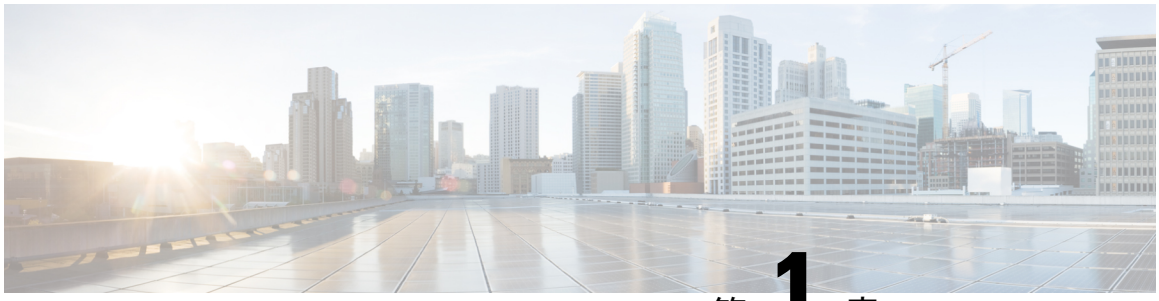
Cisco Identity Services Engine リリース 3.2 アップグレードガイド

初版：2022 年 8 月 16 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/

目 次



第 1 章

Cisco ISE のアップグレード

Cisco ISE アップグレードの概要

Cisco Identity Services Engine（Cisco ISE）リリース 3.1 以降、すべての pxGrid 接続は pxGrid 2.0 に基づく必要があります。 pxGrid 1.0 ベース（XMPP ベース）の統合は、リリース 3.1 以降の Cisco ISE では動作しなくなります。

WebSocket に基づく pxGrid バージョン 2.0 は、Cisco ISE リリース 2.4 で導入されました。統合の中断を防ぐために、他のシステムを計画して pxGrid 2.0 準拠バージョンにアップグレードすることをお勧めします。

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（VM）で Cisco ISE ソフトウェアをリリース 3.2 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 3.2 リリースノート』の「Cisco ISE リリース 3.2 の新機能」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ー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。

Cisco ISE のネイティブクラウド展開の違い

Cisco ISE アップグレードワークフローは、クラウドプラットフォームにネイティブに展開された Cisco ISE インスタンスではサポートされていません。新規インストールのみがサポートされています。ただし、設定データのバックアップと復元は実行できます。Cisco ISE のネイティブ展開を可能にするクラウドプラットフォーム：

1. Amazon Web Services（AWS）
2. Azure Cloud
3. Oracle Cloud Infrastrucure（OCI）

AWS の場合、Cisco ISE リリース 3.1 からリリース 3.2 にアップグレードするには、次の手順を実行します。

1. Cisco ISE リリース 3.1 AWS インスタンスから設定データをバックアップします。
2. Cisco ISE リリース 3.2 で AWS インスタンスを再設定します。
3. 新しく作成された Cisco ISE リリース 3.2 インスタンスで設定データを復元します。

ルート CA チェーンの再生成

次のイベントが発生した場合は、ルート CA チェーンを再生成する必要があります。

- PAN または PSN のドメイン名またはホスト名の変更。
- 新しい展開でのバックアップの復元。
- アップグレード後に古いプライマリ PAN を新しいプライマリ PAN に昇格。

ルート CA チェーンを再生成するには、次のように選択します。

1. Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、[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から、[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。

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、Cisco ISE リリース 3.2 に直接アップグレードできます。

- Cisco ISE リリース 2.7
- Cisco ISE リリース 3.0
- Cisco ISE リリース 3.1

2 段階のアップグレード

Cisco ISE リリース リリース 2.7 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 3.2 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 3.2 では、ADE-OS は RHEL 8.4 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 リリース	RHEL リリース
Cisco ISE 2.3	RHEL 7.0
Cisco ISE 2.4	RHEL 7.3
Cisco ISE 2.6	RHEL 7.5
Cisco ISE 2.7	RHEL 7.6
Cisco ISE 3.0	RHEL 7.6
Cisco ISE 3.1	RHEL 8.2
Cisco ISE 3.2	RHEL 8.4

（注） RHEL 8.2 以降は、次の VMware ESXi バージョンをサポートしています。

- VMware ESXi 6.7
- VMware ESXi 6.7 U1
- VMware ESXi 6.7 U2
- VMware ESXi 6.7 U3
- VMware ESXi 7.0
- VMware ESXi 7.0 U1
- VMware ESXi 7.0 U2
- VMware ESXi 7.0 U3

上記に加えて、RHEL 8.4 は、互換性のある新しい VMware ESXi バージョンもサポートします。

Cisco ISE リリース 3.0 以降のリリースでは、VMware ESXi 7.0.3 以降のリリースに更新することを推奨します。

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す。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

この項では、Cisco ISE リリース のライセンスの変更点について説明します。

Cisco ISE ライセンスの詳細については、次の資料を参照してください。

- Cisco ISE 発注ガイド
- Cisco ISE 移行ガイド
- Cisco ISE ライセンス FAQ

Cisco ISE GUI でのライセンスのアクティブ化については、「Licensing」を参照してください。

仮想アプライアンスのライセンス

Cisco ISE リリース 3.1 以降は ISE VM ライセンスをサポートしています。これは、リリース 3.1 以前にサポートされていた VM Small、VM Medium、および VM Large ライセンスに代わるものです。新しい ISE VM ライセンスは、オンプレミス展開とクラウド展開の両方の Cisco ISE VM ノードを対象としています。

詳細については、『*Cisco ISE Administrator Guide, Release 3.3*』の「Licensing」の章にある「Cisco ISE Licenses」を参照してください。

特定ライセンス予約

特定のライセンス予約は、組織のセキュリティ要件で Cisco ISE と Cisco Smart Software Manager（CSSM）間の永続的な接続が許可されていない場合にスマートライセンスを管理するためのスマートライセンス方式です。特定のライセンス予約では、Cisco ISE ノードで特定のライセンス権限を予約できます。

予約する必要があるライセンスのタイプと数を定義して特定のライセンス予約を作成し、Cisco ISE ノードで予約をアクティブ化します。登録して予約を有効にした Cisco ISE ノードは、ライセンスの使用を追跡し、ライセンス消費のコンプライアンスを適用します。

詳細については、『*Cisco ISE Administrator Guide, Release 3.2*』の「Licensing」の章にある「Specific License Reservation」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 で作業するときに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

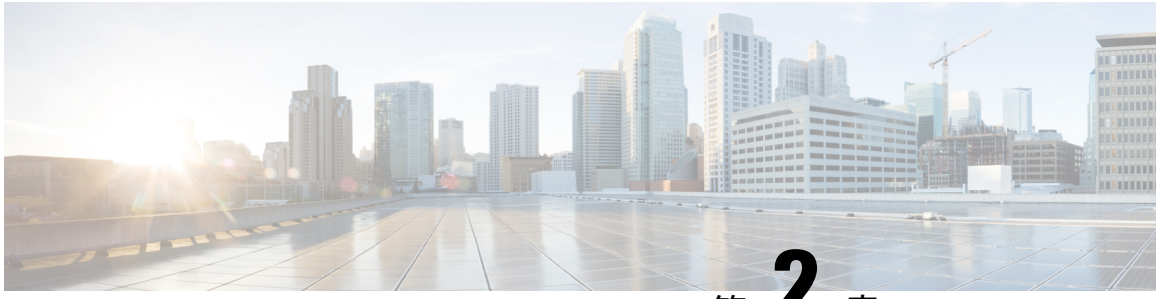
- シスコからタイムリーな関連情報を受け取るには、Cisco Profile Manager でサインアップしてください。
- 重要な技術によりビジネスに必要な影響を与えるには、シスコサービスにアクセスしてください。
- サービス リクエストを送信するには、シスコサポートにアクセスしてください。
- 安全で検証済みのエンタープライズクラスのアプリケーション、製品、ソリューション、およびサービスを探して参照するには、Cisco DevNet にアクセスしてください。
- 一般的なネットワーク、トレーニング、認定関連の出版物を入手するには、Cisco Press にアクセスしてください。
- 特定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

