロセスを開始する前に、次のタスクを必ず実行してください。



- (注) プライマリおよびセカンダリ PAN のマルチノード展開で、監視ダッシュボードおよびレポートが、データレプリケーションの警告のため、アップグレード後に失敗することがあります。詳細については [CSCvd79546](#) を参照してください。回避策として、アップグレードを開始する前に、プライマリ PAN からセカンダリ PAN への手動での同期を実行します。



- (注) 現在、リリース 2.3 では、例外のため、リリース 2.3 パッチ 1 にアップグレードできません。詳細については [CSCvd79546](#) を参照してください。回避策として、アップグレードの前に、プライマリ PAN とセカンダリ PAN を同期します。

- [アップグレード中の時間を最小限に抑えて効率を最大化するためのガイドライン \(8 ページ\)](#)
- [アップグレードの失敗を防ぐためのデータの検証 \(10 ページ\)](#)
- [同じ名前の事前定義済み承認複合条件が存在する場合は、承認単純条件の名前を変更する \(13 ページ\)](#)
- [VMware 仮想マシンのゲスト オペレーティング システムと設定の変更 \(14 ページ\)](#)
- [スポンサーグループ名から 非 ASCII 文字を削除する \(14 ページ\)](#)
- [通信用に開く必要があるファイアウォールポート \(14 ページ\)](#)
- [プライマリ管理ノードからの Cisco ISE 設定および運用データのバックアップ \(15 ページ\)](#)
- [プライマリ管理ノードからのシステムログのバックアップ \(16 ページ\)](#)
- [CA 証明書チェーン \(16 ページ\)](#)
- [証明書の有効性の確認 \(16 ページ\)](#)
- [証明書を削除する \(17 ページ\)](#)
- [証明書および秘密キーのエクスポート \(17 ページ\)](#)
- [アップグレード前の PAN 自動フェールオーバーとスケジュールバックアップの無効化 \(18 ページ\)](#)

- NTP サーバーの設定と可用性の確認 (19 ページ)
- 仮想マシンのアップグレード (19 ページ)
- プロファイラ設定の記録 (19 ページ)
- Active Directory および内部管理者アカウントの資格情報の取得 (20 ページ)
- アップグレード前の MDM ベンダーのアクティベート (20 ページ)
- リポジトリの作成およびアップグレードバンドルのコピー (20 ページ)
- 利用可能なディスクサイズの確認 (21 ページ)
- ロードバランサ構成の確認 (21 ページ)
- ログの保持と MnT ハードディスクのサイズ変更 (22 ページ)

アップグレード中の時間を最小限に抑えて効率を最大化するためのガイドライン

次のガイドラインに従うと、アップグレードプロセス中に発生する可能性のある現在の展開の問題に対処できます。これにより、全体的なアップグレードのダウンタイムが削減され、効率性が向上します。

- アップグレードの開始前に、既存のバージョンで最新のパッチにアップグレードします。
- 実稼働ネットワークのアップグレード前に、ステージング環境でアップグレードをテストし、アップグレードの問題を特定して修正することをお勧めします。
 - データを交換するには、Cisco ISE 展開内のすべてのノードが同じパッチレベルにあることが必要です。



(注) 展開内のすべてのノードが同じ Cisco ISE バージョンおよびパッチバージョンにない場合、「**Upgrade cannot begin**」という警告メッセージが表示されます。このメッセージは、アップグレードがブロック状態にあることを示しています。アップグレードプロセスを開始する前に、展開のすべてのノードのバージョン（該当する場合はパッチバージョンを含む）が同じであることを確認します。

- 展開内の PSN の数と人員の可用性に基づいて、アップグレードする必要がある Cisco ISE の最終バージョンをインストールし、最新のパッチを適用して、対応可能な状態に保つことができます。
- MnT ログを保持する場合は、MnT ノードに対して前述のタスクを実行し、MnT ノードとして新しい展開に参加します。ただし、操作ログを保持する必要がない場合は、MnT ノードを再イメージ化してこの手順をスキップできます。

- 実稼働環境に影響のないマルチノード展開がある場合、Cisco ISE のインストールを並行して実行できます。ISE サーバーを並列にインストールすると、特に以前のリリースのバックアップと復元を使用している場合、時間が節約されます。
- 新しい展開に PSN を追加して、PAN からの登録プロセス中に既存のポリシーをダウンロードすることができます。ISE の遅延と帯域幅の計算ツールを使用して、Cisco ISE の展開における遅延と帯域幅の要件を理解します。
- 古いログをアーカイブし、それらを新しい展開に転送しないことをお勧めします。これは、後で MnT ロールを変更する場合に、MnT で復元された操作ログが異なるノードに同期されないためです。
- 完全な分散型展開を使用する2つのデータセンター (DC) がある場合は、バックアップ DC をアップグレードし、プライマリ DC をアップグレードする前に使用例をテストします。
- アップグレード前にローカルリポジトリでアップグレードソフトウェアをダウンロードおよび保存し、プロセスを高速化します。
- アップグレードプロセスの開始前にアップグレード準備ツール (URT) を使用し、設定データのアップグレードの問題を検出して修正します。ほとんどのアップグレードの障害は、設定データのアップグレードの問題が原因で発生します。URT は、可能な場合は、必ずアップグレード前にデータを検証し、問題を特定、報告、または修正します。URT は、セカンダリポリシー管理ノードまたはスタンドアロンノードで実行できる個別のダウンロード可能なバンドルとして利用できます。このツールを実行するのにダウンタイムは発生しません。次のビデオでは、URT の使用方法について説明します。
<https://www.cisco.com/c/en/us/td/docs/security/ise/videos/urt/v1-0/cisco-urt.html>



警告 プライマリポリシー管理ノードでは URT を実行しないでください。URT ツールは、MnT 運用データのアップグレードのシミュレーションは行いません。

- GUI を使用して Cisco ISE をアップグレードする場合、ノードあたりのプロセスのタイムアウトは4時間です。アップグレード所要時間が4時間を超えると、アップグレードは失敗します。アップグレード準備ツール (URT) のアップグレードに4時間以上かかる場合は、このプロセスに CLI を使用することをお勧めします。
- 設定を変更する前に、ロードバランサのバックアップを作成します。アップグレードウィンドウ中にロードバランサから PSN を削除し、アップグレード後に再び追加できます。
- 自動 PAN フェールオーバーを無効にして (設定されている場合)、アップグレード中に PAN 間のハートビートを無効にします。
- 既存のポリシーとルールを確認し、古くて、冗長な、更新されていないポリシーおよびルールを削除します。
- 不要なモニターリングログとエンドポイントデータを削除します。

- 設定と動作のログのバックアップを作成し、ネットワークに接続されていない一時的なサーバーで復元することができます。アップグレードウィンドウ中はリモートロギングターゲットを使用できます。

アップグレード後に次のオプションを使用して、MnT ノードに送信されるログの量を削減し、パフォーマンスを向上させることができます。

- MnT コレクションフィルタ ([管理 (Administration)] > [システム (System)] > [ロギング (Logging)] > [コレクションフィルタ (Collection Filters)]) を使用して、着信ログをフィルタリングし、AAA ログでエントリが重複しないようにします。
- リモートロギングターゲット ([管理 (Administration)] > [システム (System)] > [ロギング (Logging)] > [リモートロギングターゲット (Remote Logging Target)]) を作成し、個々のロギングカテゴリを特定のロギングターゲット ([システム (System)] > [ロギング (Logging)] > [ロギングカテゴリ (Logging categories)]) にルーティングできます。
- [管理 (Administration)] > [システム (System)] > [設定 (Settings)] > [プロトコル (Protocols)] > [RADIUS] ウィンドウで [繰り返し発生する更新を無視 (Ignore Repeated Updates)] オプションを有効にして、繰り返し発生するアカウントの更新を回避します。
- アップグレードの最新のアップグレードバンドルをダウンロードして使用します。バグ検索ツールで次のクエリを使用して、アップグレードを探し、オープンで修正済みの関連不具合をアップグレードします。 <http://cs.co/ise-upgrade-bugsearch>
- ユーザー数を減らした新しい展開ですべての使用例をテストし、サービスの継続性を確保します。

アップグレードの失敗を防ぐためのデータの検証

Cisco ISE には、アップグレードプロセスを開始する前に、データのアップグレードの問題を検出し修正するために実行できるアップグレード準備ツール (URT) が用意されています。

ほとんどのアップグレードの失敗は、データのアップグレードの問題が原因で発生します。URT は、可能な場合は、必ずアップグレード前にデータを検証し、問題を特定、報告または修正するように設計されています。

URT は、複数のノードにおけるハイアベイラビリティと他の展開を実現するためのセカンダリ管理ノード、または単一ノード展開のスタンドアロンノードで実行できる個別のダウンロード可能なバンドルとして使用できます。このツールを実行する場合、ダウンタイムは必要ありません。



警告 複数ノード展開の場合、プライマリポリシー管理ノードでは URT を実行しないでください。

Cisco ISE ノードのコマンドライン インターフェイス (CLI) から URT を実行できます。URT は次のことを行います。

1. サポートされているバージョンの Cisco ISE で URT が実行されているかどうかをチェックします。サポートされているバージョンは、リリース 2.1、2.2、2.3、および 2.4 です。
2. URT がスタンドアロン Cisco ISE ノードまたはセカンダリポリシー管理ノード (セカンダリ PAN) で実行されているかどうかを確認します。
3. URT バンドルの使用開始日から 45 日未満であるかどうかをチェックします。このチェックは、最新の URT バンドルを使用していることを確認するために行われます。
4. すべての前提条件が満たされているかどうかをチェックします。

次の前提条件が URT によって確認されます。

- バージョンの互換性
- ペルソナのチェック
- ディスク容量



(注) 「」 「」 「」 「」 で、利用可能なディスクサイズを確認します。ディスクサイズを増やす必要がある場合は、ISE を再インストールし、設定のバックアップを復元します。

- NTP サーバー
- メモリ
- システムと信頼できる証明書の検証

5. 構成データベースを複製します。
6. 最新のアップグレードファイルをアップグレードバンドルにコピーします。



(注) URT バンドルにパッチがない場合、出力は N/A を返します。これは、ホットパッチのインストール時の正常な動作です。

7. 複製されたデータベースでスキーマとデータのアップグレードを実行します。
 - (複製されたデータベースでアップグレードが成功した場合) アップグレードが完了するまでに要する予測時間を提示します。
 - (アップグレードが成功した場合) 複製されたデータベースを削除します。
 - (複製されたデータベースでアップグレードが失敗した場合) 必要なログを収集し、暗号化パスワードの入力を求めるプロンプトを表示し、ログバンドルを生成してローカルディスクに格納します。

アップグレード準備ツールのダウンロードと実行

アップグレード準備ツール（URT）は、アップグレードを実際に行う前に設定データを検証して、アップグレードの失敗を引き起こす可能性のある問題を特定します。

始める前に

URT の実行中は、同時に実行しないようにします。：

- データをバックアップまたは復元する
- ペルソナ変更の実行

ステップ 1 リポジトリの作成および URT バンドルのコピー（12 ページ）

ステップ 2 アップグレード準備ツールの実行（13 ページ）

リポジトリの作成および URT バンドルのコピー

リポジトリを作成して、URT バンドルをコピーします。リポジトリの作成方法については、『[Cisco ISE 管理者ガイド](#)』の「メンテナンスとモニター」の章にある「リポジトリの作成」を参照してください。

パフォーマンスと信頼性を高めるために、FTP を使用することを推奨します。低速 WAN リンクを介したリポジトリを使用しないでください。ノードに近い位置にあるローカルリポジトリを使用することを推奨します。

始める前に

リポジトリとの帯域幅接続が良好であることを確認してください。

ステップ 1 Cisco.com から URT バンドルをダウンロードします ([ise-urtbundle-2.6.0.xxx-1.0.0.SPA.x86_64.tar.gz](#))。

ステップ 2 必要に応じて、時間節約のために、次のコマンドを使用して Cisco ISE ノードのローカルディスクに URT バンドルをコピーします。

```
copy repository_url/path/ise-urtbundle-2.6.0.xxx-1.0.0.SPA.x86_64.tar.gz disk:/
```

たとえば、アップグレードバンドルのコピーに SFTP を使用するには、次を実行できます。

```
(Add the host key if it does not exist) crypto host_key add host mySftpserver  
copy sftp://aaa.bbb.ccc.ddd/ ise-urtbundle-2.6.0.xxx-1.0.0.SPA.x86_64.tar.gz disk:/
```

aaa.bbb.ccc.ddd は SFTP サーバーの IP アドレスまたはホスト名、ise-urtbundle-2.6.0.xxx-1.0.0.SPA.x86_64.tar.gz は URT バンドルの名前です。

アップグレード準備ツールの実行

アップグレード準備ツールは、アップグレードの失敗を引き起こす可能性のあるデータの問題を特定し、可能な限り問題を報告または修正します。URTを実行するには、次の手順を実行します。

