

# アップグレード プロセス

## ノードのアップグレードの順序

GUI（推奨）、バックアップおよび復元メソッド、または CLI を使用して Cisco ISE をアップグレードできます。GUI（推奨）を使用してアップグレードする場合、ノードのアップグレード順序を選択できます。推奨される順序でノードをアップグレードすることで、ダウンタイムを最小限に抑え、復元力を最大化することができ、必要に応じてロールバックをシンプル化できます。

### アップグレード前のタスク

アップグレードを開始する前に、次のタスクを完了してください。

- すべての設定およびモニタリングデータをバックアップします。
- 内部 CA キーと証明書チェーンをエクスポートします。
- すべての Cisco ISE ノードのサーバー証明書をバックアップします。

### 推奨されるアップグレード順序

次の順序でノードをアップグレードします。

#### 1. SAN

この時点では、PAN 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。

#### 2. 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、SAN があるサイトで使用可能なノードをアップグレードします。

#### 3. PSN

- GUI を使用して以前の Cisco ISE リリースから最近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 のグループを選択して、全体的なダウンタイムを短縮できます。
- 一連の PSN セットをアップグレードした後、アップグレードの成功を確認してから（[アップグレードプロセスの確認, on page 26](#)を参照）、新しい展開が想定どおりに機能していることを確認するネットワークテストを実行します。テストに成功したら、次の PSN セットに進みます。

#### 4. 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

#### 5. PAN

PAN 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。

- PAN の登録時にアップグレードが失敗すると、システムによってロールバックが開始され、ノードがスタンダアロンモードに変更されます。CLI を使用してノードをスタンダアロンとしてアップグレードしてから、SAN として新しい展開に登録します。
- アップグレード後、SAN は PAN になり、元の PAN が SAN 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 SAN を PAN にします。

## 複数のペルソナを持つノードのアップグレードシーケンス

管理ノードにモニタリングペルソナも設定されている場合は、現在の展開内のノードペルソナに基づいて、以下のアップグレードシーケンスを使用します。

**Table 1:** ノードのペルソナとそのアップグレードシーケンス

| 展開内のノードペルソナ                                   | アップグレードの順序                                                                                                                         |
|-----------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| SAN/プライマリ モニタリング ノード、PSN、PAN/セカンダリ モニタリング ノード | <ol style="list-style-type: none"><li>1. SAN/プライマリ モニタリング ノード</li><li>2. PSN</li><li>3. PAN/セカンダリ モニタリング ノード</li></ol>             |
| SAN/セカンダリ モニタリング ノード、PSN、PAN/プライマリ モニタリング ノード | <ol style="list-style-type: none"><li>1. SAN/セカンダリ モニタリング ノード</li><li>2. PSN</li><li>3. PAN/プライマリ モニタリング ノード</li></ol>             |
| SAN、プライマリ モニタリング ノード、PSN、PAN/セカンダリ モニタリング ノード | <ol style="list-style-type: none"><li>1. SAN</li><li>2. プライマリ モニターリング ノード</li><li>3. PSN</li><li>4. PAN/セカンダリ モニタリング ノード</li></ol> |
| SAN、セカンダリ モニタリング ノード、PSN、PAN/プライマリ モニタリング ノード | <ol style="list-style-type: none"><li>1. SAN</li><li>2. セカンダリ モニターリング ノード</li><li>3. PSN</li><li>4. PAN/プライマリ モニタリング ノード</li></ol> |
| SAN/プライマリ モニタリング ノード、PSN、セカンダリ モニタリング ノード、PAN | <ol style="list-style-type: none"><li>1. SAN/プライマリ モニタリング ノード</li><li>2. PSN</li><li>3. セカンダリ モニターリング ノード</li><li>4. PAN</li></ol> |
| SAN/セカンダリ モニタリング ノード、PSN、プライマリ モニタリング ノード、PAN | <ol style="list-style-type: none"><li>1. SAN/セカンダリ モニタリング ノード</li><li>2. PSN</li><li>3. プライマリ モニターリング ノード</li><li>4. PAN</li></ol> |