ヘルスチェック

アップグレードプロセスの前に Cisco ISE 展開のヘルスチェックを実行して、アップグレードのダウンタイムを引き起こす可能性のある重大な問題を特定して解決してください。詳細については、『Cisco ISE Admin Guide』の「Troubleshooting」の章にある「**Health Check**」の項を参照してください。

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。

（注） Cisco ISE リリース 2.6 パッチ 10 以降または 2.7 パッチ 4 以降のリリースからアップグレードし、SSM オンプレミスサーバーが設定されている場合は、アップグレードプロセスを開始する前に SSM オンプレミスサーバーを切断する必要があります。

- 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。
- 現在 Cisco ISE リリース 3.0 以降にアップグレードしている場合は、ヘルスチェックまたはアップグレード準備ツール（URT）を使用して、アップグレードプロセスを開始する前にシステム診断を実行できます。
- 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（このウィンドウを表示するには、[メニュー（Menu）]アイコン（☰）をクリックして、**[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（このウィンドウを表示するには、[メニュー（Menu）]アイコン（☰）をクリックして、**[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（このウィンドウを表示するには、[メニュー（Menu）]アイコン（☰）をクリックして、**[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。
  - [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ます。このウィンドウを表示するには、[メニュー（Menu）]アイコン（☰）をクリックして、[管理（Administration）]>[システム（System）]>[設定（Settings）]>[プロトコル（Protocols）]>[RADIUS]ウィンドウに移動して、繰り返し発生するアカウンティング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 2.7、3.0、および 3.1 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） 「」「」「」「「ディスク領域に関する要件」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実行する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。

Before you begin

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
- ペルソナ変更を実行する

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, on page 12
ステップ 2 アップグレード準備ツールの実行, on page 13

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。

Before you begin

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-3.2.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-3.2.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-3.2.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-3.2.*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。

Before you begin

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-3.2.0.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

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（ユーザー定義された）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

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. Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[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。
3. [すぐにバックアップ（Backup Now）] をクリックします。
4. バックアップを実行するために必要な値を入力します。
5. [OK] をクリックします。
6. 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、指定されたリ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 3.2 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. Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [認証局証明書（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。このウィンドウを表示するには、[メニュー（Menu）]アイコン（☰）をクリックして、**[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）]**を選択します。

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（このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして、[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [証明書の管理（Certificate Managemen）]を選択）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（このウィンドウを表示するには、[メニュー（Menu）]アイコン（☰）をクリックして、[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）]を選択）内の証明書の [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。

証明書の削除

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 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[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）]**を選択します。

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 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、[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）] を選択します。

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 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、[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）] を選択します。

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 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[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）]**を選択します。

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 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、[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）]を選択します。

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。

Cisco ISE リリース 2.7 以降では、Network Time Protocol デーモン（ntpd）の代わりに chrony が使用されます。ntpd はルート分散が最大 10 秒のサーバーと同期しますが、chrony はルート分

散が3秒未満のサーバーと同期します。したがって、NTPサービスの中断を回避するために、Cisco ISE リリース 2.7 以降にアップグレードする前に、ルート分散が低い NTP サーバーを使用することを推奨します。詳細については、『Troubleshoot ISE and NTP Server Synchronization Failures on Microsoft Windows』を参照してください。

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（このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして、[管理（Administration）] > [システム（System）] > [展開（Deployment）] > <ノード> > を選択します）。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 からダウンロードします。

リリース 3.2 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-3.2.0.*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-3.2.0.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-3.2.0.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-3.2.0.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。

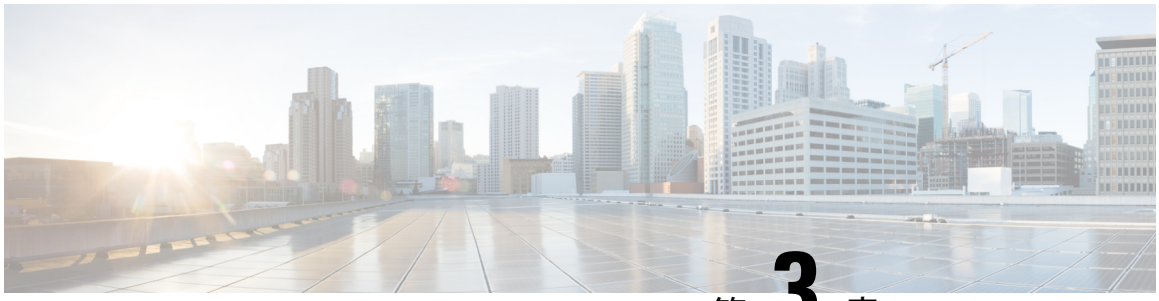
ログの保持と MnT ハードディスクのサイズ変更

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（このウィンドウを表示するには、[メニュー（Menu）]アイコン（☰）をクリックして、**[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）]**を選択します）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

アップグレードを実行します。

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で、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 （57 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ー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/セカンダリ モニターリング ノード	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. プライマリ管理/セカンダリ モニターリング 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、プライマリ管理/プライマリ モニターリング ノード	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. プライマリ管理/プライマリ モニターリング 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、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、プライマリ管理/セカンダリ モニターリング ノード	**1.** セカンダリ管理ノード **2.** プライマリ 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/セカンダリ モニターリング ノード
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	**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	**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	**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

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 2.7 以降	Cisco ISE 2.7 以降	Cisco ISE 2.7 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いため、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。Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[ISE管理（ISE Administration）]**>**[アップグレード（Upgrade）]**を選択します。ISO イメージをダウンロードする新しいリポジトリを作成します。

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ギン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。

（注） Nutanix プラットフォームでは、フルアップグレード方式または分割アップグレード方式を使用した GUI からの Cisco ISE のアップグレードや、CLI からの Cisco ISE のアップグレードはサポートされていません。Nutanix プラットフォームでは新規インストールの方式またはバックアップと復元の方式を使用して Cisco ISE をアップグレードできます。

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

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、PAN UI 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る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。

（注） バックアップと復元の方法を使用して Cisco ISE をアップグレードした後に、展開内のすべてのノードを手動で同期する必要があります。

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 2.7 以降を使用している場合は、Cisco ISE リリース 3.2 に直接アップグレードできます。

Cisco ISE リリース 3.2 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 3.2 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 3.2 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 ノードの Cisco ISE リリース 2.7、3.0 または 3.13.0、3.1 または 3.2 へのアップグレード

Before you begin

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。古いレポートデータを保持しない場合は、手順 4 ～ 6 をスキップします。

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。インストール後に、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 3.2 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 3.2 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 3.2 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 3.2 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 3.2 の最新パッチに再イメージ化し、新しい Cisco ISE リリース 3.2 展開環境に参加させます。

What to do next

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 3.2 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。

Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[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には、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。

Cisco ISE における GUI ベースのアップグレードのオプション

展開済みの Cisco ISE のリリースに応じて、[Administration] > [System] > [Upgrade] > [Upgrade Selection] ウィンドウで次のオプションのいずれかを選択して、Cisco ISE 展開をアップグレードできます。