始める前に

ローカルディスクにURTバンドルを置くと、時間を短縮できます。

application install コマンドを入力して、URT をインストールします。

```
application install ise-urtbundle-2.6.0.x.SPA.x86_64.tar.gz reponame
```

前述の操作を実行中にアプリケーションが正常にインストールされなかった場合、URT はアップグレードの失敗の原因を返します。問題を修正し、URT を再実行する必要があります。

同じ名前の事前定義済み承認複合条件が存在する場合は、承認単純条件の名前を変更する

Cisco ISEにはいくつかの事前定義された承認複合条件が付属しています。古い展開内の（ユーザ一定義された）承認単純条件が事前定義済み承認複合条件と同じ名前である場合、アップグレードプロセスは失敗します。アップグレードする前に、次の事前定義済み承認複合条件名のいずれかと名前が同じ承認単純条件は名前を変更する必要があります。

- Compliance_Unknown_Devices
- Non_Compliant_Devices
- Compliant_Devices
- Non_Cisco_Profiled_Phones
- Switch_Local_Web_Authentication
- Catalyst_Switch_Local_Web_Authentication
- Wireless_Access
- BYOD_is_Registered
- EAP-MSCHAPv2
- EAP-TLS
- Guest_Flow
- MAC_in_SAN
- Network_Access_Authentication_Passed

VMware 仮想マシンのゲストオペレーティングシステムと設定の変更

仮想マシンの Cisco ISE ノードをアップグレードする場合は、ゲストオペレーティングシステムを Red Hat Enterprise Linux (RHEL) のサポートされるバージョンに変更してあることを確認します。これを行うには、VM の電源をオフにし、ゲストオペレーティングシステムを更新し、変更後に VM の電源をオンにする必要があります。

RHEL 7 は E1000 および VMXNET3 ネットワークアダプタのみをサポートします。アップグレードする前に、ネットワークアダプタのタイプを変更する必要があります。

スポンサーグループ名から 非 ASCII 文字を削除する

リリース 2.2 より前に、非 ASCII 文字を持つスポンサーグループを作成した場合、アップグレードの前に、スポンサーグループの名前を変更し、ASCII 文字のみを使用するようにしてください。

Cisco ISE リリース 2.2 以降のスポンサーグループ名では、非 ASCII 文字はサポートされません。

通信用に開く必要があるファイアウォールポート

プライマリ管理ノードと他のノードとの間にファイアウォールが設置されている場合は、次の各ポートがアップグレード前に開いている必要があります。

- TCP 1521 : プライマリ管理ノードとモニターリングノード間の通信用。
- TCP 443 : プライマリ管理ノードとその他すべてのセカンダリノード間の通信用。
- TCP 12001 : グローバルクラスタのレプリケーション用。
- TCP 7800 および 7802 : (ポリシーサービスノードがノードグループの一部である場合に限り該当) PSN グループのクラスタリング用。

Cisco ISE が使用するすべてのポートのリストについては、『[Cisco Identity Services Engine Hardware Installation Guide](#)』を参照してください。

Cisco ISE が使用するポートの完全なリストについては、『[Cisco ISE Ports Reference](#)』を参照してください。

プライマリ管理ノードからの Cisco ISE 設定および運用データのバックアップ

コマンドライン インターフェイス (CLI) または GUI から Cisco ISE 設定および運用データのバックアップを取得します。CLI コマンドは次のとおりです。

```
backup backup-name repository repository-name {ise-config | ise-operational} encryption-key {hash | plain} encryption-keyname
```



(注) Cisco ISE が VMware で実行されている場合、ISE データをバックアップするのに、VMware スナップショットはサポートされていません。

VMware スナップショットは指定した時点で、VM のステータスを保存します。マルチノード Cisco ISE 展開環境では、すべてのノードのデータは、現在のデータベース情報と継続的に同期されます。スナップショットを復元すると、データベースのレプリケーションと同期の問題を引き起こす可能性があります。シスコは、データのアーカイブおよび復元用に、Cisco ISE に含まれるバックアップ機能を使用することを推奨します。

VMware スナップショットを使用して ISE データをバックアップすると、Cisco ISE サービスが停止します。ISE ノードを起動するには、再起動が必要です。

また、Cisco ISE 管理者用ポータルから設定および運用データのバックアップを取得することができます。バックアップファイルを格納するリポジトリを作成したことを確認します。ローカルリポジトリを使用してバックアップしないでください。リモートモニターリングノードのローカルリポジトリで、モニターリングデータをバックアップすることはできません。次のリポジトリタイプはサポートされていません。CD-ROM、HTTP、HTTPS、または TFTP。これは、これらのリポジトリタイプが読み取り専用であるか、またはプロトコルでファイルのリストがサポートされないためです。

1. [管理 (Administration)]>[メンテナンス (Maintenance)]>[バックアップと復元 (Backup and Restore)] を選択します。
2. [すぐにバックアップ (Backup Now)] をクリックします。
3. バックアップを実行するために必要な値を入力します。
4. [OK] をクリックします。
5. バックアップが正常に完了したことを確認します。

分散展開では、バックアップの実行中にノードのロールを変更したり、ノードの設定を行ったりすることはできません。バックアップの実行中にノードのロールを変更すると、すべてのプロセスがシャットダウンし、データに不一致が生じる場合があります。ノードのロールを変更する際は、バックアップが完了するまで待機してください。

Cisco ISE はタイムスタンプを持つバックアップファイル名を付け、指定されたりポジトリにファイルを保存します。タイムスタンプに加えて、Cisco ISE は設定バックアップには CFG タグ、操作バックアップには OPS タグを追加します。バックアップファイルが指定リポジトリにあることを確認します。



- (注) Cisco ISE では、ある ISE ノード (A) からバックアップを取得して、別の ISE ノード (B) に復元することができます。両方のノードは同じホスト名 (IP アドレスは異なる) です。ただし、ノード B 上のバックアップを復元した後は、証明書とポータルグループタグの問題が生じる可能性があるため、ノード B のホスト名を変更することはできません。

プライマリ管理ノードからのシステムログのバックアップ

コマンドラインインターフェイス (CLI) を使用して、プライマリ管理ノードからシステムログのバックアップを取得します。CLI コマンドは次のとおりです。

```
backup-logs backup-name repository repository-name encryption-key { hash | plain } encryption-key name
```

CA 証明書チェーン

Cisco ISE 2.6 にアップグレードする前に、内部 CA 証明書チェーンが有効であることを確認します。

1. [管理 (Administration)] > [システム (System)] > [証明書 (Certificates)] > [認証局 (Certificate Authority Certificates)] を選択します。
2. 展開内の各ノードについて、[フレンドリ名 (Friendly Name)] 列に [証明書サービスエンドポイントサブ CA (Certificate Services Endpoint Sub CA)] と示されている証明書を選択します。[表示 (View)] をクリックして、「証明書のステータスが良好 (Certificate Status is Good)」メッセージが表示されるかどうか確認します。
3. 証明書チェーンが破損している場合は、Cisco ISE をアップグレードする前に問題を修正する必要があります。[管理 (Administration)] > [システム (System)] > [証明書 (Certificates)] > [証明書の管理 (Certificate Management)] > [証明書署名要求 (Certificate Signing Requests)] > [ISE ルート CA (ISE Root CA)] の順に選択します。

証明書の有効性の確認

アップグレードプロセスは、Cisco ISE の信頼できる証明書またはシステム証明書ストアの証明書の期限が切れていると、失敗します。アップグレードの前に、[信頼できる証明書 (Trusted

Certificates)] と [システム証明書 (System Certificates)] ウィンドウ ([管理 (Administration)] > [システム (System)] > [証明書 (Certificates)] > [証明書の管理 (Certificate Management)]) の [有効期限 (Expiration Date)] の有効性を確認し、必要に応じて更新してください。

また、アップグレードの前に、[CA 証明書 (CA Certificates)] ウィンドウ ([管理 (Administration)] > [システム (System)] > [証明書 (Certificates)] > [証明書機関 (Certificate Authority)] > [証明書機関の証明書 (Certificate Authority Certificates)]) の [有効期限 (Expiration Date)] の有効性を確認し、必要に応じて更新してください。

証明書を削除する

期限切れの証明書を削除するには、次の手順を実行します。

-
- ステップ 1 [管理 (Administration)] > [システム (System)] > [証明書 (Certificates)] > [証明書の管理 (Certificate Management)] > [システム証明書 (System Certificates)] の順に選択します。
 - ステップ 2 期限切れの証明書を選択します。
 - ステップ 3 [削除 (Delete)] をクリックします。
 - ステップ 4 [管理 (Administration)] > [システム (System)] > [証明書 (Certificates)] > [証明書の管理 (Certificate Management)] > [信頼できる証明書 (Trusted Certificates)] の順に選択します。
 - ステップ 5 期限切れの証明書を選択します。
 - ステップ 6 [削除 (Delete)] をクリックします。
 - ステップ 7 [管理 (Administration)] > [システム (System)] > [証明書 (Certificates)] > [認証局 (Certificate Authority)] > [認証局証明書 (Certificate Authority Certificates)] の順に選択します。
 - ステップ 8 期限切れの証明書を選択します。
 - ステップ 9 [削除 (Delete)] をクリックします。
-

証明書および秘密キーのエクスポート

次の項目をエクスポートすることを推奨します。

- すべてのローカル証明書 (展開内のすべてのノードから) およびその秘密キーを安全な場所にエクスポートします。証明書設定 (どのサービスに証明書が使用されたか) を記録します。

-
- ステップ 1 [管理 (Administration)] > [システム (System)] > [証明書 (Certificates)] > [証明書の管理 (Certificate Management)] > [システム証明書 (System Certificates)] の順に選択します。
 - ステップ 2 証明書を選択し、[エクスポート (Export)] をクリックします。
 - ステップ 3 [証明書および秘密キーをエクスポート (Export Certificates and Private Keys)] ラジオボタンを選択します。

ステップ4 [秘密キーのパスワード (Private Key Password)] と [パスワードの確認 (Confirm Password)] を入力します。

ステップ5 [エクスポート (Export)] をクリックします。

- プライマリ管理ノードの信頼できる証明書ストアからすべての証明書をエクスポートします。証明書設定 (どのサービスに証明書が使用されたか) を記録します。

ステップ1 [管理 (Administration)] > [システム (System)] > [証明書 (Certificates)] > [証明書の管理 (Certificate Management)] > [信頼できる証明書 (Trusted Certificates)] の順に選択します。

ステップ2 証明書を選択し、[エクスポート (Export)] をクリックします。

ステップ3 [ファイルを保存 (Save File)] をクリックして証明書をエクスポートします。

ステップ4 [管理 (Administration)] > [システム (System)] > [証明書 (Certificates)] > [認証局 (Certificate Authority)] > [認証局証明書 (Certificate Authority Certificates)] の順に選択します。

ステップ5 証明書を選択し、[エクスポート (Export)] をクリックします。

ステップ6 [証明書および秘密キーをエクスポート (Export Certificates and Private Keys)] ラジオボタンを選択します。

ステップ7 [秘密キーのパスワード (Private Key Password)] と [パスワードの確認 (Confirm Password)] を入力します。

ステップ8 [エクスポート (Export)] をクリックします。

ステップ9 [ファイルを保存 (Save File)] をクリックして証明書をエクスポートします。

アップグレード前の PAN 自動フェールオーバーとスケジュールバックアップの無効化

Cisco ISE のバックアップを実行した場合は、展開の変更を実行できません。そのため、アップグレードの妨げにならないようにするには自動設定を無効にする必要があります。Cisco ISE をアップグレードする前に、次の設定を無効にしていることを確認してください。

- プライマリ管理ノードの自動フェールオーバー：プライマリ管理ノードを自動フェールオーバーに設定している場合は、Cisco ISE をアップグレードする前に、自動フェールオーバーオプションを必ず無効にします。
- スケジュールバックアップ：アップグレード後にバックアップをスケジュールし直すように展開のアップグレードを計画します。バックアップスケジュールを無効にし、アップグレード後に再作成することができます。

スケジュール頻度が一度のバックアップは、Cisco ISE アプリケーションが再起動するたびにトリガーされます。このように、一度だけ実行するように設定されたバックアップスケジュールは、アップグレード前に設定を無効にしてください。

NTP サーバーの設定と可用性の確認

アップグレード中、Cisco ISE ノードは再起動して、プライマリ管理ノードからセカンダリ管理ノードにデータを移行、複製します。これらの操作では、ネットワーク内の NTP サーバーが正しく設定され、到達可能であることが重要です。NTP サーバーが正しく設定されていない、または到達不能な場合、アップグレードプロセスは失敗します。