## 一般的なアップグレードの問題: 「No SAN in the Deployment (展開内に SAN がありません)」

以下の状況では、「No SAN in the Deployment (展開内に SAN がありません)」というエラーメッセージが表示されることがあります。

- 展開内に設定されている SAN が存在しない。
- SAN がダウンしている。
- SAN がアップグレードされ、アップグレード済みの展開に移動された（たとえば、[展開の詳細の更新 (Refresh Deployment Details)] オプションの使用後）。

### 解決手順

この問題を解決するには、次のいずれかのタスクを実行します。

- 展開内に SAN がない場合は、SAN を設定してからアップグレードを再試行します。
- SAN がダウンしている場合は、そのノードを起動してからアップグレードを再試行します。
- SAN がアップグレードされ移動されている場合は、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

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基づいて、アップグレードプロセスを選択できます。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。

- [GUI を使用したアップグレード \(推奨\)](#)
- [バックアップおよび復元メソッドを使用したアップグレード \(Cisco ISE リリース 3.2 パッチ 2 に限定\)](#)
- [CLI を使用したアップグレード](#)

次の表に、Cisco ISE のアップグレードメソッドの比較を示します。

**Table 2: Cisco ISE のアップグレードメソッドの比較**

| 比較要素    | GUIを使用したアップグレード (推奨) | バックアップと復元を使用したアップグレード (Cisco ISE リリース 3.2 パッチ 2 に限定) | CLIを使用したアップグレード |
|---------|----------------------|------------------------------------------------------|-----------------|
| プロセスタイプ | 時間がかかる               | 高速                                                   | 時間がかかる          |
| 管理作業が必要 | 少ない                  | 多い                                                   | 多い              |
| 難易度     | 容易                   | 困難                                                   | 適度              |

| 比較要素        | GUIを使用したアップグレード（推奨）              | バックアップと復元を使用したアップグレード（Cisco ISE リリース 3.2 パッチ 2 に限定）         | CLIを使用したアップグレード               |
|-------------|----------------------------------|-------------------------------------------------------------|-------------------------------|
| VM          | 各 PSN は並行してアップグレードされる。           | 十分なキャパシティがある場合は、新しい VM を事前ステージングして、新しい PAN にすぐに参加させることができる。 | 各 PSN はアップグレードされるが、並行して実行できる。 |
| アップグレード時間   | 少ない（各 PSN は並行してアップグレードされるため）。    | 最も少ない（PSN はアップグレードされずに新しいバージョンでイメージ化されるため）。                 | 少ない（各 PSN は並行してアップグレードされるため）。 |
| 人員の要件       | アップグレードプロセスが自動化されるため、手動介入は少なくなる。 | 設定と運用のログをやりとりする複数事業部門の関係者。                                  | Cisco ISE に関する技術力が必要。         |
| ロールバックオプション | 容易                               | 難しい（ノードの再イメージ化が必要）                                          | 容易                            |

GUIまたはCLIを使用したアップグレードでは、アップグレードに固有のサポートバンドルが自動的に生成されます。リポジトリが到達可能で書き込み可能な場合、サポートバンドルは、アップグレードバンドルをホストするのと同じリポジトリに保存します。リポジトリに到達できない場合、または書き込みできない場合、サポートバンドルは、ローカルディスクに保存します。このサポートバンドルは、アップグレードに失敗した際のトラブルシューティングに使用できます。

## GUIを使用したアップグレード (推奨)

### 概要

Cisco ISE リリース 3.2 パッチ 3 以降では、GUI を介したアップグレードが推奨される方法です。

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。アップグレードを実行するには、以下の手順に従います。

1. Cisco ISE GUI で、**[管理（Administration）]>[システム（System）]>[アップグレードおよびロールバック（Upgrade & Rollback）]**に移動します。
2. 新しいリポジトリを作成して、アップグレードバンドルをダウンロードします。



### Note

この方法は、Oracle Cloud Infrastructure（OCI）、Amazon Web Services（AWS）、Azure Cloud Services などのクラウドプラットフォームではサポートされていません。