- [フルアップグレード（Full Upgrade）]：フルアップグレードは、同時に Cisco ISE 展開のすべてのノードの完全なアップグレードを可能にするマルチステッププロセスです。この方法により、展開は、分割アップグレードプロセスよりも短時間でアップグレードされます。すべてのノードが並行してアップグレードされるため、アップグレードプロセス中にアプリケーションサービスがダウンします。

  フルアップグレード方式は、Cisco ISE 2.6 パッチ 10 以降、Cisco ISE 2.7 パッチ 4 以降、および Cisco ISE 3.0 パッチ 3 以降でサポートされます。

- [分割アップグレード（Split Upgrade）]：分割アップグレードは、アップグレードプロセス中にサービスを引き続き利用できるようにしながら、Cisco ISE 展開のアップグレードを可能にするマルチステッププロセスです。このアップグレード方法では、展開時にアップグレードする Cisco ISE ノードを選択できます。新しい分割アップグレードワークフローでは、システムが稼働しているときに事前チェックとデータアップグレードが行われます。これにより、ダウンタイムが大幅に短縮され、信頼性の高いアップグレードにつながります。

  新しい分割アップグレード方式は、Cisco ISE 3.2 パッチ 2 以降でサポートされています。

- **[Split Upgrade]**：従来の分割アップグレードは、アップグレードプロセス中にサービスを引き続き利用できるようにしながら、Cisco ISE 展開のアップグレードを可能にするマルチステッププロセスです。このアップグレード方法では、展開時にアップグレードする Cisco ISE ノードを選択できます。

  Cisco ISE リリース 2.7、3.0、または 3.1 から Cisco ISE リリース 3.2 への従来の分割アップグレードを実行できます。このオプションは、Cisco ISE リリース 3.2 パッチ 3 以降の Cisco ISE GUI では使用できません。

（注） Cisco ISE 3.2 では、**分割アップグレード**方式の使用中にアップグレード準備ツール（URT）とユーザーインターフェイス（UI）の事前チェックが必要になります。**フルアップグレード**方式を使用する場合は UI の事前チェックのみが必要です。

これらの GUI アップグレード方式は Cisco ISE 2.6 パッチ 10 以降から利用できますが、Cisco ISE 3.2 にアップグレードするには、少なくとも Cisco ISE 2.7 パッチ 4 を実行している必要があります

GUI からの Cisco ISE 展開のフルアップグレード

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。フルアップグレードは、Cisco ISE 展開の完全なアップグレードを可能にするマルチステッププロセスです。

Cisco ISE 展開のフルアップグレードを実行するには、次の手順を実行します。

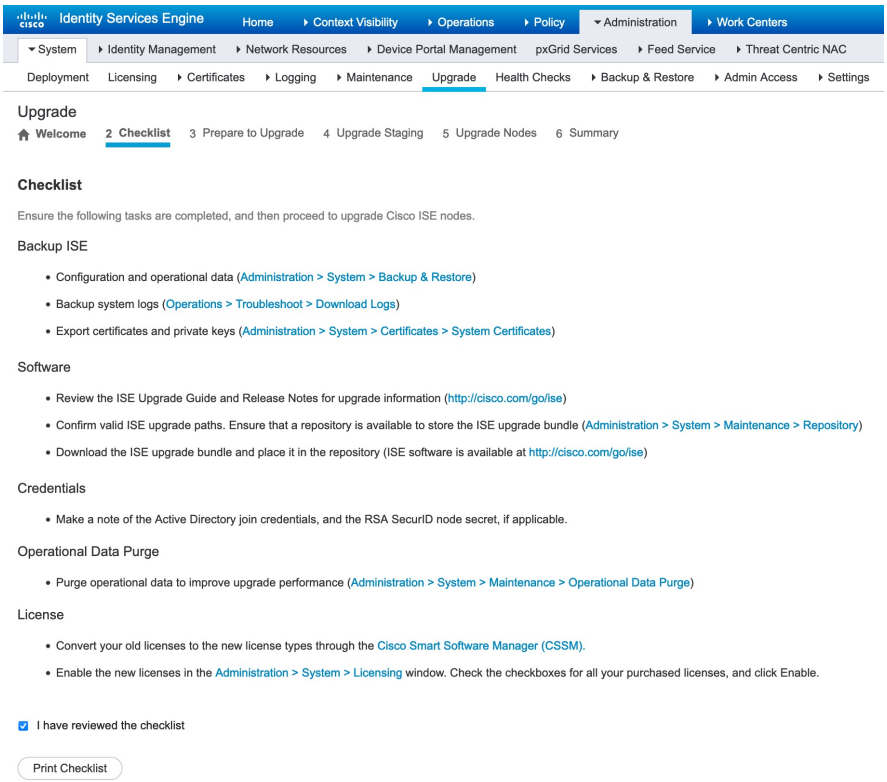
ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[管理（Administration）]** > **[システム（System）]** > **[アップグレード（Upgrade）]**の順に選択します。

ステップ 2 [アップグレードを選択（Upgrade Selection）] ウィンドウで、[フルアップグレード（Full Upgrade）] をクリックし、[アップグレードを開始（Start Upgrade）] をクリックします。

ステップ 3 **[ようこそ（Welcome）]** ウィンドウで [次へ（Next）] をクリックして、アップグレードワークフローを開始します。

ステップ 4 アップグレードプロセス中のブロッカーやダウンタイムを回避するために、[チェックリスト（Checklist）] ウィンドウに記載されているすべてのタスクを完了させてください。

Figure 1: チェックリストを表示するアップグレードウィンドウ



ステップ 5 （オプション）チェックリストを参照用にダウンロードするには、[チェックリストの印刷（Print Checklist）] をクリックします。

ステップ 6 アップグレードチェックリストに記載されている項目の確認が完了したら、[チェックリストを確認しました（I have reviewed the checklist）] チェックボックスをオンにして [次へ（Next）] をクリックします。

[アップグレードの準備（Prepare to Upgrade）] ウィンドウが表示されます。

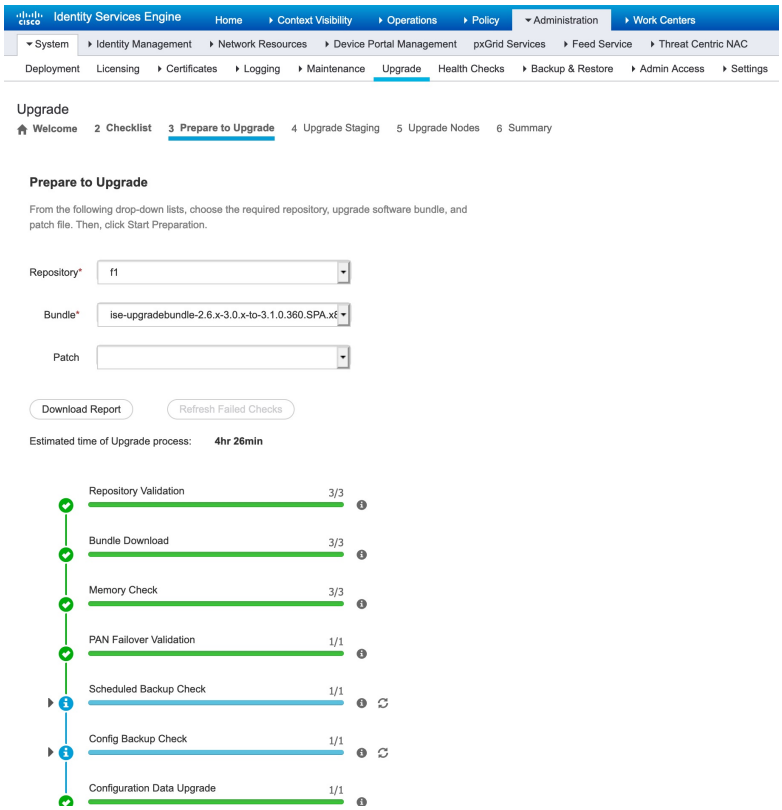
ステップ 7 [リポジトリ（Repository）] ドロップダウンリストから、アップグレードバンドルが格納されているリポジトリを選択します。