ネットワーク内の NTP サーバーが、アップグレード中に到達可能で、応答性があり、同期していることを確認します。

仮想マシンのアップグレード

Cisco ISE ソフトウェアは、UCS ハードウェアで使用可能な最新の CPU/メモリ容量をサポートするために、チップおよびアプライアンスのキャパシティと同期している必要があります。ISE のバージョンが新しくなるにつれ、古いハードウェアのサポートが段階的に廃止され、新しいハードウェアが導入されます。パフォーマンスを向上させるために、仮想マシン (VM) のキャパシティをアップグレードすることをお勧めします。VM のアップグレードを計画する際は、OVA ファイルを使用するして ISE ソフトウェアをインストールすることを強くお勧めします。各 OVA ファイルは、VM を記述するために使用されるファイルを含むパッケージであり、Cisco ISE ソフトウェアをインストールするためにアプライアンスに必要なハードウェアリソースを確保します。

VM とハードウェア要件の詳細については、『[Cisco Identity Services Engine インストールガイド](#)』の「ハードウェアおよび仮想アプライアンスの要件」を参照してください。

Cisco ISE VM は、VM インフラストラクチャに専用リソースが必要です。ISE には、パフォーマンスと拡張性のためにハードウェアアプライアンスに類似した十分な量の CPU コアが必要です。リソースの共有は、高い CPU 使用率、ユーザー認証の遅延、登録、ログの遅延と廃棄、レポート、ダッシュボードの応答性などによりパフォーマンスに影響することが判明しています。これは、企業内のエンドユーザーと管理者のユーザーエクスペリエンスに直接影響します。



- (注) アップグレード時には、共有リソースではなく、CPU、メモリ、ハードディスク領域に予約済みのリソースを使用することが重要です。

Cisco ISE リリース 2.4 以降では、ローカルディスク割り当てが 29 GB に増えるため、仮想マシンの最小ディスクサイズが 300 GB 必要です。

プロファイラ設定の記録

プロファイラサービスを使用する場合、管理者ポータルから、各ポリシーサービスノードのプロファイラ構成を必ず記録してください ([管理 (Administration)] > [システム (System)] >

[展開 (Deployment)]><ノード>>)。ノードを選択して、[ノードの編集 (Edit Node)]をクリックします。[ノードの編集 (Edit Node)] ページで、[プロファイリング設定 (Profiling Configuration)] タブに移動します。構成情報をメモするか、スクリーンショットを取得できます。

Active Directory および内部管理者アカウントの資格情報の取得

外部アイデンティティソースとして Active Directory を使用する場合は、Active Directory のクレデンシャルと有効な内部管理者アカウントクレデンシャルを手元に用意してください。アップグレード後に、Active Directory 接続が失われることがあります。この場合、管理者ポータルにログインするために ISE 内部管理者アカウント、Cisco ISE と Active Directory を再接続するために Active Directory のクレデンシャルが必要です。

アップグレード前の MDM ベンダーのアクティベート

MDM機能を使用する場合は、アップグレードの前に、MDMベンダーのステータスがアクティブであることを確認します。

MDM サーバー名が承認ポリシーで使用され、対応する MDM サーバーが無効の場合は、アップグレードプロセスは失敗します。回避策として、次のいずれかが可能です。

1. アップグレードの前に MDM サーバーを有効にします。
2. 承認ポリシーから MDM サーバー名属性を使用する条件を削除します。

リポジトリの作成およびアップグレードバンドルのコピー

リポジトリを作成して、バックアップを取得してアップグレードバンドルをコピーします。リポジトリの作成方法については、『[Cisco ISE 管理者ガイド](#)』の「メンテナンスとモニター」の章にある「リポジトリの作成」を参照してください。

パフォーマンスと信頼性を高めるために、FTP を使用することを推奨します。低速 WAN リンクを介したリポジトリを使用しないでください。ノードに近い位置にあるローカルリポジトリを使用することを推奨します。

リポジトリとのインターネット接続が良好であることを確認します。



- (注) リポジトリからノードにアップグレードバンドルをダウンロードする場合、ダウンロードが完了するまでに 35 分以上かかるとダウンロードがタイムアウトします。この問題は、インターネットの帯域幅が不十分なために発生します。

ローカルディスクにアップグレードバンドルを置くと、アップグレード時間を短縮できます。また、**application upgrade prepare <upgrade bundle name> <repository name>** コマンドを使用してアップグレードバンドルをローカルディスクにコピーして抽出することもできます。



- (注)
- リポジトリとの帯域幅接続が良好であることを確認してください。リポジトリからノードにアップグレードバンドル（ファイルサイズは約9GB）をダウンロードする場合、ダウンロードが完了するまでに35分以上かかるとダウンロードがタイムアウトします。
 - ローカルディスクに設定ファイルが保存されている場合は、アップグレードの実行時に削除されます。したがって、Cisco ISE リポジトリを作成し、このリポジトリにコンフィギュレーションファイルをコピーすることをお勧めします。

アップグレードバンドルは [Cisco.com](https://www.cisco.com) からダウンロードします。

リリース 2.6 にアップグレードするには、このアップグレードバンドルを使用します。
`ise-upgradebundle-2.x-to-2.6.0.xxx.SPA.x86_64.tar.gz`

アップグレード用に、次のコマンドを使用して Cisco ISE ノードのローカルディスクにアップグレードバンドルをコピーできます。

copy repository_url/path/ise-upgradebundle-2.x-to-2.6.0.xxx.SPA.x86_64.tar.gz disk:/

たとえば、アップグレードバンドルのコピーに SFTP を使用するには、次を実行できます。

1. （ホストキーが存在しない場合は追加します） **crypto host_key add host mySftpserver**
2. **copy sftp://aaa.bbb.ccc.ddd/ise-upgradebundle-2.x-to-2.6.0.xxx.SPA.x86_64.tar.gz disk:/**

`aaa.bbb.ccc.ddd` は SFTP サーバーの IP アドレスまたはホスト名、
`ise-upgradebundle-2.x-to-2.6.0.xxx.SPA.x86_64.tar.gz` はアップグレードバンドルの名前です。

利用可能なディスクサイズの確認

仮想マシンに必要なディスク容量が割り当てられていることを確認します。詳細については、『[Cisco ISE インストールガイド](#)』を参照してください。ディスクサイズを増やす必要がある場合は、ISE を再インストールし、設定のバックアップを復元する必要があります。

ロードバランサ構成の確認

プライマリ管理ノード（PAN）とポリシーサービスノード（PSN）間でロードバランサを使用している場合は、ロードバランサで設定されたセッションタイムアウトがアップグレードプロセスに影響しないことを確認してください。セッションタイムアウト値を低く設定すると、ロードバランサの背後にある PSN でアップグレードプロセスに影響する可能性があります。たとえば、PAN から PSN へのデータベースダンプ中にセッションがタイムアウトすると、PSN でアップグレードプロセスが失敗する可能性があります。

ログの保持と MnT ハードディスクのサイズ変更

アップグレードでは、MnT ディスクの容量を変更する必要はありません。ただし、ログを継続的に記録し、ハードウェアの容量を増やす必要がある場合は、ログ保持のニーズに応じて MnT のハードディスクのサイズを計画できます。ログ保持の容量が Cisco ISE リリース 2.2 から何倍も増加していることを理解することが重要です。

また、Cisco ISE MnT に負荷をかける可能性があるさまざまなデバイスからの不要なログについては、アクティブなコレクションフィルタ（[管理（Administration）]>[システム（System）]>[ロギング（Logging）]>[コレクションフィルタ（Collection filters）]に移動）を使用することもできます。

コレクションフィルタの詳細については、『Cisco Identity Services Engine 管理者ガイド』の「メンテナンスとモニター」の章にある「収集フィルタの設定」を参照してください。

ISE のパフォーマンスと拡張性に関するコミュニティページの ISE ストレージ要件を参照してください。該当の表には、RADIUS のエンドポイントの数と TACACS+ のネットワークデバイスの数に基づくログの保持が示されています。ログの保持は、TACACS+ または RADIUS あるいはその両方について個別に計算する必要があります。



第 3 章

ノードのアップグレードの順序

GUI、バックアップと復元、または CLI を使用して Cisco ISE をアップグレードできます。GUI を使用してアップグレードする場合は、アップグレードするノードの順序を選択できます。ただし、展開環境をアップグレードする場合は、次に示すノードの順序に従うことをお勧めします。これにより、復元力とロールバック機能を最大限に活用しながら、ダウンタイムを短縮できます。

1. すべての設定とモニターリングデータをバックアップします。また、内部 CA キーと証明書チェーンのコピーをエクスポートし、すべての ISE ノードの ISE サーバー証明書のバックアップを取る必要があります。必要に応じて、手動で簡単にロールバックできるように、アップグレードを開始する前にこのタスクを実行する必要があります。

2. セカンダリ管理ノード

この時点では、プライマリ管理ノードは以前のバージョンのまま、アップグレードに失敗した場合はロールバックに使用できます。

3. プライマリ モニターリング ノードまたはセカンダリ モニターリング ノード

分散展開の場合、既存の Cisco ISE 展開のセカンダリ管理ノードがあるサイトで使用可能なすべてのノードをアップグレードします。

4. ポリシーサービスノード

GUI を使用して 2.6 からそれ以降のリリースにアップグレードする場合は、同時にアップグレードする PSN のグループを選択できます。PSN のグループを選択することにより、全体的なアップグレードのダウンタイムが削減されます。

ポリシー サービス ノードのセットをアップグレードした後、アップグレードが成功したかどうかを確認し ([アップグレードプロセスの確認 \(41 ページ\)](#) を参照)、ネットワークテストを実行して新しい展開環境が期待どおりに機能していることを確認します。アップグレードが成功した場合は、ポリシーサービスノードの次のセットをアップグレードできます。

5. セカンダリ モニターリング ノードまたはプライマリ モニターリング ノード
6. プライマリ管理ノード

プライマリ管理ノードをアップグレードした後、アップグレードの検証テストとネットワークテストを再実行します。



- (注) プライマリ管理ノード (アップグレードの必要がある古い展開からの最後のノード) で登録中にアップグレードが失敗した場合、アップグレードはロールバックされ、ノードはスタンドアロンノードになります。CLIから、スタンドアロンノードとしてノードをアップグレードします。セカンダリ管理ノードとして新しい展開にノードを登録します。

アップグレード後、セカンダリ管理ノードはプライマリ管理ノードになり、元のプライマリ管理ノードはセカンダリ管理ノードになります。必要に応じて、[ノードの編集 (Edit Node)] ウィンドウで[プライマリに昇格 (Promote to Primary)] をクリックして、セカンダリ管理ノードを昇格してプライマリ管理ノードにします (古い展開環境と一致させます)。

管理ノードがモニタリングペルソナも担当する場合は、次の表に示す手順に従ってください。

現在の展開内のノードペルソナ	アップグレードの順序
セカンダリ管理/プライマリ モニタリングノード、ポリシーサービスノード、プライマリ管理/セカンダリ モニタリングノード	<ol style="list-style-type: none"> 1. セカンダリ管理/プライマリ モニタリングノード 2. ポリシーサービスノード 3. プライマリ管理/セカンダリ モニタリングノード
セカンダリ管理/セカンダリ モニタリングノード、ポリシーサービスノード、プライマリ管理/プライマリ モニタリングノード	<ol style="list-style-type: none"> 1. セカンダリ管理/セカンダリ モニタリングノード 2. ポリシーサービスノード 3. プライマリ管理/プライマリ モニタリングノード
セカンダリ管理ノード、プライマリ モニタリングノード、ポリシーサービスノード、プライマリ管理/セカンダリ モニタリングノード	<ol style="list-style-type: none"> 1. セカンダリ管理ノード 2. プライマリ モニタリングノード 3. ポリシーサービスノード 4. プライマリ管理/セカンダリ モニタリングノード

現在の展開内のノードペルソナ	アップグレードの順序
セカンダリ管理ノード、セカンダリ モニターリング ノード、ポリシーサービスノード、プライマリ管理/プライマリ モニターリング ノード	<ol style="list-style-type: none"> 1. セカンダリ管理ノード 2. セカンダリ モニターリング ノード 3. ポリシーサービスノード 4. プライマリ管理/プライマリ モニターリング ノード
セカンダリ管理/プライマリ モニターリング ノード、ポリシーサービスノード、セカンダリ モニターリング ノード、プライマリ管理 ノード	<ol style="list-style-type: none"> 1. セカンダリ管理/プライマリ モニターリング ノード 2. ポリシーサービスノード 3. セカンダリ モニターリング ノード 4. プライマリ管理ノード
セカンダリ管理/セカンダリ モニターリング ノード、ポリシーサービスノード、プライマリ モニターリング ノード、プライマリ管理 ノード	<ol style="list-style-type: none"> 1. セカンダリ管理/セカンダリ モニターリング ノード 2. ポリシーサービスノード 3. プライマリ モニターリング ノード 4. プライマリ管理ノード