## GUIを使用してアップグレードする理由 (推奨)

この方法は、Cisco ISE リリース 3.2 パッチ 3 またはの からアップグレードする場合に推奨されます。

GUI（推奨）方式を使用してアップグレードすべき理由は、次のとおりです。

- アップグレード中、セカンダリ PAN がアップグレードされた展開に自動的に移動して、最初にアップグレードされ、次にプライマリ MnT がアップグレードされます。その結果、これらのアップグレードのいずれかが失敗した場合、ノードを以前のバージョンにロールバックして、以前の Cisco ISE 展開に再参加する必要があります。複数の PSN を一括で選択し、同時にアップグレードできます。
- 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は技術力が不要なため、管理者 1 人でアップグレードを開始できます。その後、アップグレードステータスの監視と報告を行ったり、TAC ケースを開いたりする NOC または SOC エンジニアを割り当てることができます。

## 利点

GUI メソッドを使用して Cisco ISE リリース 3.2 パッチ 3 以降のバージョンからアップグレードすると、次のような利点があります。

- 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。

## アップグレード前の主な考慮事項

GUI を使用して Cisco ISE リリース 3.2 パッチ 3 以降のバージョンからアップグレードする前に、次の点を考慮してください（推奨）。

- **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 URT 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。多数の PSN を順番にアップグレードすると、プロセスに膨大な時間がかかります。段階的にアップグレードすると、全体の所要時間が短縮されます。

## アップグレードプロセスのベストプラクティス

次に、GUI を使用した Cisco ISE リリース 3.2 パッチ 3 以降のバージョンからのアップグレード（推奨）に関するベストプラクティスのリストを示します。

- 多数の PSN がある場合は、それらをバッチにグループ化します。各バッチを個別にアップグレードします。
- 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。
- ノードがアクティブ状態の場合にのみ、アップグレードを開始します。

Cisco ISE GUI で、**[管理 (Administration)] > [システム (System)] > [アップグレード (Upgrade)] > [概要 (Overview)]** に移動します。この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を示す）が一覧表示されます。

## 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、**[管理 (Administration)] > [システム (System)] > [アップグレード (Upgrade)] > [アップグレードを選択 (Upgrade Selection)]** ページ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
- 分割アップグレード

### Note

GUI ベースのアップグレードオプションを使用して Cisco ISE をアップグレードする場合は、次の点を考慮してください。

- Cisco ISE リリース 3.2 以降では、分割アップグレード方式で URT と UI の両方の事前チェックを使用する必要があります。フルアップグレード方法の場合、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以前のリリース以降から利用できますが、Cisco ISE 3.2 以降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 を実行する必要があります。
- GUI または CLI アップグレードオプションを介して別のアップグレードが進行中の間は、CLI を使用してノードにパッチをインストールまたはロールバックしないでください。

## フルアップグレード

フルアップグレードは、次のような複数ステップのプロセスです。

- すべての Cisco ISE ノードを同時にアップグレードします。
- 分割アップグレードプロセスよりも速くアップグレードを完了します。
- すべてのノードが並行してアップグレードされるため、アプリケーションサービスを使用できなくなります。
- Cisco ISE リリースがサポートされます。

フルアップグレード オプションを使用して Cisco ISE をアップグレードするには、次の手順を実行します。

1. アップグレードの開始, on page 7
2. 事前チェックの開始, on page 7
3. ステージングプロセスの開始, on page 10

## アップグレードの開始

Cisco ISE 展開のアップグレードを開始するには、次の手順を実行します

- Step 1** Cisco ISE GUI で、[管理（Administration）]>[システム（System）]>[アップグレードおよびロールバック（Upgrade & Rollback）]に移動します。
- Step 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）]をクリックします。
- Step 3** [初期化（Initialize）]をクリックします。
- Step 4** [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。
- Step 5** 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。
- Step 6** 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）]（オプション）をクリックします。
- Step 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ます。[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。

## 事前チェックの開始

Cisco ISE 展開の事前チェックを開始するには、次の手順を実行します。

- Step 1** [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。
- Step 2** [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。
- Step 3** 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 リリースのパッチを選択します。
- Step 4** [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。