ステップ 8 [バンドル（Bundle）] ドロップダウンリストから、アップグレードバンドルを選択します。

ステップ 9 すべてのパッチリリースが [パッチ（Patch）] ドロップダウンリストに表示されます。アップグレードする Cisco ISE リリースの最新のパッチを選択することを推奨します。

ステップ 10 [準備の開始（Start Preparation）] をクリックして、すべての Cisco ISE コンポーネントを検証し、展開のレポートを生成します。

Figure 2: [アップグレードの準備（Prepare to Upgrade）] タブにノードを表示するアップグレードウィンドウ



Cisco ISE は、アップグレードプロセス中に次のことを確認します。

事前チェックリスト	説明
リポジトリの検証	リポジトリがすべてのノードに設定されているかどうかを確認します。
バンドルのダウンロード	すべてのノードについてアップグレードバンドルをダウンロードして準備するようにします。
メモリ チェック	PAN またはスタンドアロンノードで 25 % のメモリ領域が使用可能かどうか、および他のすべてのノードで 1 GB のメモリ領域が使用可能かどうかを確認します。
PAN のフェールオーバーの検証	PAN のハイアベイラビリティが有効になっているかどうかを確認します。 アップグレードの開始前に、PAN のハイアベイラビリティが無効になることが管理者に通知されます。

事前チェックリスト	説明
スケジュールバックアップの確認	スケジュールバックアップが有効になっているかどうかを確認します。 **Note** このチェックは、アップグレードプロセスでは必須ではありません。
構成のバックアップの確認	構成のバックアップが最近行われたかどうかを確認します。アップグレードプロセスは、バックアップが完了していないと実行されません。
構成データのアップグレード	構成データベースのクローンで構成データのアップグレードを実行し、アップグレードされたデータダンプを作成します。このチェックは、バンドルのダウンロード後に開始されます。
プラットフォーム サポート チェック	展開でサポートされているプラットフォームを確認します。システムに少なくとも 12 コア CPU、300 GB のハードディスク、および 16 GB のメモリがあるかどうかも確認します。また、ESXi バージョンが 6.5 以上であるかどうかも確認します。
展開の検証	展開のノードの状態（同期しているか進行中か）を確認します。
DNS の解決可能性	ホスト名と IP アドレスの正引きと逆引きを確認します。
信頼ストア証明書の検証	信頼ストア証明書が有効か期限切れかを確認します。
システム証明書の検証	各ノードのシステム証明書の検証を確認します。
ディスク容量チェック	アップグレードプロセスを続行するための十分な空き領域がハードディスクにあるかどうかを確認します。
NTP の到達可能性と時刻源の確認	システムで設定されている NTP をチェックし、時刻源が NTP サーバーからのものかどうかを確認します。
負荷平均チェック	指定した間隔でシステムの負荷を確認します。指定できる間隔は、1、5、または 15 分です。
サービスまたはプロセスの失敗	サービスまたはアプリケーションの状態（実行中か障害状態か）を示します。

非アクティブなコンポーネントや失敗したコンポーネントがある場合、それらは赤色で表示されます。また、トラブルシューティング情報も表示されます。失敗したコンポーネントのアップグレードのシビラティ（重大度）に基づいて、アップグレードプロセスを続行できる場合と、アップグレードプロセスを進めるために問題を解決するように通知される場合があります。

[失敗したチェックの更新（Refresh Failed Checks）] オプションは、赤色で強調表示された障害のみを更新します。アップグレードを実行する前に、これらの障害を修正する必要があります。オレンジ色で強調表示された警告では、アップグレードプロセスは停止しません。ただし、アップグレード後に特定の Cisco ISE 機能に影響する可能性があります。各警告の横に表示される [更新（Refresh）] アイコンをクリックすると、問題の解決後にこれらのチェックが更新されます。

[展開して表示（Expand to Show）] アイコンをクリックすると、各ノードとそのステータスに関する追加情報が表示されます。

[情報（Information）] アイコンをクリックして、各コンポーネントの詳細を確認することもできます。

生成されたレポートのコピーを取得するには、[レポートのダウンロード（Download Report）] をクリックします。

ステージングおよびアップグレードプロセスにかかる推定時間を確認できます。これは、次の情報に基づいて計算されます。

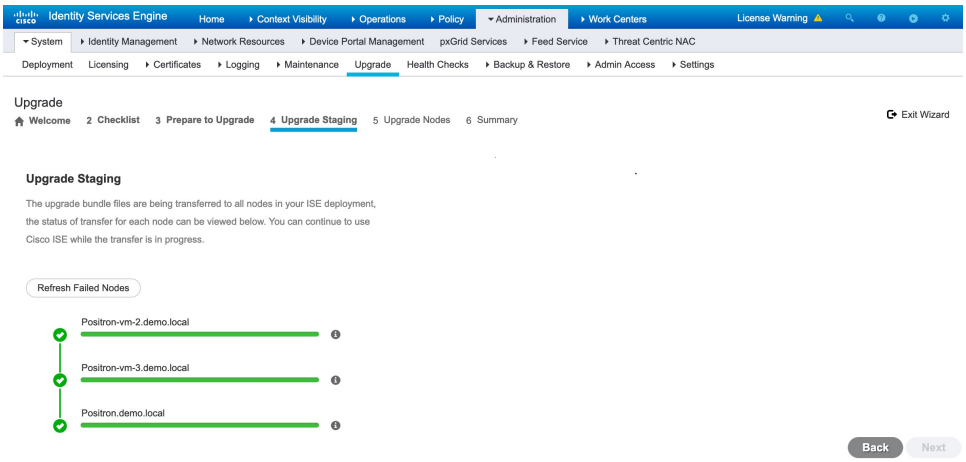
- ネットワーク速度
- ノードの構成：プロセッサ、RAM、およびハードディスクの数
- データベースのデータサイズ
- ノードがアプリケーションサーバーを起動するのにかかった時間

Note バンドルのダウンロードと構成データのアップグレードを除くすべての事前チェックは、システムの検証を開始してから 4 時間後に自動的に期限切れになります。

ステップ 11 すべてのノードの事前チェックが完了したら、[ステージングを開始（Start Staging）] をクリックしてステージングプロセスを開始します。

アップグレードのステージング中に、アップグレードされたデータベースファイルが展開のすべてのノードにコピーされ、展開のすべてのノードで構成ファイルがバックアップされます。

Figure 3: アップグレードステージングを示すアップグレードウィンドウ



ノードのアップグレードステージングに成功した場合、緑色で表示されます。特定のノードのアップグレードステージングに失敗した場合は、赤色で表示されます。また、トラブルシューティング情報も表示されます。

[リフレッシュに失敗したノード（Refresh Failed Nodes）] アイコンをクリックして、失敗したノードのアップグレードステージングをもう一度開始します。

