Cisco ISE 3.0 アップグレードガイド：アップグレード方法

初版：2023 年 7 月 11 日

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 （20 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
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

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、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 *1 : 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 2.4 以降	Cisco ISE 2.4 以降	Cisco ISE 2.4 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
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 [Menu] アイコン（☰）をクリックして、次の順に選択します。 **[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。

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 2.4 以降を使用している場合は、Cisco ISE リリース 3.0 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 3.0 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 3.0 への参加
- プライマリ PAN および MnT の Cisco ISE リリース 3.0 へのアップグレード

Cisco ISE リリース 3.0 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 3.0 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 3.0 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 MnT ノードの Cisco ISE リリース 3.0 へのアップグレード

手順

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 3.0 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 3.0 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 3.0 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。

手順

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 3.0 の最新パッチに再イメージ化し、新しい Cisco ISE リリース 3.0 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 3.0 へのアップグレード

手順

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 [Menu] アイコン（☰）をクリックして、次の順に選択します。 **[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。

リリース 2.4、2.6 または 2.7からリリース 3.0 へのアップグレード

始める前に

「Prepare for Upgrade」の項の手順を必ず読んでください。

手順

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

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。

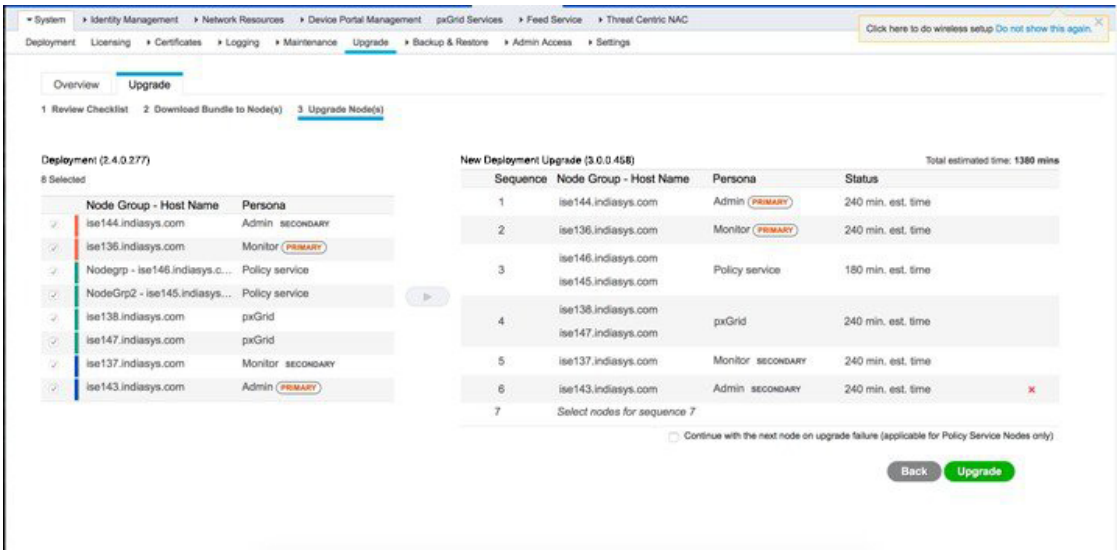
e) [確認（Confirm）] をクリックします。

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。

図 *1*: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。

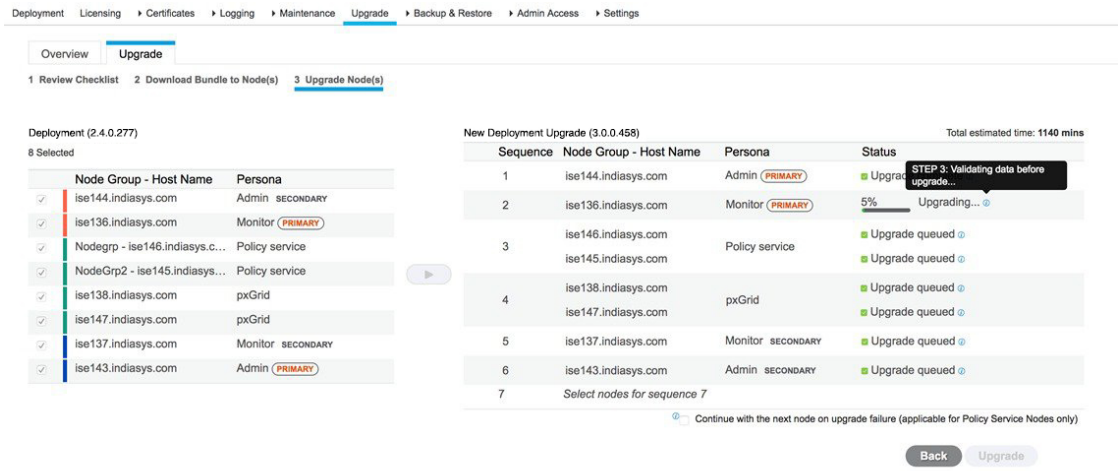
d) セカンダリ モニタリング ノードを選択し、新しい展開に移動します。
e) 最後に、プライマリ管理ノードを選択し、新しい展開に移動します。

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。

図 *2:* 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。

（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-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。

（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（☰）をクリックして選択します **[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。

始める前に

「Prepare for Upgrade」の項の手順を必ず読んでください。

手順

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。

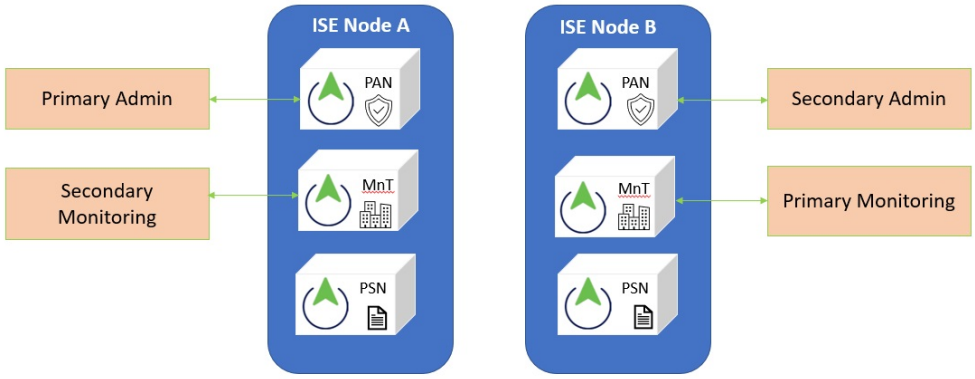
次のタスク

アップグレードプロセスの確認 （20 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。

図 *3 : Cisco ISE 2* ノード管理展開



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。

手順

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。

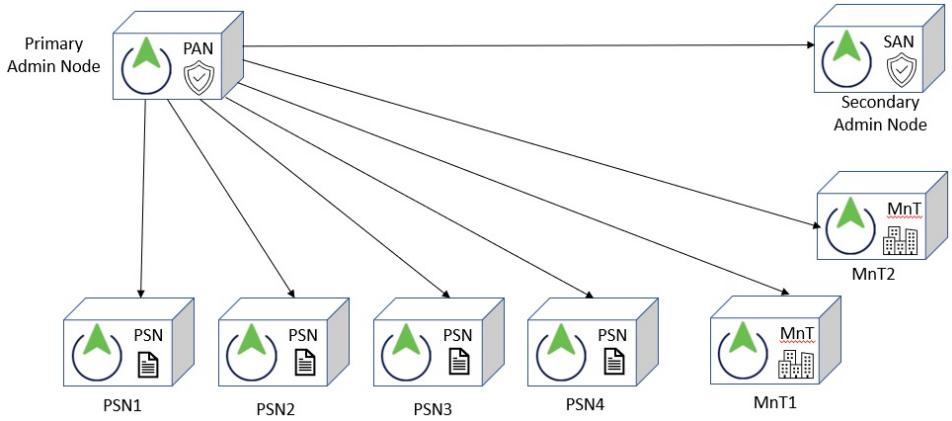
次のタスク

アップグレードプロセスの確認 （20 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 *4:* 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。

- 「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。

手順

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。

次のタスク

アップグレードプロセスの確認 （20 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。

手順

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。

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。