アップグレードプロセス中、Cisco ISE は複数のチェックを実行します。

| 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チェックします。 |

| 事前チェックリスト          | 説明                                                                                                                                                                                               |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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。アップグレードを開始する前に、PAN の高可用性 (HA) が無効になることを示す通知が表示されます。                                                                                                           |
| スケジュールバックアップの確認    | <p>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。</p> <div>  <p>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。</p> </div> <p><b>Note</b></p> |
| 構成のバックアップの確認       | 構成のバックアップが直前に正常に完了し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た後に開始できます。                                                                                                                                 |
| 構成データのアップグレード      | データベースのクローンで構成データをアップグレードし、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 | 展開にサポートされているプラットフォームを使用しているかどうかを確認します。システムは、ハードウェアが少なくとも 12 コア以上の CPU、300 GB のハードディスク、および 16 GB のメモリを備えており、ESXi バージョン 6.5 以降を使用していることを確認します。                                                     |
| 展開の検証              | 展開のノードが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 アドレスの順方向ルックアップと逆方向ルックアップの両方が正しく機能していることを確認します。                                                                                                                                          |
| 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が適切に検証されているかどうかを確認します。                                                                                                                                                               |

| 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できるように、ハードディスクに十分な空き領域が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 | NTP を設定しているかどうかを確認し、時間送信元が NTP サーバーであることを確認します。     |
| 負荷平均チェック          | 指定した間隔でシステムの負荷をチェックします。頻度は、1 分、5 分、または 15 分に設定できます。 |
| 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が実行中か失敗したかを示します。                     |

コンポーネントが非アクティブまたは失敗した場合、システムはそのコンポーネントを赤色で表示します。障害対応の提案が表示されます。コンポーネント障害の重大度に応じて、アップグレードプロセスを続行できる場合と、続行する前に問題を解決する必要がある場合があります。

| フィールド                        | 説明                                                                                                                                                                                          |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Refresh Failed Checks</b> | このオプションは、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、これらの障害を解決する必要があります。オレンジで強調表示されている警告は、アップグレードを妨げませんが、後で Cisco ISE の機能に影響を与える可能性があります。各警告の横の [更新 (Refresh)] アイコンをクリックすると、問題の解決後にチェックがアップデートされます。 |
| <b>Expand to Show</b>        | この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。                                                                                                                                                 |
| <b>Information</b>           | この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。                                                                                                                                                      |
| <b>Download Report</b>       | 生成されたレポートのコピーを取得するには、このオプションをクリックします。                                                                                                                                                       |

Cisco ISE は、展開をステージングおよびアップグレードするために必要な推定時間を表示します。計算には次の要因を使用します。

- ネットワーク速度
- プロセッサ、RAM、およびハードディスクの数などのノードの構成
- データベース 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った時間



**Note**

[バンドルダウンロード (Bundle Download)] と [構成データのアップグレード (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。

## ステージングプロセスの開始

Cisco ISE 展開のステージングプロセスを開始するには、次の手順を実行します。

**Step 1** 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、システムはアップグレードされたデータベースファイルをすべてのノードにコピーします。また、システムは各ノード上の構成ファイルもバックアップします。

ノードのアップグレードステージングに成功した場合、システムはそのノードを緑色で表示します。ノードのアップグレードステージングが失敗すると、システムはそのノードを赤色で表示し、障害対応の提案を提供します。

[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。

**Step 2** [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)] ウィンドウには、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が表示されます。

**Step 3** [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、次のメッセージが表示されます。

システムはまもなくアップグレードされます。Logging out)」というポップアップが表示されます。

**Step 4** [OK] をクリックして続行します。



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。

### Note

セカンダリ PAN のダッシュボードを使用して、プライマリ PAN のアップグレードステータスを監視します。プライマリ PAN のアップグレード後、プライマリ PAN ダッシュボードを使用してすべての Cisco ISE ノードを監視します。

アップグレードプロセスをモニターするには、アクティブな Cisco ISE 階層ライセンスが必要です。アップグレードプロセスを表示するには、Cisco ISE 評価ライセンスで十分です。アップグレードプロセスを表示および監視できるのは、有効なライセンスがある場合のみです。詳細については、『Cisco ISE Administrator Guide, Release 3.5』の「[Licensing](#)」の章を参照してください。



後で[概要 (Summary)] ウィンドウを表示する場合、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ないでください。