ステップ 12 [次へ（Next）] をクリックして [ノードのアップグレード（Upgrade Nodes）] ウィンドウに進みます。

[ノードのアップグレード（Upgrade Nodes）] ウィンドウで、全体的なアップグレードの進行状況と、展開内の各ノードのステータスを確認できます。

ステップ 13 [次へ（Next）] をクリックしてアップグレードプロセスを開始します。

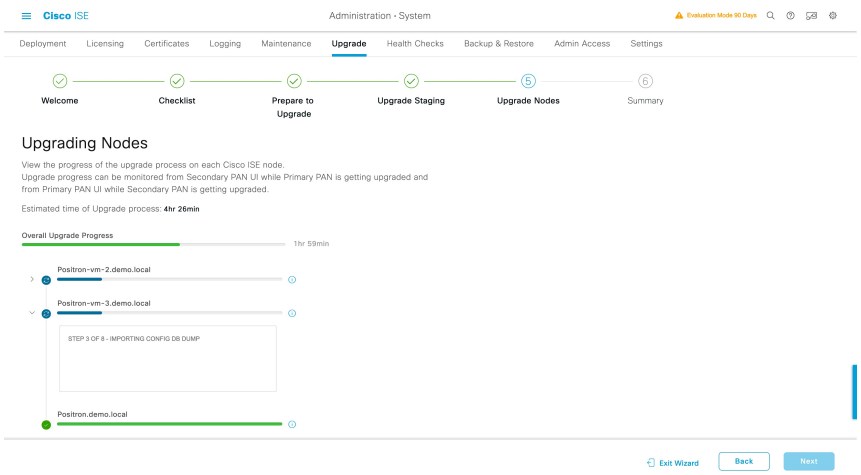
アップグレード手順が完了する直前に、「システムのアップグレードを開始します。ログアウトしています。（`The system is about to upgrade. Logging Out.`）」が表示されます。

ステップ 14 [OK] をクリックして続行します。

Note セカンダリ PAN にログインし直して、アップグレードの進行状況をモニターできます。

プライマリ PAN のアップグレード中に、セカンダリ PAN のダッシュボードからプライマリ PAN のアップグレードステータスをモニターできます。プライマリ PAN のアップグレードが完了したら、プライマリ PAN ダッシュボードからすべての Cisco ISE ノードのアップグレードステータスをモニターできます。

Figure 4: アップグレードステータスを示すアップグレード ノード ウィンドウ



Note このウィンドウで [ウィザードの終了（Exit Wizard）] オプションをクリックした場合、後で [概要（Summary）] ウィンドウを表示できません。

ステップ 15 [ノードのアップグレード（Upgrade Nodes）] ウィンドウで [次へ（Next）] をクリックして、すべてのノードが正常にアップグレードされたかどうかを確認します。

失敗したノードがある場合は、そのノードに関する情報を示すダイアログボックスが表示されます。

ステップ 16 失敗したノードを展開から登録解除するには、ダイアログボックスで [OK] をクリックします。

アップグレードプロセスが完了したら、[概要（Summary）] ウィンドウで展開の診断アップグレードレポートを表示およびダウンロードできます。チェックリスト、アップグレードの準備、アップグレードレポート、およびシステムヘルスの各チェックリスト項目に関する詳細を含むアップグレードサマリーレポートを確認してダウンロードできます。

GUI からの Cisco ISE 展開の分割アップグレード

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。分割アップグレードは、ユーザーがサービスを引き続き利用できるようにしながら、Cisco ISE 展開のアップグレードを可能にするマルチステッププロセスです。これには、認証の実行にノードを確実に利用できるように、ネットワークまたはロードバランサの変更が必要になる場合があります。安定性を向上させ、ダウンタイムを削減するために、新しい分割アップグレードフレームワークが Cisco ISE リリース 3.3 に追加されました。分割アップグレードでは、ノードをバッチに分割し、バッチごとにアップグレードを繰り返すことで、ダウンタイムを制限できます。ただし、このプロセスは、フルアップグレードよりも時間がかかる場合があります。Cisco ISE リリース 3.2 パッチ 3 以降から Cisco ISE リリース 3.3 以降にアップグレードできます。

新しい分割アップグレードワークフローには、次の利点があります。

- 事前チェックは、アップグレードの進行フェーズの前に行われます。
- データのアップグレードは、事前チェックフェーズ中に行われます。これにより、データアップグレードにかかる時間が短縮され、データアップグレードの問題が原因でシステムが使用不能になるリスクが軽減されます。
- PSN と MnT ノードは、最初の反復自体でセカンダリ PAN とともに選択することができ、最後の反復でプライマリ PAN と共に選択することもできます。選択した MnT ノードは、プライマリまたはセカンダリにすることができます。セカンダリまたはプライマリ PAN を個別にアップグレードする必要はありません。
- PSN と MnT ノードは、同じ反復の一部として選択されたときに同時にアップグレードされるため、アップグレード時間がさらに短縮されます。

Cisco ISE 展開の分割アップグレードを実行するには、次の手順を実行します。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[管理（Administration）] > [システム（System）] > [アップグレード（Upgrade）]**の順に選択します。

ステップ 2 [Upgrade Selection] ウィンドウで、[Split Upgrade] をクリックします。アップグレードタイプを分割アップグレードに変更されると事前チェックレポートがクリアされることと、事前チェック実行段階およびノードステージング段階では ISE サービスが引き続き機能することを示す警告メッセージが表示されます。[OK] をクリックして作業を続行します。

ステップ 3 [Start Upgrade] をクリックします。

ステップ 4 **[ようこそ（Welcome）]** ウィンドウで [やってみましょう（Let's Do It）] をクリックして、アップグレードワークフローを開始します。

ステップ 5 アップグレードプロセス中の遅延やダウンタイムを回避するために、[Checklist] ウィンドウに記載されているすべてのタスクを完了させてください。

ステップ 6 （オプション）チェックリストを参照用にダウンロードするには、[チェックリストの印刷（Print Checklist）] をクリックします。

ステップ 7 アップグレードチェックリストに記載されている項目の確認が完了したら、[チェックリストを確認しました（I have reviewed the checklist）] チェックボックスをオンにして [次へ（Next）] をクリックします。

[ノード選択（Node Selection）] ウィンドウが表示されます。

ステップ 8 現在の反復でアップグレードするノードの横にあるチェックボックスをオンにします。

Note

- セカンダリ PAN は、アップグレードの最初の反復でデフォルトで選択されます。最初の反復ではプライマリ PAN を選択できません。また、他のすべてのノードがアップグレードされるか、アップグレード対象として選択されるまで、反復でプライマリ PAN を選択することはできません。最初の反復でのプライマリ MnT またはセカンダリ MnT と、任意の数の PSN を選択できます。
- 最初の反復でセカンダリ PAN 以外のノードが選択された場合、最初の反復は 2 つのバッチで行われます。セカンダリ PAN は最初のバッチでアップグレードされ、その後、最初の反復の一部として選択された残りのノードの同時アップグレードが続きます。
- PSN と MnT ノードは、どの反復でも並行してアップグレードできます。
- アップグレードプロセス中は、反復ごとに 15 以下のノードを選択することをお勧めします。

ステップ 9 [次へ（Next）] をクリックします。

[アップグレードの準備（Prepare to Upgrade）] ウィンドウが開きます。

ステップ 10 [リポジトリ（Repository）] ドロップダウンリストから、アップグレードバンドルが格納されているリポジトリを選択します。

Note SFTP リポジトリを使用している場合は、CLI を使用してすべてのノードに暗号ホストキーを追加する必要があります。

ステップ 11 [バンドル（Bundle）] ドロップダウンリストから、アップグレードバンドルを選択します。

すべてのパッチリリースが [パッチ（Patch）] ドロップダウンリストに表示されます。アップグレードする Cisco ISE リリースの最新のパッチを選択することを推奨します。