次の場合にエラーメッセージ「**No Secondary Administration Node in the Deployment**」が表示されます。

- 展開内にセカンダリ管理ノードが存在しない。
- セカンダリ管理ノードがダウンしている。
- セカンダリ管理ノードはアップグレードされ、アップグレード済みの展開に移行されている。通常、セカンダリ管理ノードをアップグレードした後に、[展開の詳細の更新 (Refresh Deployment Details)] オプションを使用したときに、この問題が発生する可能性があります。

この問題を解決するには、該当する次のいずれかのタスクを実行します。

- 展開にセカンダリ管理ノードがない場合は、セカンダリ管理ノードを設定して、アップグレードを再試行します。
- セカンダリ管理ノードがダウンしている場合は、そのノードを起動し、アップグレードを再試行します。
- セカンダリ管理ノードがアップグレードされ、アップグレード済みの展開に移行されている場合は、CLI を使用して展開内の他のノードを手動でアップグレードします。

- [アップグレード方法の選択 \(26 ページ\)](#)
- [バックアップと復元方法を使用した Cisco ISE 展開のアップグレード \(推奨\) \(30 ページ\)](#)
- [GUI からの Cisco ISE 展開のアップグレード \(34 ページ\)](#)
- [CLI からの Cisco ISE 展開のアップグレード \(36 ページ\)](#)

アップグレード方法の選択

Cisco ISE のこのリリースでは、次のアップグレードプロセスがサポートされています。アップグレードの技術上の専門知識とアップグレードに割くことのできる時間に応じて、以下のアップグレードプロセスから選択できます。

- [バックアップと復元の手順を使用した Cisco ISE のアップグレード \(推奨\)](#)
- [GUI からの Cisco ISE 展開環境のアップグレード](#)
- [CLI からの Cisco ISE 展開環境のアップグレード](#)

表 2: Cisco ISE アップグレード方法の比較

比較要素	バックアップと復元 (推奨)	GUI を使用したアップグレード	CLI を使用したアップグレード
比較の概要	高速だが、より多くの管理作業が必要	時間がかかるが、必要な管理作業は少ない	時間がかかり、必要な管理作業も多い
難しさ	困難	容易	適度
最小バージョン	Cisco ISE 2.1 以降	Cisco ISE 2.1 以降	Cisco ISE 2.1 以降
VM	十分なキャパシティがある場合は、新しい VM を事前設定して、新しい PAN にそれらの VM をすぐに参加させることができる	各 PSN は順次アップグレードされ、合計アップグレード時間が直線的に増加する	各 PSN はアップグレードされるが、同時にアップグレードされるため、合計アップグレード時間が短縮される
時間	PSN は新しいバージョンでイメージ化され、アップグレードされなため、アップグレードのダウンタイムは最小	各 PSN は順次アップグレードされ、合計アップグレード時間が直線的に増加する	各 PSN はアップグレードされるが、同時にアップグレードされるため、合計アップグレード時間が短縮される

比較要素	バックアップと復元 (推奨)	GUIを使用したアップ グレード	CLIを使用したアップ グレード
担当者	設定と運用のログをやりとりするさまざまな事業部門の複数の関係者が参加	手動操作の少ない自動アップグレードプロセス	Cisco ISEに関する技術的な専門知識
ロールバック	ノードの再イメージ化が必要	簡単なロールバックオプション	簡単なロールバックオプション

アップグレード方法の詳細な比較を以下に示します。

バックアップと復元方法を使用した Cisco ISE のアップグレード

Cisco ISE ノードの再イメージ化は、初期展開の一部としておよびトラブルシューティング時に実行されますが、新しいバージョンが展開された後、新しい展開にポリシーを復元している間に Cisco ISE ノードを再イメージ化して展開をアップグレードすることもできます。

リソースが制限されていて、新しい展開で並列の ISE ノードをスピンアップできない場合、他のノードがアップグレードされる前に、セカンダリ PAN と MnT がアップグレードされる実稼働展開から削除されます。ノードは新しい展開に移動します。設定と運用のバックアップは、1つの並列展開を作成している各ノード上の以前の展開から復元されます。これにより、手動で操作する必要なく、ポリシーセット、カスタムプロファイル、ネットワーク アクセス デバイス、およびエンドポイントを新しい展開に復元できます。

バックアップと復元プロセスを使用して Cisco ISE をアップグレードする利点は、次のとおりです。

- 以前の ISE 展開から設定と運用ログを復元できます。したがって、データ損失を防ぐことができます。
- 新しい展開で再利用する必要があるノードを手動で選択できます。
- 複数の PSN を同時にアップグレードすることで、アップグレードのダウンタイムを削減できます。
- メンテナンス時間外にノードをステージングして、実稼働時のアップグレード時間を短縮できます。

バックアップと復元を使用して Cisco ISE をアップグレードする前に考慮すべき事項

必要なリソース：バックアップおよび復元によるアップグレードプロセスでは、リリース前に ISE 展開用に予約できる追加のリソースが必要です。既存のハードウェアを再利用する場合は、オンラインのままのノードに追加の負荷を分散させる必要があります。したがって、展開でノードあたりのユーザー数に対処できるように、展開の開始前に現在の負荷と遅延の制限を評価する必要があります。

必要な人員：アップグレードを実行するには、ネットワーク管理、セキュリティ管理、データセンター、仮想化リソースなど、複数の事業部門の参加が必要です。さらに、ノードを新しい

展開に再参加させて、証明書を復元し、アクティブディレクトリに参加させて、ポリシーの動機を待機する必要があります。これにより、複数のリロードが行われ、新規展開のタイムフレームが必要になる場合があります。

ロールバックメカニズム：ノードの再イメージ化により、すべての情報と構成の設定は、以前の展開から消去されます。したがって、バックアップと復元によるアップグレードのロールバックメカニズムは、2回目のノードの再イメージ化と同じ手順になります。

バックアップと復元によるアップグレードプロセスのベストプラクティスは次のとおりです。

- スタンドアロン環境を作成するか、または RADIUS 要求の仮想 IP アドレスを切り替える専用のロードバランサを用意します。
- メンテナンス期間の前に余裕を持って展開プロセスを開始し、ユーザーのロードバランサの切り替え先を新しい展開環境に設定できます。

GUI からの Cisco ISE 展開環境のアップグレード

また、カスタマイズ可能なオプションを使用して、GUI からワンクリックで Cisco ISE をアップグレードすることもできます。GUI によるアップグレードは、**[ISE管理 (ISE Administration)] > [アップグレード (Upgrade)]** メニューを使用して実行し、ISO イメージをダウンロードするための新しいリポジトリが必要です。

アップグレード中、セカンダリ PAN がアップグレードされた展開に自動的に移動して、最初にアップグレードされ、次にプライマリ MnT がアップグレードされます。その結果、これらのアップグレードのいずれかが失敗した場合、ノードを以前のバージョンにロールバックして、以前の ISE 展開に再参加する必要があります。後から PSN が 1 つずつ新しい展開に移動し、アップグレードされます。アップグレードに失敗した場合に、アップグレードの続行、または中止を選択することもできます。これにより、同じ Cisco ISE 展開のデュアルバージョンが作成され、アップグレードを続行する前にトラブルシューティングを行えます。すべての PSN がアップグレードされると、セカンダリ MnT とプライマリ PAN がアップグレードされて、新しい Cisco ISE 展開に参加します。

このアップグレードプロセスに必要な技術知識はわずかであるため、1 人の管理者がアップグレードを開始し、NOC または SOC エンジニアを割り当てて、アップグレードのステータスをモニターしてレポートするか、TAC ケースをオープンします。

GUI から Cisco ISE をアップグレードする利点は次のとおりです。

- アップグレードが最小限の操作で自動化されます。
- PSN のアップグレード順序を選択すると、特にデータセンター間で冗長性が得られる場合、可能な限り継続性を確保できます。
- 追加の人員、サードパーティ製のハイパーバイザ、またはネットワーク アクセス デバイスを使用せずに、1 人の管理者だけでアップグレードを実行できます。

GUI から Cisco ISE をアップグレードする前に考慮すべき事項

失敗した場合の続行：アップグレードに失敗した場合に、アップグレードの続行、または中止を選択することもできます。これにより、同じ Cisco ISE 展開のデュアルバージョンが作成さ

れ、アップグレードを続行する前にトラブルシューティングを行えます。シスコのアップグレード準備ツールで非互換性や不良構成が示されますが、[続行 (Proceed)] フィールドがオンになっている場合、アップグレード前にデューデリジェンスが機能しないと、追加のエラーが発生する可能性があります。

ロールバックメカニズム : PAN ノードまたは MnT ノードでアップグレードが失敗した場合、ノードは自動的にロールバックされます。ただし、PSN がアップグレードに失敗した場合、ノードは同じ Cisco ISE バージョンに残り、修正できますが、冗長性が低下します。この間、Cisco ISE はまだ動作しているため、再イメージ化しない限りロールバック機能は制限されます。

必要な時間 : 各 PSN のアップグレードには約 90 ~ 120 分かかります。したがって、PSN の数が多い場合は、それらすべてをアップグレードする時間が必要です。

GUI からのアップグレードのベストプラクティス : PSN の数が多い場合は、PSN をまとめてグループ化し、アップグレードを実行してください。

CLI からの Cisco ISE 展開環境のアップグレード

CLI からの Cisco ISE のアップグレードは複雑なプロセスであり、管理者がアップグレードイメージをローカルノードにダウンロードして、アップグレードを実行し、アップグレードプロセス全体を通じて各ノードを個別にモニターする必要があります。アップグレードのシーケンスは GUI によるアップグレードの場合と基本的に似ていますが、このアプローチではモニターリングと操作に手間がかかります。

CLI からのアップグレードは、必要な作業レベルが高いため、トラブルシューティング目的でのみ使用することをお勧めします。

CLI から Cisco ISE をアップグレードする利点は次のとおりです。

- CLI では、アップグレードの実行中に管理者に追加のログメッセージが示されます。
- アップグレードされるノードは、より細かな制御のうえで選択して、同時にアップグレードできます。アップグレードされていないノードは、エンドポイントが展開全体で再調整されるため、追加の負荷に対処できます。
- CLI でのロールバックは、スクリプトで以前の変更を取り消すことができるため、はるかに簡単です。
- イメージはノード上にローカルに存在するため、PAN と PSN の間のコピーエラー（存在する場合）は排除されます。

CLI から Cisco ISE をアップグレードする前に考慮すべき事項

CLI を使用して Cisco ISE をアップグレードするには、技術的な専門知識が必要で、時間もかかります。

バックアップと復元方法を使用した Cisco ISE 展開のアップグレード (推奨)

バックアップと復元によるアップグレード方法の概要

シスコでは、バックアップと復元によるアップグレードプロセスを他のアップグレードプロセスよりも推奨しています。バックアップと復元によるアップグレードプロセスを使用すれば、現在の Cisco ISE 展開ノードの設定を復元でき、アップグレードプロセス中に障害が発生した場合にデータの損失を防ぐこともできます。この手順を開始するには、既存の Cisco ISE 展開環境の設定と運用のバックアップを作成し、新しい展開環境に適用します。

バックアップと復元によるアップグレードプロセスのベストプラクティスは次のとおりです。

- スタンドアロン環境を作成するか、または RADIUS 要求の仮想 IP アドレスを切り替える専用のロードバランサを用意します。
- メンテナンス期間の前に余裕を持って展開プロセスを開始し、ユーザーのロードバランサの切り替え先を新しい展開環境に設定できます。
- RSA SecurID ID ソースを使用する場合、新しい PSN を追加するときに、RSA 認証マネージャのプライマリインスタンスですべての PSN を使用して新しい構成ファイルを生成する必要があります。



(注) 新しい PSN を追加するたびに新しい RSA 構成が生成されないようにするには、バックアップおよび復元プロセスを開始する前に、展開に追加するすべてのノードの IP アドレスを知っておく必要があります。次に、すべての IP アドレスを使用して RSA 構成ファイルを生成し、PANUI にアップロードする必要があります。

手順

1. RSA Authentication Manager セキュリティコンソールのプライマリインスタンスで、展開に含まれていないノードを含むすべてのノードのすべての IP アドレスを使用して、Authentication Manager 構成ファイルを生成します。
2. 新しい構成ファイルを PAN UI にインポートします。



(注) 新しい RSA 構成ファイルをアップロードする前に、RSA Authentication Manager のノード秘密をクリアする必要があります。これは、新しいノード秘密を作成し、それを ISE と RSA Authentication Manager の間で共有するのに役立ちます。

これで、インポートされた構成ファイルにすでに存在する IP アドレスを使用して構成の一部として複製されるため、新しい構成ファイルを生成せずに新しいノードを展開に追加できます。

次に、バックアップと復元によるアップグレード方法で実行する手順の概要を示します。

1. ノードの登録解除

展開からノードを削除するには、ノードの登録を解除する必要があります。ノードの登録解除または削除の詳細については、『[Cisco Identity Services Engine 管理者ガイド](#)』の「展開からのノードの削除」のセクションを参照してください。