### Note

**Step 5** [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。

いずれかのノードが失敗した場合、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。

**Step 6** 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あと、[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。次のような詳細を含むアップグレード概要レポートを検証してダウンロードします。

- 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
- システム正常性チェックリスト項目

## GUI からの分割アップグレード

分割アップグレードは、次のようなマルチステッププロセスです。

- 他のサービスを利用可能な状態のままで、Cisco ISE 展開をアップグレードします。
- ネットワークまたはロードバランサを更新して、ノードを認証に使用できるようにします。
- ノードをバッチに分割し、各バッチを順番にアップグレードすることで、分割アップグレードのダウンタイムを限定できます。
- 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 以降へのアップグレードに使用できます。

Cisco ISE リリース 3.2 パッチ 3 以降のリリースでは、新しい分割アップグレードフレームワークが導入され、安定性が向上し、ダウンタイムが短縮されました。

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。このプロセスにより、アップグレード時間が短縮され、データアップグレードの問題が原因でシステムが使用できなくなるのを防ぎます。
- セカンダリ PAN を使用する最初の反復中、またはプライマリ PAN を使用する最後の反復中に、PSN および MnT ノードを選択できます。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。
- PSN と MnT ノードを同じ反復内で選択すると、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。

分割アップグレードを使用して Cisco ISE をアップグレードするには、次の手順を実行します。

1. [アップグレードの準備, on page 11](#)
2. [準備を開始, on page 12](#)
3. [ステージングを開始, on page 15](#)

### アップグレードの準備

分割アップグレードの準備をするには、次の手順を実行します。

- Step 1** Cisco ISE GUI で、[管理（Administration）]>[システム（System）]>[アップグレード（Upgrade）]に移動します。
- Step 2** [アップグレードを選択（Upgrade Selection）] ウィンドウで、[分割アップグレード（Split Upgrade）] をクリックします。警告メッセージが表示されます。アップグレードタイプを分割アップグレードに変更すると、事前チェックレポートが消去されるというメッセージが表示されます。また、メッセージには [事前チェック実行（Precheck Execution）] および [ステージングノード（Staging Nodes）] ステージング中も、ISE サービスは動作し続けるとも記載されています。[OK] をクリックして作業を続行します。
- Step 3** [アップグレードを開始（Start Upgrade）] をクリックします。
- Step 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。
- Step 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、[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。
- Step 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。
- Step 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ます。次に、[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。

- Step 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。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、最初の反復またはその後の反復でプライマリ PAN を選択することはできません。最初の反復では、プライマリ MnT、セカンダリ MnT、および任意の数の PSN を選択できます。
- 最初の反復でセカンダリ PAN 以外のノードを選択すると、アップグレードは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ます。残りの選択したノードは、次のバッチで同時にアップグレードされます。
- 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ノード以下を選択することをお勧めします。

- Step 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。

## 準備を開始

分割アップグレードの準備を開始するには、次の手順を実行します。

- Step 1** [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 リポジトリを使用する場合は、CLI を使用してすべてのノードに暗号ホストキーを追加してください。

**Step 2**

[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します。

**Step 3**

[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、最初の反復の間のプライマリ 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。以降の反復の間は、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。

**Table 3:** 次の表で、各事前チェックとそれに対応する機能について説明します。

| 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チェックします。                                                                                                                          |
| 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。                                                                           |
| パッチバンドルのダウンロード   | 選択したノードのパッチバンドルをダウンロードします。                                                                                                                                  |
| PAN のフェールオーバーの検証 | PAN の高可用性 (HA) が有効になっているかどうかを確認します。<br><br>アップグレードが開始する前に、PAN の高可用性 (HA) が無効になることを示す通知を受け取ります。                                                              |
| 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。<br><br> 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直前に正常に完了したかどうかを確認します。アップグレードは、バックアップの完了後のみ実行されます。                                                                        |
| 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 コア以上の 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を確認します。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 NTP が設定されているかどうかを確認し、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           | 指定された間隔（1 分、5 分、または 15 分）でシステム負荷をチェックします。                                                                                          |
| 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。障害対応の提案が表示されます。障害が発生したコンポーネントがアップグレードにとって不可欠な場合は、続行する前に問題を解決してください。それ以外の場合は、アップグレードを続行できます。