ステップ 12 [準備の開始（Start Preparation）] をクリックして、すべての Cisco ISE コンポーネントを検証し、展開のレポートを生成します。

Cisco ISE は、アップグレードプロセス中に次のことを確認します。

Note

- [バンドルダウンロード（Bundle Download）] は、最初の反復のプライマリ PAN を含む、選択されたすべてのノードでトリガーされます。残りの反復では、[バンドルダウンロード（Bundle Download）] は選択したノードに対してのみトリガーされます。
- [スケジュールバックアップの確認（Scheduled Backup Check）] と [構成のバックアップの確認（Config Backup Check）] は、最初の反復でのみ発生します。

事前チェックリスト	説明
リポジトリの検証	リポジトリがすべてのノードに設定されているかどうかを確認します。
バンドルのダウンロード	すべてのノードについてアップグレードバンドルをダウンロードして準備するようにします。

事前チェックリスト	説明
メモリ チェック	PAN またはスタンドアロンノードで 25 % のメモリ領域が使用可能かどうか、および他のすべてのノードで 1 GB のメモリ領域が使用可能かどうかを確認します。
パッチバンドルのダウンロード（Patch Bundle Download）	選択したノードのパッチバンドルをダウンロードするのに役立ちます。
PAN のフェールオーバーの検証	PAN のハイアベイラビリティが有効になっているかどうかを確認します。 アップグレードの開始前に、PAN のハイアベイラビリティが無効になることが管理者に通知されます。
スケジュールバックアップの確認	スケジュールバックアップが有効になっているかどうかを確認します。 **Note** このチェックは、アップグレードプロセスでは必須ではありません。
構成のバックアップの確認	構成のバックアップが最近行われたかどうかを確認します。アップグレードプロセスは、バックアップが完了していないと実行されません。
構成データのアップグレード	構成データベースのクローンで構成データのアップグレードを実行し、アップグレードされたデータダンプを作成します。このチェックは、バンドルのダウンロード後に開始されます。
プラットフォーム サポート チェック	展開でサポートされているプラットフォームを確認します。システムに少なくとも 12 コア CPU、300 GB のハードディスク、および 16 GB のメモリがあるかどうかも確認します。また、ESXi バージョンが 6.5 以上であるかどうかも確認します。
展開の検証	展開のノードの状態（**同期している**か**進行中**か）を確認します。
DNS の解決可能性	ホスト名と IP アドレスの正引きと逆引きを確認します。
信頼ストア証明書の検証	信頼ストア証明書が有効か期限切れかを確認します。
システム証明書の検証	各ノードのシステム証明書の検証を確認します。

事前チェックリスト	説明
ディスク容量チェック	アップグレードプロセスを続行するための十分な空き領域がハードディスクにあるかどうかを確認します。
NTP の到達可能性と時刻源の確認	システムで設定されている NTP をチェックし、時刻源が NTP サーバーからのものかどうかを確認します。
負荷平均チェック	指定した間隔でシステムの負荷を確認します。指定できる間隔は、1、5、または 15 分です。
サービスまたはプロセスの失敗	サービスまたはアプリケーションの状態（実行中か障害状態か）を示します。

非アクティブなコンポーネントや失敗したコンポーネントがある場合、それらは赤色で表示されます。また、トラブルシューティング情報も表示されます。失敗したコンポーネントのアップグレードのシビラティ（重大度）に基づいて、アップグレードプロセスを続行できる場合と、アップグレードプロセスを進めるために問題を解決するように通知される場合があります。

[失敗したチェックの更新（Refresh Failed Checks）] オプションは、赤色で強調表示された障害のみを更新します。アップグレードを実行する前に、これらの障害を修正する必要があります。オレンジ色で強調表示された警告では、アップグレードプロセスは停止しません。ただし、アップグレード後に特定の Cisco ISE 機能に影響する可能性があります。各警告メッセージの横に表示される [更新（Refresh）] アイコンをクリックすると、問題の解決後にこれらのチェックが更新されます。

[展開して表示（Expand to Show）] アイコンをクリックすると、各ノードとそのステータスに関する追加情報が表示されます。

[情報（Information）] アイコンをクリックして、各コンポーネントの詳細を確認することもできます。

生成されたレポートのコピーを取得するには、[レポートのダウンロード（Download Report）] をクリックします。

アップグレードプロセスにかかる推定時間を確認できます。これは、次の情報に基づいて計算されます。

- Cisco ISE のインストール時間
- ノードのハードウェア仕様：プロセッサ、RAM、およびハードディスクの数
- データベースのデータサイズ
- ノードがアプリケーションサーバーを起動するのにかかった時間

Note [Bundle Download] と [Configuration Data Upgrade] を除くすべての事前チェックは、システムの検証を開始してから 3 時間後に自動的に期限切れになります。

ステップ 13 すべてのノードの事前チェックが完了したら、[ステージングを開始（Start Staging）] をクリックしてステージングプロセスを開始します。

[アップグレードのステージング（Upgrade Staging）] ウィンドウが開きます。

アップグレードのステージング中に、アップグレードされたデータベースファイルが反復で選択されたすべてのノードにコピーされ、反復で選択されたすべてのノードで構成ファイルがバックアップされます。

ノードのアップグレードステージングに成功した場合、緑色で表示されます。特定のノードのアップグレードステージングに失敗した場合は、赤色で表示されます。また、トラブルシューティング情報も表示されます。

[リフレッシュに失敗したノード（Refresh Failed Nodes）] アイコンをクリックして、失敗したノードのアップグレードステージングをもう一度開始します。

ステップ 14 [次へ（Next）] をクリックして [ノードのアップグレード（Upgrade Nodes）] ウィンドウに進みます。

[ノードのアップグレード（Upgrade Nodes）] ウィンドウで、全体的なアップグレードの進行状況と、展開内の各ノードのステータスを確認できます。

ステップ 15 [次へ（Next）] をクリックしてアップグレードプロセスを開始します。

アップグレードの進行状況は、プライマリ PAN のアップグレード中はセカンダリ PAN GUI から、セカンダリ PAN のアップグレード中はプライマリ PAN GUI からモニターできます。

Note このウィンドウで [ウィザードの終了（Exit Wizard）] オプションをクリックした場合、後で [概要（Summary）] ウィンドウを表示できません。

ステップ 16 [ノードのアップグレード（Upgrade Nodes）] ウィンドウで [次へ（Next）] をクリックして、すべてのノードが正常にアップグレードされたかどうかを確認します。

失敗したノードがある場合は、そのノードに関する情報を示すダイアログボックスが表示されます。

ステップ 17 [概要（Summary）] ウィンドウで、[終了（Finish）] をクリックします。

[Node Selection] ウィンドウにリダイレクトされ、次の反復のためにノードを選択できます。

ステップ 18 すべてのノードがアップグレードされるまで、ステップ 8 からステップ 18 のシーケンスに従って、次の反復を続行します。

プロセスの最初の反復を除くすべての反復で、[Configuration Data Dump Generation] 事前チェックが、[Configuration Data Upgrade] 事前チェックの代わりに実行されます。

分割アップグレードプロセスの実行中に展開のすべてのノードをアップグレードする必要はありません。任意の回数の反復後に停止できますが、管理シェルから CLI コマンドを **application configure ise** > **reset upgrade tables** の順に使用して新しい展開の**アップグレードテーブル**をクリアする必要があります。

アップグレードプロセスが完了したら、[概要（Summary）] ウィンドウで展開の診断アップグレードレポートを表示およびダウンロードできます。アップグレードされたノードの新旧ペルソナ、実行された事前チェック、および**アップグレードの準備**と**アップグレードレポート**のチェックリスト項目などの関連する詳細を含むアップグレード サマリー レポートを確認してダウンロードできます。