2. ノードの再イメージ化

Cisco ISE ノードを再イメージ化するには、最初に展開からノードを削除してから、Cisco ISE のインストールに進む必要があります。Cisco ISE のインストール方法の詳細については、『[Cisco Identity Services Engine インストールガイド](#)』の「Cisco ISE のインストール」の章を参照してください。

新しくインストールされた Cisco ISE リリースの最新のパッチを適用することを推奨します。

3. 設定または運用データベースのバックアップと復元

バックアップと復元操作の詳細については、『[Cisco Identity Services Engine 管理者ガイド](#)』の「バックアップ/復元操作」のセクションを参照してください。

4. ノードへのプライマリまたはセカンダリロールの割り当て

必要に応じて、ノードにプライマリまたはセカンダリのロールを割り当てることができます。モニタリングとトラブルシューティング (MnT) ノードにロールを割り当て方法の詳細については、『[Cisco Identity Services Engine 管理者ガイド](#)』の「MnT ロールの手動変更」のセクションを参照してください。

5. ポリシーサービスノードの参加

新しい展開にポリシーサービスノード (PSN) を参加させるには、ノードを PSN として登録する必要があります。PSN の登録または参加の詳細については、『[Cisco Identity Services Engine 管理者ガイド](#)』の「セカンダリ Cisco ISE ノードの登録」を参照してください。

6. 証明書のインポート

Cisco ISE で新しく展開されたノードにシステム証明書をインポートする必要があります。システム証明書を Cisco ISE ノードにインポートする方法の詳細については、『[Cisco Identity Services Engine 管理者ガイド](#)』の「システム証明書のインポート」セクションを参照してください。

バックアップと復元によるアップグレードプロセス

ここでは、推奨のバックアップと復元によるアップグレード方法を使用したアップグレードプロセスについて説明します。

現在 Cisco ISE リリース 2.1 以降を使用している場合は、Cisco ISE リリース 2.6 に直接アップグレードできます。

- セカンダリ PAN および MnT ノードの Cisco ISE リリース 2.6 へのアップグレード
- ポリシーサービスノードの Cisco ISE リリース 2.6 への参加
- プライマリ PAN および MnT の Cisco ISE リリース 2.6 へのアップグレード

Cisco ISE リリース 2.6 と互換性がない Cisco ISE バージョンを使用している場合は、最初に Cisco ISE リリース 2.6 と互換性のある中間バージョンにアップグレードする必要があります。その後、中間バージョンから Cisco ISE リリース 2.6 にアップグレードできます。Cisco ISE の中間バージョンにアップグレードするには、次の手順に従います。

セカンダリ PAN およびセカンダリ MnT ノードを、Cisco ISE リリース 2.1、2.2、2.3 または 2.4 にアップグレードします。

始める前に

既存の Cisco ISE からのバックアップを Cisco ISE 中間リリースに復元します。

-
- ステップ 1** セカンダリ PAN ノードを登録解除します。
 - ステップ 2** 登録解除されたセカンダリ PAN ノードを、スタンドアロンノードとして、Cisco ISE 中間リリースに再イメージ化します。アップグレード後に、このノードを新しい展開でプライマリ管理ノードにします。
 - ステップ 3** バックアップデータから Cisco ISE の設定を復元します。
 - ステップ 4** セカンダリ MnT ノードを登録解除します。
 - ステップ 5** 登録解除されたセカンダリ MnT ノードを、スタンドアロンノードとして、Cisco ISE の中間リリースに再イメージ化します。
 - ステップ 6** この MnT ノードにプライマリロールを割り当て、バックアップリポジトリから運用バックアップを復元します。これは省略可能な手順であり、古いログを報告する必要がある場合にのみ実行する必要があります。
 - ステップ 7** 元の Cisco ISE バックアップリポジトリから ise-https-admin CA 証明書をインポートします。
-

セカンダリ PAN および MnT ノードの Cisco ISE リリース 2.6 へのアップグレード

-
- ステップ 1** Cisco ISE の構成設定と運用ログのバックアップを作成します。
 - ステップ 2** セカンダリ PAN ノードを登録解除します。
 - ステップ 3** 登録解除されたセカンダリ PAN ノードを Cisco ISE リリース 2.6 に再イメージ化します。

- ステップ4 バックアップデータから ISE 設定を復元し、このノードを新しい展開のプライマリノードとして設定します。
- ステップ5 ワイルドカード証明書を使用していない場合は、このノードのバックアップから ise-https-admin CA 証明書をインポートします。
- ステップ6 セカンダリ MnT ノードを登録解除します。
- ステップ7 登録解除されたセカンダリ MnT ノードを Cisco ISE リリース 2.6 に再イメージ化します。
- ステップ8 現在の ISE 運用バックアップを復元し、新しい展開環境のプライマリ MnT としてノードを参加させます。これは省略可能な手順であり、古いログを報告する必要がある場合にのみ実行する必要があります。

ポリシーサービスノードの Cisco ISE リリース 2.6 への参加

Cisco ISE ノードが複数のサイトに展開されている場合は、最初に（セカンダリ PAN および MnT ノードを含む）サイトに使用可能な PSN を参加させてから、他のサイトに使用可能な PSN を参加させ、その後（既存の Cisco ISE のプライマリ PAN および MnT ノードを含む）サイトに使用可能な PSN を参加させます。

-
- ステップ1 PSN を登録解除します。
 - ステップ2 PSN を Cisco ISE リリース 2.6 の最新パッチに再イメージ化し、新しい Cisco ISE リリース 2.6 展開環境に参加させます。

次のタスク

この時点で、部分的にアップグレードされた展開環境をテストすることをお勧めします。これを行うには、ログが存在するかどうかを確認し、アップグレードされたノードが通常どおり機能していることを確認します。

プライマリ PAN および MnT の Cisco ISE リリース 2.6 へのアップグレード

-
- ステップ1 プライマリ MnT ノードを再イメージ化し、セカンダリ MnT として新しい展開環境に参加させます。レポート用のデータを保持する場合は、運用バックアップのコピーをセカンダリ MnT ノードに復元します。
 - ステップ2 プライマリ PAN ノードを再イメージ化し、セカンダリ PAN として新しい展開環境に参加させます。
-

GUI からの Cisco ISE 展開のアップグレード

GUI からの Cisco ISE 展開のアップグレード

Cisco ISE では、管理者ポータルから GUI ベースの一元化されたアップグレードが提供されます。アップグレードプロセスは大幅に簡素化され、アップグレードの進行状況およびノードのステータスが画面に表示されます。

[管理 (Administration)] > [システム (System)] > [アップグレード (Upgrade)] > [概要 (Overview)] メニューオプションを選択すると、展開内のすべてのノード、そのノードで有効なペルソナ、インストールされている ISE のバージョン、およびノードのステータス（ノードがアクティブか非アクティブか）がリストされます。ノードがアクティブな状態である場合にのみアップグレードを開始できます。

管理者用ポータルからの GUI ベースのアップグレードは、現在リリース 2.0 以降で、リリース 2.0.1 以上にアップグレードする場合にのみサポートされます。

リリース 2.1、2.2、2.3、または 2.4 からリリース 2.6 へのアップグレード

始める前に

の項の手順を必ず読んでください。

-
- ステップ 1** 管理者ポータルの [アップグレード (Upgrade)] タブをクリックします。
- ステップ 2**
- ステップ 3** [続行 (Proceed)] をクリックします。
- ステップ 4** [レビューチェックリスト (Review Checklist)] ウィンドウが表示されます。表示された手順を確認してください。
- ステップ 5** [チェックリストを確認済み (I have reviewed the checklist)] チェックボックスをオンにし、[続行 (Continue)] をクリックします。
- [バンドルをノードにダウンロードする (Download Bundle to Nodes)] ウィンドウが表示されます。
- ステップ 6** リポジトリからノードにアップグレードバンドルをダウンロードします。
- アップグレードバンドルをダウンロードするノードの隣のチェックボックスをオンにします。
 - [ダウンロード (Download)] をクリックします。
- [リポジトリおよびバンドルの選択 (Select Repository and Bundle)] ウィンドウが表示されます。
- リポジトリを選択します。

異なるノードで同じリポジトリまたは異なるリポジトリを選択できますが、すべてのノードで同じアップグレードバンドルを選択する必要があります。

- d) アップグレードに使用するバンドルの隣にあるチェックボックスをオンにします。
- e) [確認 (Confirm)] をクリックします。

バンドルがノードにダウンロードされると、ノードステータスが [アップグレードの準備が整いました (Ready for Upgrade)] に変わります。

ステップ 7 [続行 (Continue)] をクリックします。

[ノードのアップグレード (Upgrade Nodes)] ウィンドウが表示されます。

ステップ 8 アップグレード順序を選択します。

ノードを新しい展開に移動すると、アップグレードの推定所要時間が [ノードのアップグレード (Upgrade Nodes)] ウィンドウに表示されます。この情報を使用して、アップグレードを計画し、ダウンタイムを最小化できます。管理ノードとモニターリングノードのペアおよび複数のポリシーサービスノードがある場合は、以下の手順に従います。

- a) デフォルトでは、セカンダリ管理ノードは、アップグレード順序の最初にリストされています。アップグレード後に、このノードは新しい展開でプライマリ管理ノードになります。
- b) プライマリモニターリングノードは、次に新しい展開にアップグレードされるノードです。
- c) ポリシーサービスノードを選択し、新しい展開に移動します。ポリシーサービスノードをアップグレードする順序を変更できます。

ポリシーサービスノードは、順番にまたは並行してアップグレードできます。ポリシーサービスノードのセットを選択し、並行してアップグレードできます。

- d) セカンダリモニターリングノードを選択し、新しい展開に移動します。
- e) 最後に、プライマリ管理ノードを選択し、新しい展開に移動します。

ステップ 9 アップグレードがアップグレード順序のいずれかのポリシーサービスノードで失敗した場合でもアップグレードを続行するには、[失敗時でもアップグレードを続行する (Continue with upgrade on failure)] チェックボックスをオンにします。

このオプションは、セカンダリ管理ノードおよびプライマリモニターリングノードには適用されません。これらのノードのいずれかに障害が発生すると、アップグレードプロセスはロールバックされます。ポリシーサービスノードのいずれかが失敗すると、セカンダリモニターリングノードおよびプライマリ管理ノードはアップグレードされず、古い展開内に残ります。

ステップ 10 [アップグレード (Upgrade)] をクリックして、展開のアップグレードを開始します。

各ノードのアップグレードの進行状況が表示されます。正常に完了すると、ノードのステータスが [アップグレード完了 (Upgrade Complete)] に変わります。

(注) 管理者ポータルからノードをアップグレードするときに、ステータスが長時間変化しない場合 (80% のままの場合) は、CLI からアップグレードログをチェックするか、コンソールからアップグレードのステータスをチェックできます。アップグレードの進行状況を表示するには、CLI にログインするか、Cisco ISE ノードのコンソールを表示します。 **show logging application** コマンドを使用すると、*upgrade-uibackend-cliconsole.log* および *upgrade-postosupgrade-yyyyymmdd-xxxxxx.log* を表示できます。

show logging application コマンドを使用すると、CLI から次のアップグレードログを表示できます。

- DB データのアップグレードログ
- DB スキーマログ
- Post OS アップグレードログ

警告メッセージ「**The node has been reverted back to its pre-upgrade state**」が表示された場合は、[アップグレード (Upgrade)] ウィンドウに移動し、[詳細 (Details)] リンクをクリックします。[アップグレードの失敗の詳細 (Upgrade Failure Details)] ウィンドウに記載されている問題を解決します。すべての問題を解決した後、[アップグレード (Upgrade)] をクリックして、アップグレードを再起動します。

(注) 新しい展開のプライマリ管理ノードでポスチャデータの更新処理が実行している場合、プライマリ管理ノードにノードを登録できません。ポスチャ更新プロセスが終了するまで待つ (約20分かかることがあります)、またはアップグレード中またはノードの新しい展開への登録中に、[更新 (Updates)] ウィンドウから、ポスチャの自動更新機能を無効化できます。このウィンドウへのナビゲーションパスは、[管理 (Administration)] > [システム (System)] > [設定 (Settings)] > [ポスチャ (Posture)] > [更新 (Updates)] です。

CLI からの Cisco ISE 展開のアップグレード

CLI を使用したアップグレードプロセスは、展開タイプによって異なります。

スタンドアロンノードのアップグレード

application upgrade <upgrade bundle name> <repository name> コマンドを直接使用したり、**application upgrade prepare <upgrade bundle name> <repository name>** および **application upgrade proceed** コマンドを指定された順番に使用してスタンドアロンノードをアップグレードすることもできます。

管理、ポリシーサービス、pxGrid、およびモニターリングのペルソナを担当するスタンドアロンノードの CLI から **application upgrade <upgrade bundle name> <repository name>** コマンドを実行できます。このコマンドを直接実行する場合は、コマンドを実行する前にリモートリポジトリから Cisco ISE ノードのローカルディスクにアップグレードバンドルをコピーして、アップグレードの時間を短縮することを推奨します。