**Table 4:** 次の表で、各フィールドとそれに対応する機能について説明します。

| フィールド                        | 説明                                                                                                                                                                                                                   |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Refresh Failed Checks</b> | このオプションは、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。オレンジで強調表示されている警告は、アップグレードを停止するものではありませんが、アップグレード後の Cisco ISE の機能に影響を与え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。 |
| <b>Expand to Show</b>        | この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を確認できます。                                                                                                                                                                          |
| <b>Information</b>           | 各コンポーネントの詳細を表示するには、このアイコンをクリックします。                                                                                                                                                                                   |
| <b>Download Report</b>       | 生成されたレポートのコピーを取得するには、このオプションをクリックします。                                                                                                                                                                                |

アップグレードにかかる推定時間を確認できます。システムは、次を使用して推定アップグレード時間を決定します。

- 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。

最初の反復時に、すべてのノードでローカル事前チェックが実行されます。ただし、後続の反復では、これらのチェックが選択したノードでのみ実行されます。

## ステージングを開始

ステージングプロセスを開始するには、次の手順を実行します。

**Step 1** 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内のすべてのノードにコピーされます。また、システムはこれらのノード上の構成ファイルもバックアップします。

ノードのアップグレードのステージングが成功すると、緑色のインジケータが表示されます。特定のノードのアップグレードのステージングが失敗すると、赤色のインジケータが表示されます。障害対応の提案も表示されます。

[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。

**Step 2** [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。

**Step 3** [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**

アップグレードプロセスをモニターするには、アクティブな Cisco ISE 階層ライセンスが必要です。アップグレードプロセスを表示するには、Cisco ISE 評価ライセンスで十分です。アクティブなライセンスが存在しない場合、アップグレードプロセスを表示またはモニターすることはできません。Cisco ISE ライセンスの詳細については、リリースに対応する『Cisco ISE Administrator Guide』の「Licensing」の章を参照してください。

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、後から [概要 (Summary)] ウィンドウを表示することはできません。

**Step 4** [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。

**Step 5** [概要 (Summary)] ウィンドウで、[終了 (Finish)] をクリックします。

[ノード選択 (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。

**Step 6** すべてのノードがアップグレードされるまで、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、[構成データダンプ生成 (Configuration Data Dump Generation)] 事前チェックが、[構成データのアップグレード (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中に、展開内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。任意の回数反復後に停止できます。ただし、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。アップグレードサマリーレポートには、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 (Prepare to Upgrade) とアップグレードの準備 (Prepare to Upgrade) のチェックリスト項目などの関連する詳細が含まれます。

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。

## バックアップと復元を使用したアップグレード（Cisco ISE リリース 3.2 パッチ 2 に限定）

### 概要

バックアップと復元による方法は、Cisco ISE リリース 3.2 パッチ 2 までの Cisco ISE リリースで推奨されます。

Cisco ISE ノードの再イメージ化は、初期展開および障害対応時に実行されます。Cisco ISE リリース 3.2 パッチ 2 またはそれ以前のバージョンへのアップグレードでは、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。この場合、新しいバージョンのインストール後に、新しい展開にポリシーを復元できます。

リソースが制限されていて、新しい展開で並列の Cisco ISE ノードをサポートできない場合、セカンダリ PAN と MnT が実稼働展開から削除され、他のノードより前にアップグレードされます。その後、ノードは新しい展開に移動されます。設定と運用のバックアップは、以前の展開から各ノードに復元され、1つの並列展開が作成されます。このプロセスにより、手動で操作せずに、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。

### Important

バックアップおよび復元アップグレードメソッドは、すべての Cisco ISE リリースとパッチでサポートされています。ただし、3.2 パッチ 2 以前の Cisco ISE リリースでは、バックアップおよび復元メソッドがプライマリ アップグレードメソッドとして推奨されていました。このメソッドでは、既存の展開の設定と運用のバックアップが作成され、それらが新しい展開で復元されます。この操作は、データ損失を防止し、ノード設定を復元するのに役立ちます。