Cisco ISE 分割アップグレードを実行した場合、プロセス中にセカンダリ PAN はプライマリ PAN に昇格されます。Cisco ISE の管理者ポータルで、[Administration] > [Licensing] を選択します。[Cisco Smart

Licensing] エリアで、[Update] をクリックします。ライセンスを更新するまで、ライセンスアラームが Cisco ISE に表示されます。

へのアップグレード GUI からの Cisco ISE 展開の従来の分割アップグレード

Cisco ISE リリース 2.7、3.0、または 3.1から Cisco ISE リリース 3.2 への従来の分割アップグレードを実行できます。

Before you begin

「Prepare for Upgrade」の項の手順を必ず読んでください。

ステップ 1 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[管理（Administration）] > [システム（System）] > [アップグレード（Upgrade）]**の順に選択します。

ステップ 2 [続行（Proceed）] をクリックします。

ステップ 3 [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 4 [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 5 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。

a) 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。

b) [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。

c) 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。

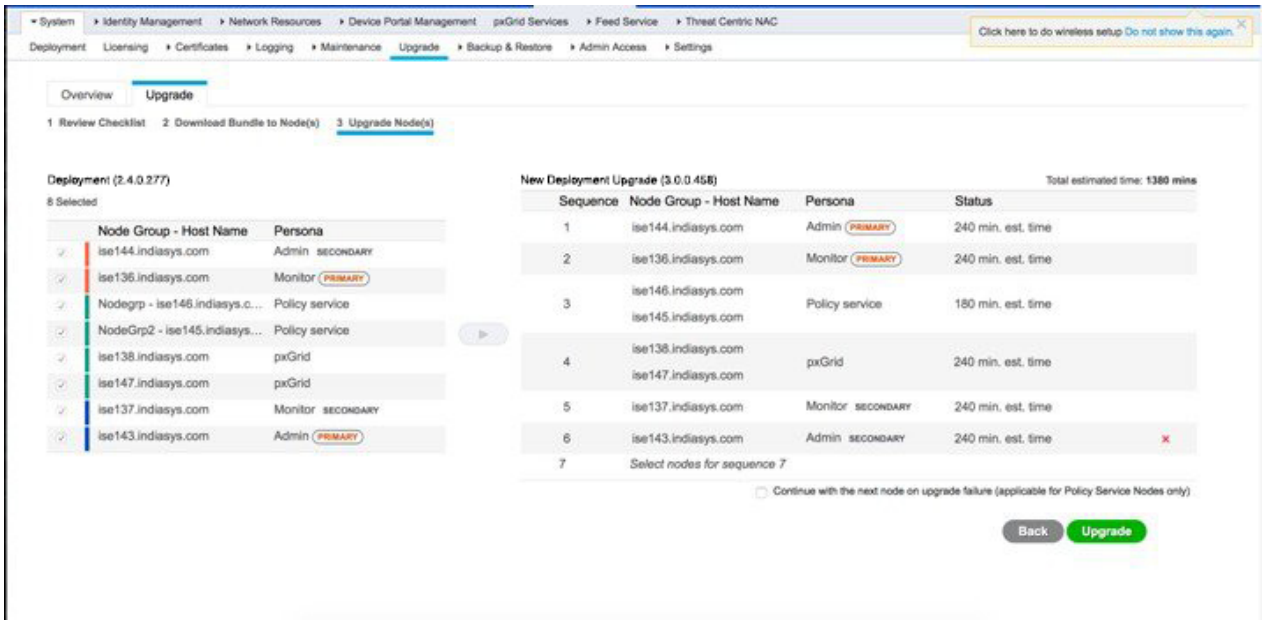
e) [確認（Confirm）] をクリックします。

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 6 [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。

Figure 5: 各ノードの選択したリポジトリを表示するアップグレードウィンドウ



ステップ 7 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。

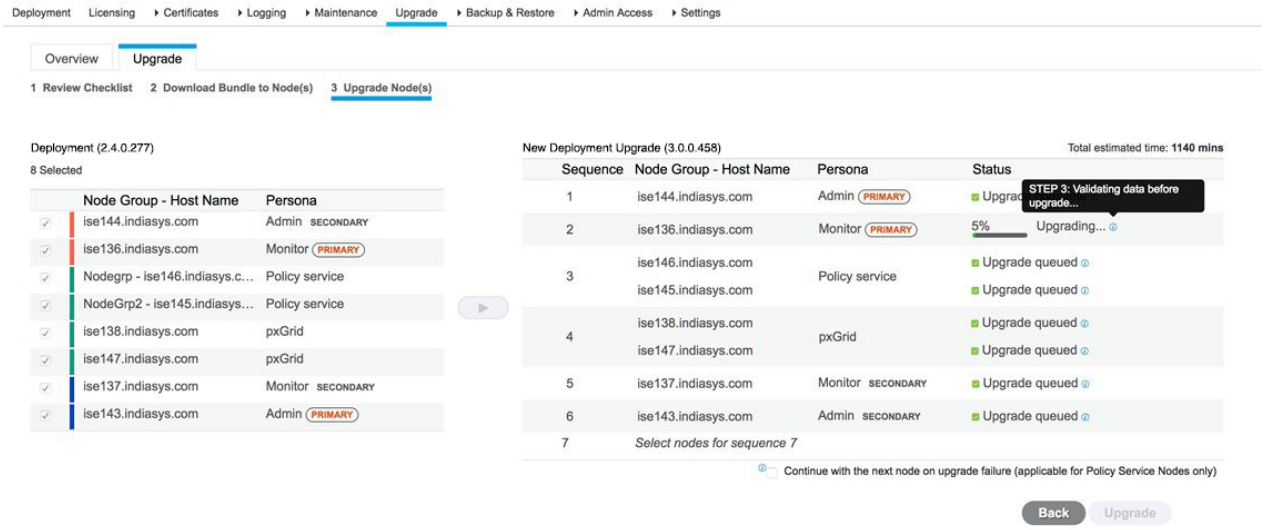
d) セカンダリ モニターリング ノードを選択し、新しい展開に移動します。
e) 最後に、プライマリ管理ノードを選択し、新しい展開に移動します。

ステップ 8 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、[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 9 [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。

Figure 6: アップグレードの進行状況を表示する *[*アップグレード（***Upgrade***）*]* ウィンドウ



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。

Note 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-yyyymmdd-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、[Upgrade] ウィンドウに移動し、[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。

Cisco ISE 分割アップグレードを実行した場合、プロセス中にセカンダリ PAN はプライマリ PAN に昇格されます。Cisco ISE の管理者ポータルで、[Administration] > [Licensing] を選択します。[Cisco Smart Licensing] エリアで、[Update] をクリックします。ライセンスを更新するまで、ライセンスアラームが Cisco ISE に表示されます。

Note 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か（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。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして、**[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。