代わりに、**application upgrade prepare <upgrade bundle name> <repository name>** コマンドと **application upgrade proceed** コマンドを使用することもできます。**application upgrade prepare <upgrade bundle name> <repository name>** コマンドを使用すると、アップグレードバンドルがダウンロードされ、ローカルに抽出されます。このコマンドはリモートリポジトリから Cisco ISE ノードのローカルディスクにアップグレードバンドルをコピーします。ノードをアップグレードする準備ができたなら、**application upgrade proceed** コマンドを実行してアップグレードを正常に完了します。

以下で説明する **application upgrade prepare <upgrade bundle name> <repository name>** および **application upgrade proceed** コマンドを実行することをお勧めします。

始める前に

の項の手順を必ず読んでください。

ステップ 1 ローカルディスクのリポジトリを作成します。たとえば、「upgrade」というリポジトリを作成できます。

例：

```
ise/admin# conf t
Enter configuration commands, one per line. End with CNTL/Z.
ise/admin(config)# repository upgrade
ise/admin(config-Repository)# url disk:
% Warning: Repositories configured from CLI cannot be used from the ISE web UI and are not replicated
to other ISE nodes.
If this repository is not created in the ISE web UI, it will be deleted when ISE services restart.
ise/admin(config-Repository)# exit
ise/admin(config)# exit
```

ステップ 2 Cisco ISE コマンドライン インターフェイス (CLI) から、**application upgrade prepare <upgrade bundle name> <repository name>** コマンドを入力します。

このコマンドは、アップグレードバンドルを前の手順で作成したローカルリポジトリ「upgrade」にコピーし、MD5 と SHA256 チェックサムを一覧表示します。

ステップ 3 (注) アップグレード後、SSH 経由でログインし、**show application status ise** コマンドを使用することで、アップグレードの進行状況を表示できます。次のメッセージが表示されます。「%NOTICE: Identity Services Engine upgrade is in progress...」

Cisco ISE CLI から、**application upgrade proceed** コマンドを入力します。

次のタスク

[アップグレードプロセスの確認 \(41 ページ\)](#)

2 ノード展開のアップグレード

application upgrade prepare <upgrade bundle name> <repository name> コマンドおよび **proceed** コマンドを使用して、2 ノード展開をアップグレードします。手動でノードの登録を解除して、

再登録する必要はありません。アップグレードソフトウェアは自動的にノードを登録解除し、新しい展開に移行します。2ノード展開をアップグレードする場合、最初にセカンダリ管理ノード（ノードB）だけをアップグレードする必要があります。セカンダリノードのアップグレードを完了したら、プライマリノード（ノードA）をアップグレードします。次の図に示すような展開の設定の場合、このアップグレード手順を続けることができます。

始める前に

- プライマリ管理ノードから設定および運用データのオンデマンドバックアップを手動で実行します。
- 管理とモニターリングのペルソナが、展開の両方のノードでイネーブルにされていることを確認します。

管理ペルソナがプライマリ管理ノードでのみイネーブルである場合、アップグレードプロセスによりセカンダリ管理ノードを最初にアップグレードすることが求められるので、セカンダリノードの管理ペルソナをイネーブルにします。

または、2ノード展開で1つの管理ノードのみがある場合は、セカンダリノードの登録を解除します。両方のノードがスタンドアロンノードになります。両方のノードをスタンドアロンノードとしてアップグレードし、アップグレード後に、展開をセットアップします。

- モニターリングペルソナが1つのノードのみでイネーブルの場合、次に進む前に他のノードのモニターリングペルソナをイネーブルにします。

ステップ1 CLIからセカンダリノード（ノードB）をアップグレードします。

アップグレードプロセスで、自動的にノードBが展開から削除され、アップグレードされます。ノードBは再起動すると、プライマリノードにアップグレードされます。

ステップ2 アップグレードノードA。

アップグレードプロセスで、自動的にノードAが展開に登録され、アップグレードされた環境でセカンダリノードになります。

ステップ3 新規の展開で、ノードAをプライマリノードに昇格させます。

アップグレードが完了した後、ノードに古いモニターリングログが含まれる場合、これらのノード上で **application configure ise** コマンドを実行し、5（データベースの統計情報の更新）を選択します。

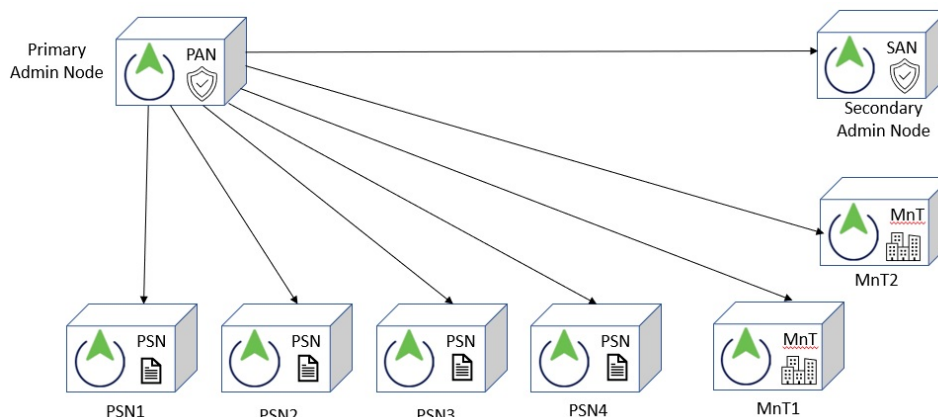
次のタスク

[アップグレードプロセスの確認（41 ページ）](#)

分散展開のアップグレード

初めに、セカンダリ管理ノード (SAN) を新しいリリースにアップグレードします。たとえば、次の図に示すように、1つのプライマリ管理ノード (PAN)、1つのセカンダリ管理ノード、4つのポリシーサービスノード (PSN)、1つのプライマリ モニターリング ノード (MnT1)、および1つのセカンダリモニターリングノード (MnT2) を含む展開がセットアップされている場合、次のアップグレード手順に進むことができます。

図 1: アップグレード前の Cisco ISE 展開



(注) アップグレードの前にノードを手動で登録解除しないでください。 **application upgrade prepare <upgrade bundle name> <repository name>** コマンドおよび **proceed** コマンドを使用して、新しいリリースにアップグレードします。アップグレードプロセスは自動的にノードを登録解除し、新しい展開に移行します。アップグレードの前に手動でノードの登録をキャンセルする場合は、アップグレードプロセスを開始する前に、プライマリ管理ノードのライセンスファイルがあることを確認します。手元にこのファイルがない場合（たとえば、シスコパートナーベンダーによってライセンスがインストールされた場合）、Cisco Technical Assistance Center に連絡してください。

始める前に

- 展開にセカンダリ管理ノードがない場合は、アップグレードプロセスを開始する前に、セカンダリ管理ノードにするポリシーサービスノードを1つ設定します。
- の項の手順を必ず読み、従ってください。
- 全 Cisco ISE 展開をアップグレードする場合は、ドメインネームシステム (DNS) のサーバー解決 (順ルックアップおよび逆ルックアップ) が必須です。そうでない場合、アップグレードは失敗します。

ステップ 1 CLI から SAN をアップグレードします。

アップグレードプロセスで、自動的にSANが展開から登録解除され、アップグレードされます。再起動すると、SANが新規展開のプライマリノードになります。各展開でモニターリングノードが少なくとも1つ必要になるため、アップグレードプロセスは古い展開の該当ノードで有効になっていなくても、SANのモニターリングペルソナを有効にします。ポリシーサービスペルソナが古い展開のSANで有効であった場合、この設定は新規展開へのアップグレード後も維持されます。

ステップ2 モニターリングノードの1つ（MnT1とMnT2）を新規展開にアップグレードします。

セカンダリモニターリングノードの前にプライマリモニターリングノードをアップグレードすることをお勧めします（古い展開でプライマリ管理ノードがプライマリモニターリングノードとしても動作している場合にはこれは不可能です）。プライマリモニターリングノードが起動し、新規展開からログを収集します。この詳細は、プライマリ管理ノードのダッシュボードから表示できます。

古い展開でモニターリングノードが1つだけある場合は、アップグレードする前に、古い展開のプライマリ管理ノードであるPANのモニターリングペルソナを有効にします。ノードペルソナの変更により、Cisco ISEアプリケーションが再起動します。PANが再起動するまで待ちます。新規展開にモニターリングノードをアップグレードすると、運用データを新しい展開に移行する必要があるために、他のノードよりも時間がかかります。

新規展開のプライマリ管理ノードであるノードBが、古い展開でイネーブルにされたモニターリングペルソナを持たない場合、モニターリングペルソナをディセーブルにします。ノードペルソナの変更により、Cisco ISEアプリケーションが再起動します。プライマリ管理ノードが起動するまで待ちます。

ステップ3 次に、ポリシーサービスマード（PSN）をアップグレードします。複数のPSNを同時にアップグレードできますが、すべてのPSNを同時にアップグレードした場合、ネットワークでダウンタイムが発生します。

アップグレード後に、新規展開SANのプライマリノードにPSNが登録され、プライマリノードからのデータがすべてのPSNに複製されます。PSNではそのペルソナ、ノードグループ情報、およびプローブのプロファイリング設定が維持されます。

ステップ4 古い展開に2番目のモニターリングノードがある場合、次のことを行う必要があります。

a) 古い展開のプライマリノードであるPANのモニターリングペルソナを有効にします。

展開でモニターリングノードは少なくとも1つ必要です。古い展開から第2のモニターリングノードをアップグレードする前に、プライマリノード自身でこのペルソナをイネーブルにします。ノードペルソナの変更により、Cisco ISEアプリケーションが再起動します。プライマリISEノードが再起動するまで待ちます。

b) セカンダリモニターリングノードを古い展開から新規展開にアップグレードします。

プライマリ管理ノードを除いて、他のすべてのノードが新規展開にアップグレードされている必要があります。

ステップ5 最後に、プライマリ管理ノードをアップグレードします。

このノードは、セカンダリ管理ノードとしてアップグレードされ、新規展開に追加されます。セカンダリ管理ノードを新規展開のプライマリノードに昇格させることができます。

アップグレードが完了した後、アップグレードされたモニターリングノードに古いログが含まれる場合、**application configure ise** コマンドを実行し、該当するモニターリングノードで 5（データベースの統計情報の更新）を選択します。

次のタスク

[アップグレードプロセスの確認 \(41 ページ\)](#)

アップグレードプロセスの確認

展開が期待どおりに機能すること、およびユーザーが認証されネットワークのリソースにアクセスできることを確認するためのネットワークテストを実行することを推奨します。

構成データベースの問題でアップグレードが失敗すると、変更された内容が自動的にロールバックされます。

アップグレードが正常に完了したかどうかを確認するには、次のいずれかのオプションを実行します。

- **ade.log** ファイルでアップグレードプロセスを確認します。**ade.log** ファイルを表示するには、Cisco ISE CLI から次のコマンドを入力します：**show logging system ade/ADE.log?**

STEP の **grep** でアップグレードの進行状況を表示できます。

- info:[application:install:upgrade:preinstall.sh] STEP 0: Running pre-checks
- info:[application:operation:preinstall.sh] STEP 1: Stopping ISE application...
- info:[application:operation:preinstall.sh] STEP 2: Verifying files in bundle...
- info:[application:operation:isedbupgrade-newmodel.sh] STEP 3: Validating data before upgrade...
- info:[application:operation:isedbupgrade-newmodel.sh] STEP 4: De-registering node from current deployment.
- info:[application:operation:isedbupgrade-newmodel.sh] STEP 5: Taking backup of the configuration data...
- info:[application:operation:isedbupgrade-newmodel.sh] STEP 6: Registering this node to primary of new deployment...
- info:[application:operation:isedbupgrade-newmodel.sh] STEP 7: Downloading configuration data from primary of new deployment...
- info:[application:operation:isedbupgrade-newmodel.sh] STEP 8: Importing configuration data...
- info:[application:operation:isedbupgrade-newmodel.sh] STEP 9: Running ISE configuration data upgrade for node specific data...
- info:[application:operation:isedbupgrade-newmodel.sh] STEP 10: Running ISE M&T database upgrade...
- info:[application:install:upgrade:post-osupgrade.sh] POST ADEOS UPGRADE STEP 1: Upgrading Identity Services Engine software...
- info:[application:operation:post-osupgrade.sh] POST ADEOS UPGRADE STEP 2: Importing upgraded data to 64 bit database...