3.2 パッチ 2 よりも新しい Cisco ISE バージョンでは、バックアップおよび復元メソッドは引き続きサポートされていますが、代わりに GUI ベースのアップグレードメソッドが推奨されています。GUI ベースのアップグレードでは、バックアップおよび復元に比べてモニタリングが改善され、アップグレードプロセスが高速化されるなど、機能が強化されています。

新しいバージョンでのアップグレード中に VM 障害や問題が発生した場合のリカバリには、ノードの再イメージ化や、GUI または CLI アップグレードメソッドでサポートされるロールバック手順の使用が含まれます。

### バックアップと復元を使用してアップグレードする理由

シスコでは、Cisco ISE リリース 3.2 パッチ 2 までのリリースでは、バックアップと復元による方法を推奨しています。この手順を開始するには、既存の Cisco ISE 展開の設定と運用のバックアップを作成し、新しい展開に適用するからです。

この方法は、現在の Cisco ISE 展開ノードの設定を復元し、アップグレード中に問題が発生した場合にデータの損失を防ぐのに役立ちます。

### 利点

バックアップおよび復元方式（Cisco ISE リリース 3.2 パッチ 2 までの利用を推奨）を使用した Cisco ISE のアップグレードには、次のような利点があります。

- 以前の Cisco ISE 展開から設定と運用ログを復元できます。これにより、データ損失を防止できます。
- 新しい展開に再利用するノードを選択できます。
- 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。

## アップグレード前の主な考慮事項

バックアップおよび復元方式を使用して Cisco ISE をアップグレードする前に、これらの考慮事項を確認してください（Cisco ISE リリース 3.2 パッチ 2 以降を推奨）。

- **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追加のリソースが必要です。リリースする前に、Cisco ISE 展開用にこれらのリソースを予約してください。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間で追加の負荷を分散させる必要があります。そのため、展開する前に現在の負荷と遅延の制限を評価してください。この評価により、展開でノードあたりのユーザー数の増加をサポートできるようになります。
- **人員の要件：** アップグレードを実行するには、複数の事業部門からのリソースが必要です。これらの部門には、ネットワーク管理、セキュリティ管理、データセンター、および仮想化の各チームが含まれます。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再参加させて、ポリシーの同期を待機する必要があります。これらのアクションにより、複数のリロードが行われ、新規展開の場合と同様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：** ノードを再イメージ化すると、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、再度ノードを再イメージ化するのと同じ手順に従います。

## アップグレードプロセスのベストプラクティス

このセクションでは、バックアップおよび復元方式を使用して Cisco ISE をアップグレードするためのベストプラクティスを示します（Cisco ISE リリース 3.2 パッチ 2 までを推奨）。

- 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できます。次に、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します。
- 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。

### Note

---

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。

---

## RSA設定ファイルの生成とインポート

RSA 構成ファイルを生成してインポートするには、次の手順を実行します。

1. プライマリ RSA Authentication Manager セキュリティ コンソール 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。

### Note

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 Cisco ISE と RSA Authentication Manager の間で共有するのに役立ちます。

3. 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します。

## プロセスの概要

このセクションでは、バックアップおよび復元メソッドを使用する場合の Cisco ISE のアップグレード手順を示します。

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します。ノードの登録解除や削除の詳細については、『*Cisco ISE Administrator Guide, Release 3.5*』の「[Remove a Node from Deployment](#)」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、まず展開からそのノードを削除した後に Cisco ISE をインストールします。Cisco ISE のインストールの詳細については、『*Cisco ISE Administrator Guide, Release 3.5*』の「[Install Cisco ISE](#)」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 リリースに最新のパッチを適用します。

3. **バックアップと復元:** 設定または運用データベースをバックアップおよび復元します。バックアップと復元操作の詳細については、『*Cisco ISE Administrator Guide, Release 3.5*』の「[Backup and Restore Operations](#)」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ロールを割り当てます。モニタリングおよび障害対応 (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 ISE Administrator Guide, Release 3.5*』の「[Manually Modify MnT Role](#)」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 として登録します。PSN の登録や参加の詳細については、『*Cisco ISE Administrator Guide, Release 3.5*』の「[Register a Secondary Cisco ISE Node](#)」セクションを参照してください。