Before you begin

「Prepare for Upgrade」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。

Example:

```
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 **Note** 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。

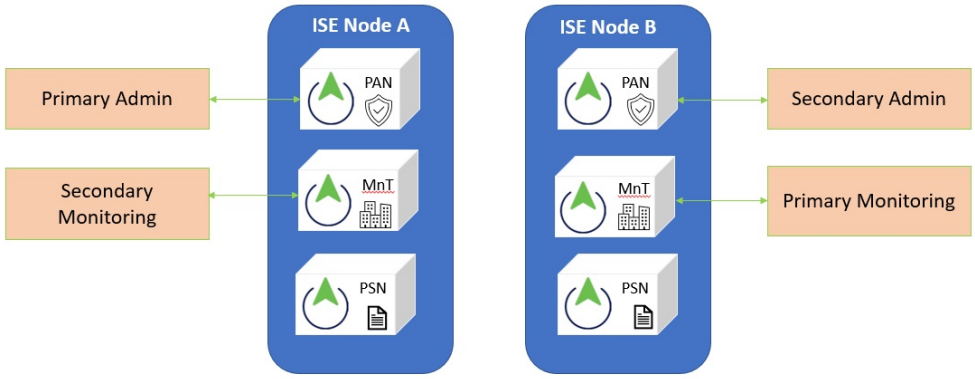
What to do next

アップグレードプロセスの確認, on page 57

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。

Figure 7: Cisco ISE 2 ノード管理展開



Before you begin

- 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。

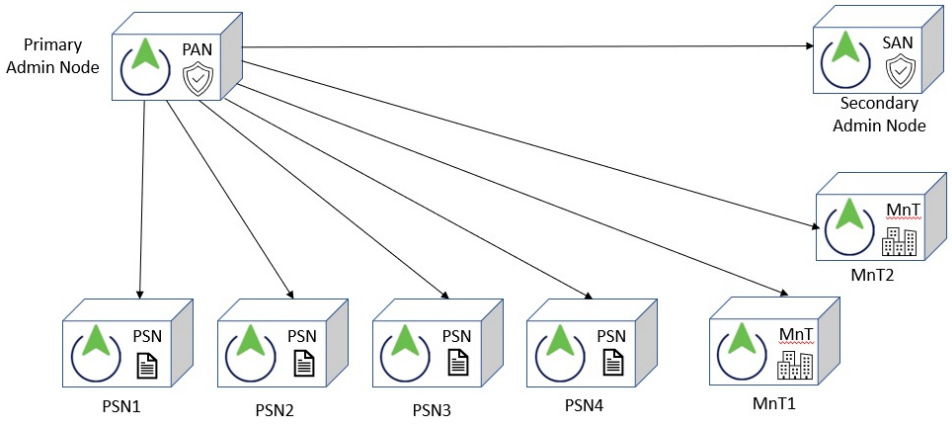
What to do next

アップグレードプロセスの確認, on page 57

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。

Figure 8: アップグレード前の ***Cisco ISE*** 展開



Note 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。

Before you begin

- 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。

- 「Prepare for Upgrade」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、ポリシーサービスモード（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。

What to do next

アップグレードプロセスの確認, on page 57

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.
```

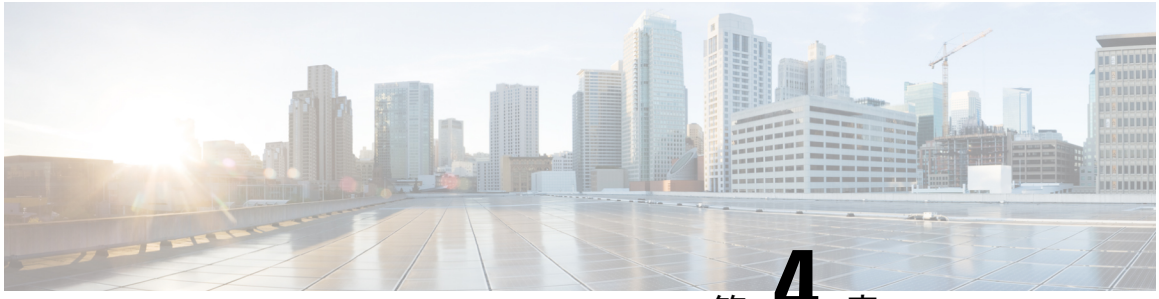
- **show version** コマンドを実行し、ビルドバージョンを検証します。
- **show application status ise** コマンドを入力して、すべてのサービスが実行されていることを確認します。

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

最新のパッチのインストール

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。Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、[管理（Administration）] > [システム（System）] > [メンテナンス（Maintenance）] > [パッチ管理（Patch Management）]。

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
```

関連トピック

ソフトウェア パッチ インストールのガイドライン （60 ページ）
ソフトウェア パッチ ロールバックのガイドライン （62 ページ）
ソフトウェアパッチのインストール （61 ページ）
ソフトウェアパッチのロールバック （61 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

Before you begin

- 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。
- Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[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 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[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。

Note 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 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[管理（Administration）] > [システム（System）] > [メンテナンス（Maintenance）] > [パッチ管理（Patch Management）]** を選択して、[パッチのインストール（Patch Installation）] ページに戻ります。

ステップ 5 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。

Before you begin

- 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 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[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。

Note 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。

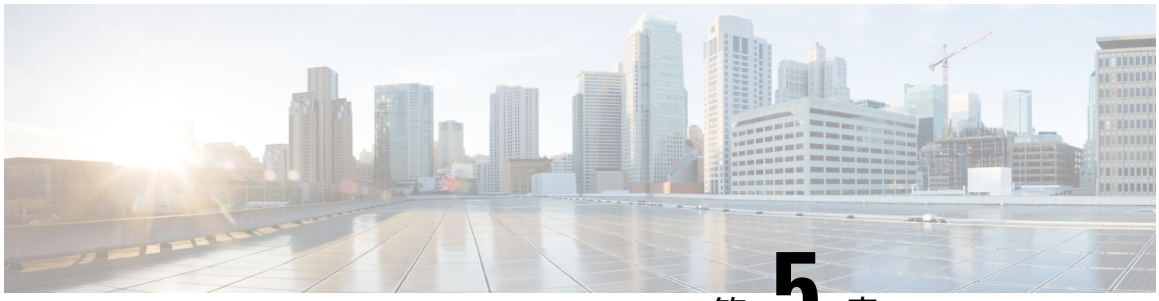
Before you begin

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、Cisco ISE GUI で [メニュー（Menu）] ア

イコン（☰）をクリックして、[管理（Administration）]>[システム（System）]>[メンテナンス（Maintenance）]>[パッチ管理（Patch Management）] ウィンドウ。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 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[操作（Operations）]** > **[レポート（Reports）]** > **[監査（Audit）]** > **[操作監査（Operations Audit）]**。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 iniated）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タスクの実行

展開のアップグレード後に、この章に記載されているタスクを実行します。

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。

新しいライセンスタイプへの変換

- Cisco Smart Software Manager（CSSM）を使用して、古いライセンスを新しいライセンスタイプに変換します。
- Cisco ISE 管理者のポータルで新しいライセンスを有効にします。

新しい Cisco ISE ライセンスタイプの詳細については、『Cisco ISE Administration Guide, Release 3.1』を参照してください。

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）8.4（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 以降は 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。

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、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て、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。 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[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

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
フルアップグレードプロセス	展開とスタンドアロ
分割アップグレードプロセス	展開とスタンドアロ

アップグレードのシナリオ	モード
構成データベースの復元プロセス	スタンドアロン
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
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

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。

SMNP 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 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 2 [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プ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 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、[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 [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 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、[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 3 [追加（Add）] をクリックします。

ステップ 4 [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 5 [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 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[ポリシー（Policy）]** > **[ポリシー要素（Policy Elements）]** > **[結果（Results）]** > **[認証（Authentication）]** > **[許可されるプロトコル（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。

Related Topics

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`

サプリカント 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、サプ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 サプリカント 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。

プロファイラエンドポイント所有権の同期/レプリケーション

Cisco ISE 2.7 以降のバージョンにアップグレードすると、JEDIS フレームワークの一部として、ポート 6379 を展開内のすべてのノード間で開いて双方向通信を行う必要があります。

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。