- この文字列を検索して、アップグレードが成功したことを確認します。

```
Upgrade of Identity Services Engine completed  
successfully.
```

- **show version** コマンドを実行し、ビルドバージョンを検証します。
- **show application status ise** コマンドを入力して、すべてのサービスが実行されていることを確認します。

以前のバージョンへのロールバック

まれに、以前のバージョンの ISO イメージを使用し、バックアップファイルからデータを復元することで、Cisco ISE アプライアンスのイメージを再作成する必要がある場合があります。データを復元した後は、古い展開を登録して、古い展開で行ったようにペルソナを有効にすることができます。したがって、アップグレードプロセスを開始する前に、Cisco ISE 設定およびモニターリングデータをバックアップすることをお勧めします。

設定およびモニターリングデータベースの問題により発生したアップグレードの障害は、自動的にロールバックされないことがあります。これが発生すると、データベースがロールバックされないことを示す通知を、アップグレードの失敗メッセージと共に受け取ります。このようなシナリオでは、手動でシステムのイメージを再作成し、Cisco ISE をインストールして、設定およびモニターリングデータを復元（モニターリングペルソナが有効な場合）する必要があります。

ロールバックまたは回復を行う前に、**backup-logs** コマンドを使用してサポートバンドルを生成し、そのサポートバンドルをリモートリポジトリに配置します。



第 4 章

Cisco ISE ソフトウェアパッチ

Cisco ISE ソフトウェアのパッチは常に累積されます。Cisco ISE では、パッチのインストールおよびロールバックを CLI または GUI から実行できます。

展開内の Cisco ISE サーバーにパッチをインストールする作業は、プライマリ PAN から行うことができます。プライマリ PAN からパッチをインストールするには、Cisco.com からクライアントブラウザを実行しているシステムにパッチをダウンロードします。

GUI からパッチをインストールする場合、パッチは最初にプライマリ PAN に自動的にインストールされます。その後、システムは、GUI にリストされている順序で、展開内の他のノードにパッチをインストールします。ノードが更新される順序を制御することはできません。パッチバージョンを手動でインストール、ロールバック、および表示することもできます。これを行うには、GUI で [管理者 (Administrator)] > [システム (System)] > [メンテナンス (Maintenance)] > [パッチ管理 (Patch management)] ウィンドウを選択します。

CLI からパッチをインストールする場合は、ノードの更新順序を制御できます。ただし、最初にプライマリ PAN にパッチをインストールすることを推奨します。残りのノードでのインストールの順序は関係ありません。プロセスを高速化するために、パッチを複数のノードに同時にインストールできます。

展開全体をアップグレードする前にいくつかのノードでパッチを検証する場合、CLI を使用すると、選択したノードでパッチをインストールできます。パッチをインストールするには、次の CLI コマンドを使用します。

```
patch install <patch_bundle> <repository_that_stores_patch_file>
```

詳細については、『Cisco Identity Services Engine CLI リファレンスガイド』の「EXEC モードの Cisco ISE CLI コマンド」の章にある「patch install」の項を参照してください。

必要なパッチバージョンを直接インストールすることができます。たとえば、Cisco ISE 2.x を使用していて、Cisco ISE 2.x パッチ 5 をインストールする場合、以前のパッチ (Cisco ISE 2.x パッチ 1 ~ 4 など) をインストールしなくても、Cisco ISE 2.x パッチ 5 を直接インストールできます。CLI でパッチバージョンを表示するには、次の CLI コマンドを使用します。

```
show version
```

- [ソフトウェアパッチインストールのガイドライン \(44 ページ\)](#)
- [ソフトウェアパッチのインストール \(44 ページ\)](#)
- [ソフトウェアパッチのロールバック \(45 ページ\)](#)

- [パッチのインストールおよびロールバックの変更の表示 \(46 ページ\)](#)

ソフトウェアパッチインストールのガイドライン

ISE ノードにパッチをインストールすると、インストールの完了後にノードが再起動されます。再びログインできる状態になるまで、数分かかることがあります。メンテナンスウィンドウ中にパッチをインストールするようにスケジュール設定し、一時的な機能停止を回避することができます。

インストールするパッチが、ネットワーク内に展開されている Cisco ISE のバージョンに適用されるものであることを確認してください。Cisco ISE はパッチファイルのバージョンの不一致とあらゆるエラーをレポートします。

Cisco ISE に現在インストールされているパッチよりも低いバージョンのパッチをインストールできません。同様に、あるバージョンのパッチの変更をロールバックしようとしたときに、それよりも高いバージョンのパッチがその時点で Cisco ISE にインストール済みの場合は、ロールバックはできません。たとえば、パッチ 3 が Cisco ISE サーバーにインストール済みの場合に、パッチ 1 または 2 をインストールしたり、パッチ 1 または 2 にロールバックすることはできません。

分散展開の一部であるプライマリ PAN からパッチのインストールを実行するときは、Cisco ISE によってそのパッチが展開内のプライマリノードとすべてのセカンダリノードにインストールされます。パッチのインストールがプライマリ PAN で成功すると、Cisco ISE はセカンダリノードでパッチのインストールを続行します。プライマリ PAN で失敗した場合は、インストールはセカンダリノードに進みません。ただし、何らかの理由でセカンダリノードのいずれかでインストールに失敗した場合は、処理が続行され、展開内の次のセカンダリノードでインストールが実行されます。

2 ノード展開の一部であるプライマリ PAN からパッチのインストールを実行するときは、Cisco によってそのパッチが展開内のプライマリノードとセカンダリノードにインストールされます。パッチのインストールがプライマリ PAN で成功すると、Cisco はセカンダリノードでパッチのインストールを続行します。プライマリ PAN で失敗した場合は、インストールはセカンダリノードに進みません。

ソフトウェアパッチのインストール

始める前に

- スーパー管理者またはシステム管理者の管理者ロールが割り当てられている必要があります。
- [管理 (Administration)] > [システム (System)] > [展開 (Deployment)] > [PAN のフェールオーバー (PAN Failover)] に移動し、[PAN の自動フェールオーバーを有効にする (Enable PAN Auto Failover)] チェックボックスがオフになっていることを確認します。このタスクの期間中は、PAN の自動フェールオーバー設定を無効にする必要があります。

ステップ 1 [管理 (Administration)] > [システム (System)] > [メンテナンス (Maintenance)] > [パッチ管理 (Patch Management)] > [インストール (Install)] を選択します。

ステップ 2 [参照 (Browse)] をクリックし、Cisco.com からダウンロードしたパッチを選択します。

ステップ 3 [インストール (Install)] をクリックしてパッチをインストールします。

PANでのパッチのインストールが完了すると、Cisco ISEから自動的にログアウトされます。再びログインできるようになるまで数分間待つ必要があります。

(注) パッチインストールの進行中は、[パッチ管理 (Patch Management)] ページ上の機能のうち、アクセスできるのは **Show Node Status** のみです。

ステップ 4 インストールしたパッチの横のオプションボタンをクリックし、[ノードステータスを表示 (Show Node Status)] をクリックしてインストールが完了したことを確認します。

ソフトウェアパッチのロールバック

複数のノードの展開の一部である PAN からパッチのロールバックを実行するときは、Cisco ISEによってそのパッチが展開内のプライマリノードとすべてのセカンダリノードにロールバックされます。

始める前に

- スーパー管理者またはシステム管理者の管理者ロールが割り当てられている必要があります。

ステップ 1 [管理 (Administration)] > [システム (System)] > [メンテナンス (Maintenance)] > [パッチ管理 (Patch Management)] を選択します。

ステップ 2 変更をロールバックするパッチバージョンのオプションボタンをクリックしてから、[ロールバック (Rollback)] をクリックします。

(注) パッチのロールバックの進行中は、[パッチ管理 (Patch Management)] ページ上の機能のうち、アクセスできるのは **Show Node Status** のみです。

PANからのパッチのロールバックが完了すると、Cisco ISEから自動的にログアウトされます。再びログインできるようになるまで数分間待つ必要があります。

ステップ 3 ログイン後に、ページの一番下にある [アラーム (Alarms)] リンクをクリックしてロールバック操作のステータスを表示します。

ステップ 4 パッチのロールバックの進行状況を表示するには、[パッチ管理 (Patch Management)] ページでパッチを選択し、[ノードステータスを表示 (Show Node Status)] をクリックします。

ステップ 5 パッチのオプションボタンをクリックし、セカンダリノード上で[ノードステータスを表示 (Show Node Status)] をクリックして、そのパッチが展開内のすべてのノードからロールバックされたことを確認します。

そのパッチがロールバックされていないセカンダリノードがある場合は、そのノードが稼働中であることを確認してから、プロセスをもう一度実行して残りのノードから変更をロールバックしてください。Cisco ISE は、このバージョンのパッチがインストールされているノードからのみパッチをロールバックします。

ソフトウェアパッチ ロールバックのガイドライン

展開の Cisco ISE ノードからパッチをロールバックするには、最初に PAN から変更をロールバックします。これに成功すると、セカンダリノードからパッチがロールバックされます。PAN でロールバックプロセスが失敗した場合は、セカンダリノードからのパッチロールバックは行われません。ただし、いずれかのセカンダリノードでパッチのロールバックが失敗しても、展開内の次のセカンダリノードからのパッチのロールバックは継続されます。

Cisco ISE によるセカンダリノードからのパッチロールバックが進行中のときも、引き続き PAN GUI から他のタスクを実行できます。セカンダリノードは、ロールバック後に再起動されます。

パッチのインストールおよびロールバックの変更の表示

インストールされているパッチに関連するレポートを表示するには、次の手順を実行します。

始める前に

スーパー管理者またはシステム管理者の管理者ロールが割り当てられている必要があります。パッチをインストールまたはロールバックするには、[管理 (Administration)] > [システム (System)] > [メンテナンス (Maintenance)] > [パッチ管理 (Patch Management)] ページを選択します。展開内の各ノードで特定のパッチのステータス ([インストール済み (installed)]、[処理中 (in-progress)]、[未インストール (not installed)]) を確認できます。このためには、特定のパッチを選択し、[ノードステータスを表示 (Show Node Status)] ボタンをクリックします。

ステップ 1 [操作 (Operations)] > [レポート (Reports)] > [監査 (Audit)] > [操作監査 (Operations Audit)] を選択します。デフォルトでは、過去 7 日間のレコードが表示されます。

ステップ 2 [フィルタ (Filter)] ドロップダウンをクリックして[クイックフィルタ (Quick Filter)] または[高度なフィルタ (Advanced Filter)] を選択し、必要なキーワード (例: patch install initiated) を使用して、インストール済みのパッチを示すレポートを生成します。



第 5 章

アップグレード後の設定と構成

Cisco ISE のアップグレード後に、次のタスクを実行します。

- 仮想マシンの設定の確認 (47 ページ)
- ポートが開いていることの確認 (48 ページ)
- ブラウザのセットアップ (48 ページ)
- Active Directory の再結合 (48 ページ)
- 逆引き DNS ルックアップ (50 ページ)
- 証明書の復元 (50 ページ)
- ルート CA チェーンの再生成 (51 ページ)
- 脅威中心型 NAC (52 ページ)
- SNMP 送信元ポリシーサービスノード設定 (52 ページ)
- プロファイラ フィールド サービス (52 ページ)
- クライアントプロビジョニング (52 ページ)
- 暗号スイート (53 ページ)
- モニタリングおよびトラブルシューティング (54 ページ)
- Trustsec NAD に対するポリシーの更新 (54 ページ)
- サプリカントプロビジョニング ウィザードの更新 (54 ページ)

仮想マシンの設定の確認

仮想マシンの Cisco ISE ノードをアップグレードする場合は、Red Hat Enterprise Linux (RHEL) 7 (64 ビット) または Red Hat Enterprise Linux (RHEL) 6 (64 ビット) にゲストオペレーティングシステムを変更してあることを確認します。これを行うには、VM の電源をオフにし、サポートされる RHEL バージョンにゲストオペレーティングシステムを変更し、変更後に VM の電源をオンにする必要があります。

RHEL 7 は E1000 および VMXNET3 ネットワークアダプタのみをサポートします。アップグレードする前に、ネットワークアダプタのタイプを変更する必要があります。

ESXi 5.x サーバー (5.1 U2 以上) で ISE を実行する場合は、RHEL 7 をゲスト OS として選択する前に、VMware ハードウェアバージョンを 9 にアップグレードする必要があります。

ポートが開いていることの確認

バージョン 2.6 より前のリリースからアップグレードする場合は、Cisco ISE リリース 2.6 のリリースノートを参照してください。

https://www.cisco.com/c/en/us/td/docs/security/ise/2-6/release_notes/b_ise_26_RN.html

注意すべき重要な変更点の 1 つは、ISE メッセージキューで、すべての Cisco ISE ノード間でポート 8671 のオープンが要求されることです。

ブラウザのセットアップ

アップグレード後、Cisco ISE 管理者用ポータルにアクセスする前に、ブラウザのキャッシュをクリアしていることを確認し、ブラウザを閉じて、新しいブラウザセッションを開きます。また、リリースノートに記載されているサポート対象のブラウザを使用していることを確認します。 <https://www.cisco.com/c/en/us/support/security/identity-services-engine/products-release-notes-list.html>

Active Directory の再結合

外部アイデンティティソースとして使用している Active Directory との接続が失われた場合は、Active Directory とすべての Cisco ISE ノードを再度結合する必要があります。結合が完了した後には、外部アイデンティティソースのコールフローを実行して、確実に接続します。

- アップグレード後に、Active Directory 管理者アカウントを使用して Cisco ISE ユーザーインターフェイスにログインした場合、アップグレード時に Active Directory の結合が失われるため、ログインが失敗します。Cisco ISE にログインし、Active Directory と結合するには、内部管理者アカウントを使用する必要があります。
- Cisco ISE への管理アクセスに対して証明書ベースの認証を有効にしている、Active Directory をアイデンティティソースとして使用している場合、アップグレード後に ISE ログインページを起動できません。これは、アップグレード中に Active Directory との結合が失われるためです。Active Directory との結合を復元するには、Cisco ISE CLI に接続し、次のコマンドを使用してセーフモードで ISE アプリケーションを開始します。

application start ise safe

Cisco ISE がセーフモードで起動したら、次のタスクを実行します。

- 内部管理者アカウントを使用して Cisco ISE ユーザーインターフェイスにログインします。
パスワードを忘れた場合または管理者アカウントがロックされている場合は、管理者パスワードをリセットする方法について、管理者ガイドの「[Cisco ISE への管理アクセス](#)」を参照してください。
- Cisco ISE と Active Directory を結合します。

Active Directory との結合の詳細については、次の項目を参照してください。

Configure Active Directory as an External Identity Source

Active Directory で使用される証明書属性

Cisco ISE は、SAM と CN のいずれか、または両方の属性を使用してユーザーを識別します。Cisco ISE リリース 2.2 パッチ 5 以降、および 2.3 パッチ 2 以降は、sAMAccountName 属性をデフォルトの属性として使用します。これ以前のリリースでは、SAM と CN の両方の属性がデフォルトで検索されていました。この動作はリリース 2.2 パッチ 5 以降と 2.3 パッチ 2 以降で、[CSCvf21978](#) バグ修正の一部として変更されました。これらのリリースでは、sAMAccountName 属性のみがデフォルトの属性として使用されます。

実際の環境で必要に応じて、SAM と CN のいずれか、または両方を使用するように Cisco ISE を設定できます。SAM および CN が使用される場合、sAMAccountName 属性の値が一意でないと、Cisco ISE は CN 属性値も比較します。

Active Directory アイデンティティ検索の属性を設定するには、次の手順を実行します。

1. [管理 (Administration)] > [ID の管理 (Identity Management)] > [外部 ID ソース (External Identity Sources)] > [Active Directory] を選択します。[Active Directory] ウィンドウで、[拡張ツール (Advanced Tools)] をクリックし、[高度な調整 (Advanced Tuning)] を選択します。次の詳細を入力します。
 - [ISE ノード (ISE Node)] : Active Directory に接続される ISE ノードを選択します。
 - [名前 (Name)] : 変更するレジストリキーを入力します。Active Directory 検索属性を変更するには、
REGISTRY.Services\lsass\Parameters\Providers\ActiveDirectory\IdentityLookupField と入力します。
 - [値 (Value)] : ユーザーを識別するために ISE で使用する属性を入力します。
 - SAM : クエリで SAM のみを使用します (このオプションがデフォルトです)。
 - CN : クエリで CN のみを使用します。
 - SAMCN : クエリで CN と SAM を使用します。
 - [コメント (Comment)] : 変更内容を記述します (たとえば「デフォルト動作を SAM および CN に変更」)。
2. [値の更新 (Update Value)] をクリックしてレジストリを更新します。

ポップアップウィンドウが表示されます。メッセージを読み取り、変更を受け入れます。ISE の AD コネクタサービスが再起動します。

逆引き DNS ルックアップ

すべての DNS サーバーに分散展開されているすべての Cisco ISE ノードに対して、逆引き DNS ルックアップが設定されていることを確認します。そうしないと、アップグレード後にデプロイメント配置関連の問題が発生する可能性があります。

証明書の復元

PAN での証明書の復元

分散展開をアップグレードすると、次の両方の条件が満たされた場合は、プライマリ管理ノードのルート CA 証明書は信頼できる証明書ストアに追加されません。

- セカンダリ管理ノードは新しい展開でプライマリ管理ノードに昇格されている。
- セッションサービスはセカンダリノードでディセーブルになっている。

証明書がストアにない場合は、認証エラーが発生し、次のエラーが表示される可能性があります：

- Unknown CA in chain during a BYOD flow
- OCSP unknown error during a BYOD flow

これらのメッセージは、失敗した認証の [ライブログ (Live Logs)] ページの [詳細 (More Details)] リンクをクリックすると表示されます。

プライマリ管理ノードのルート CA 証明書を復元するには、新しい Cisco ISE ルート CA 証明書チェーンを生成します。[管理 (Administration)] > [証明書 (Certificates)] > [証明書署名要求 (Certificate Signing Requests)] > [ISE ルート CA 証明書チェーンの置き換え (Replace ISE Root CA certificate chain)] を選択します。

証明書とキーをセカンダリ管理ノードで復元する

セカンダリ管理ノードを使用している場合は、プライマリ管理ノードから Cisco ISE CA 証明書およびキーのバックアップを取得し、セカンダリ管理ノードで復元します。これにより、プライマリ PAN に障害が発生し、セカンダリ管理ノードをプライマリ管理ノードに昇格する場合に、セカンダリ管理ノードが外部 PKI ルート CA または下位 CA として動作するようになります。

証明書とキーのバックアップおよび復元に関する詳細については、次の項目を参照してください。

[Cisco ISE CA 証明書およびキーのバックアップと復元](#)

ルート CA チェーンの再生成

特定のアップグレードシナリオでは、アップグレードプロセスの完了後にルート CA チェーンを再生成する必要があります。次の手順に従って、ルート CA チェーンを再生成します。

1. Cisco ISE メインメニューから、[管理 (Administration)] > [システム (System)] > [証明書 (Certificates)] > [証明書の管理 (Certificate Management)] > [証明書署名要求 (Certificate Signing Requests)] の順に選択します。
2. [証明書署名要求 (CSR) の生成 (Generate Certificate Signing Request (CSR))] をクリックします。
3. [証明書の使用先 (Certificate(s) will be used for)] ドロップダウンリストで [ISE ルート CA (ISE Root CA)] を選択します。
4. [ISE ルート CA 証明書チェーンの置き換え (Replace ISE Root CA Certificate Chain)] をクリックします。

表 3: ルート CA チェーンの再生シナリオ

アップグレードのシナリオ	モード	ルート CA チェーンの再生成
フルアップグレードプロセス	展開	アップグレードプロセス中に展開が変更されないため、ルート CA の再生成は必要ありません。
分割アップグレードプロセス	展開	ルート CA チェーンの再生成
構成データベースの復元プロセス	スタンドアロン	ルート CA チェーンの再生成
ノードの昇格: 分割アップグレードプロセス後に、セカンダリ PAN をプライマリ PAN に昇格する	展開	ルート CA チェーンの再生成
Cisco ISE ノードのドメイン名またはホスト名の変更	スタンドアロンと展開	ルート CA チェーンの再生成

アップグレードプロセス後、次のイベントが発生する可能性があります。

1. ライブログにデータがない。
2. キューリンクエラー。
3. ヘルスステータスが使用不可。
4. 一部のノードのシステム概要に利用できる日付がない。

キューリンクエラーを解決し、情報を復元するには、[MnT Database](#) をリセットし、ISE ルート CA 証明書チェーンを置き換える必要があります。

脅威中心型 NAC

脅威中心型 NAC (TC-NAC) サービスを有効にしている場合は、アップグレード後に、TC-NAC アダプタが機能しない可能性があります。ISE GUI の [脅威中心型 NAC (Threat-Centric NAC)] ページからアダプタを再起動する必要があります。アダプタを再起動するには、アダプタを選択して [再起動 (Restart)] をクリックします。

SNMP 送信元ポリシーサービスノード設定

SNMP の設定で、手動で [元のポリシーサービスノード (Originating Policy Services Node)] の値を設定した場合、この設定はアップグレード中に失われます。SNMP 設定を再設定する必要があります。

詳細については、

[「Network Device Definition Settings」](#) の「SNMP Settings」を参照してください。

プロファイラ フィード サービス

アップグレード後にプロファイラ フィード サービス更新して、最新 OUI がインストールされているようにします。

Cisco ISE 管理者用ポータルから：

-
- ステップ 1 [管理 (Administration)] > [フィード サービス (FeedService)] > [プロファイラ (Profiler)] を選択します。プロファイラ フィード サービスが有効にされていることを確認します。
 - ステップ 2 Cisco ISE GUI で [メニュー (Menu)] アイコン (☰) をクリックして、[管理 (Administration)] > [フィード サービス (FeedService)] > [プロファイラ (Profiler)] を選択します。プロファイラ フィード サービスが有効にされていることを確認します。
 - ステップ 3 [今すぐ更新 (Update Now)] をクリックします。
-

クライアント プロビジョニング

クライアントプロビジョニングポリシーで使用されているネイティブのサブリカントプロファイルをチェックして、ワイヤレス SSID が正しいことを確認します。iOS デバイスの場合、接続対象ネットワークが非表示の場合は、[iOS の設定 (iOS Settings)] エリアで [ターゲットネッ

トワーク非表示時にイネーブルにする (Enable if target network is hidden)] チェックボックスをオンにします。

ISE でのクライアント プロビジョニング リソースの更新：

オンライン更新

-
- ステップ 1 [ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [結果 (Results)] > [クライアント プロビジョニング (Client Provisioning)] > [リソース (Resources)] を選択して、クライアント プロビジョニング リソースを設定します。
 - ステップ 2 [追加 (Add)] をクリックします。
 - ステップ 3 [シスコサイトからのエージェントリソース (Agent Resources From Cisco Site)] を選択します。
 - ステップ 4 [リモートリソースのダウンロード (Download Remote Resources)] ウィンドウで、Cisco Temporal Agent リソースを選択します。
 - ステップ 5 [保存 (Save)] をクリックして、ダウンロードしたリソースが [リソース (Resources)] ページに表示されていることを確認します。
-

オフライン更新

-
- ステップ 1 [追加 (Add)] をクリックします。
 - ステップ 2 [ローカルディスクからのエージェントリソース (Agent Resources from Local Disk)] を選択します。
 - ステップ 3 [カテゴリ (Category)] ドロップダウンから、[シスコが提供するパッケージ (Cisco Provided Packages)] を選択します。
-

暗号スイート

これらの廃止予定の暗号方式を Cisco ISE に対する認証に使用する古い IP フォンなどのレガシーデバイスがある場合、これらのデバイスは従来の暗号方式を使用するため、認証は失敗します。アップグレード後に Cisco ISE がレガシーデバイスを認証できるようにするには、次のように [許可されているプロトコル (Allowed Protocols)] の設定を更新してください。

-
- ステップ 1 管理者用ポータルから、[ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [結果 (Results)] > [認証 (Authentication)] > [許可されているプロトコル (Allowed Protocols)] を選択します。
 - ステップ 2 許可されているプロトコルサービスを編集し、[弱い暗号方式をEAPに許可する (Allow weak ciphers for EAP)] チェックボックスをオンにします。

ステップ3 [送信 (Submit)] をクリックします。

関連トピック

[Cisco Identity Services Engine リリースノート](#)

[Cisco Identity Services Engine ネットワークコンポーネントの互換性](#)

モニターリングおよびトラブルシューティング

- 電子メール設定、お気に入りレポート、データ削除設定を再設定します。
- 必要とする特定のアラームのしきい値またはフィルタを確認します。すべてのアラームは、アップグレード後にデフォルトでイネーブルになります。
- 必要に応じてレポートをカスタマイズします。古い展開でレポートをカスタマイズした場合は、加えた変更が、アップグレードプロセスによって上書きされます。

MnT バックアップの復元

更新前に作成した MnT データの運用データバックアップを使用して、バックアップを復元します。

詳細については、以下を参照してください。

詳細については、『Cisco ISE 管理者ガイド』の「[バックアップ/復元操作](#)」を参照してください。

Trustsec NAD に対するポリシーの更新

次のコマンドを次の順序で実行して、システムの Cisco TrustSec 対応レイヤ 3 インターフェイスにポリシーをダウンロードします。

- `no cts role-based enforcement`
- `cts role-based enforcement`

サブリカント プロビジョニング ウィザードの更新

新しいリリースにアップグレードする場合、またはパッチを適用する場合、サブリカントプロビジョニングウィザード (SPW) は更新されません。SPW を手動で更新し、新しい SPW を参照する新しいネイティブサブリカントプロファイルと新しいクライアントプロビジョニングポリシーを作成する必要があります。新しい SPW は ISE ダウンロードページで使用できます。

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。