### Note

バックアップおよび復元メソッドを使用して 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 に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します。Cisco ISE ノードへのシステム証明書のインポートの詳細については、『*Cisco ISE Administrator Guide, Release 3.5*』の「[Import a System Certificate](#)」セクションを参照してください。

## アップグレードプロセス

現在 Cisco ISE リリース 3.2 以降を使用している場合は、Cisco ISE リリース 3.5 に直接アップグレードできます。

使用している Cisco ISE バージョンが、Cisco ISE リリース 3.5 と互換性がない場合は、

1. 最初に、Cisco ISE リリース 3.5 と互換性のある中間バージョンにアップグレードしてから、
2. 中間バージョンから Cisco ISE リリース 3.5 にアップグレードする必要があります。

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。

### ステージ 1: 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 3.2、3.3 または 3.4 へのアップグレード

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。

- Step 1** セカンダリ PAN ノードを登録解除します。
- Step 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 PAN にします。
- Step 3** バックアップデータから Cisco ISE の設定を復元します。
- Step 4** セカンダリ MnT ノードを登録解除します。
- Step 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。
- Step 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。
- Step 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。

### ステージ 2: セカンダリ PAN および MnT ノードの Cisco ISE リリース 3.5 へのアップグレード

- Step 1** Cisco ISE の構成設定と運用ログをバックアップします。
- Step 2** セカンダリ PAN ノードを登録解除します。
- Step 3** 登録解除されたセカンダリ PAN ノードを Cisco ISE リリース 3.5 に再イメージ化します。
- Step 4** バックアップデータから Cisco 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に設定します。
- Step 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。
- Step 6** セカンダリ MnT ノードを登録解除します。
- Step 7** 登録解除されたセカンダリ MnT ノードを Cisco ISE リリース 3.5 に再イメージ化します。
- Step 8** 現在の Cisco ISE 運用バックアップを復元し、新しい展開のプライマリ MnT としてノードを追加します。

古いログからレポートを生成する必要がある場合にのみ、このオプションの手順を実行します。

### ステージ 3: PSN の Cisco ISE リリース 3.5 への参加

複数のサイトに展開されている Cisco ISE ノードがある場合は、次のことを行う必要があります。

1. セカンダリ PAN および MnT ノードを含むサイトで PSN に参加
2. 他のサイトで PSN に参加
3. 既存の Cisco ISE のプライマリ PAN および MnT ノードがあるサイトで、PSN に参加

PSN を Cisco ISE リリース 3.5 に参加させるには、次の手順を実行します。

**Step 1** PSN を登録解除します。

**Step 2** PSN を Cisco ISE リリース 3.5 の最新パッチに対して再イメージ化し、新しい Cisco ISE リリース 3.5 展開に参加させます。

#### What's 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、ログが存在することを確認し、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。

### ステージ 4: プライマリ PAN および MnT を Cisco ISE リリース 3.5 にアップグレードします。

プライマリ PAN および MnT を新しい Cisco ISE リリースにアップグレードするには、次の手順を実行します。

**Step 1** プライマリ MnT ノードを再イメージ化し、セカンダリ MnT として新しい展開に参加させます。  
レポート用のデータを保持するには、運用バックアップをセカンダリ MnT ノードに復元します。

**Step 2** プライマリ PAN ノードを再イメージ化し、セカンダリ PAN として新しい展開に参加させます。

## CLI を使用したアップグレード

### 概要

CLI から Cisco ISE にアップグレードするには、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、アップグレードを実行し、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似ていますが、このアプローチはモニタリングと操作の点で運用の負荷が高いです。

Cisco ISE を CLI からアップグレードすることは複雑な場合があります。この方法は多大な労力を必要とするため、CLI アップグレードは障害対応の目的でのみ使用してください。

### この方法からアップグレードする利点

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。

- アップグレードするノードをより細かな制御のうえで選択して、並行して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、追加の負荷を対処します。
- 以前の変更を元に戻すことがスクリプトに指示できるため、CLI で簡単にロールバックできます。
- 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がなくなります。

## アップグレード前の主な考慮事項

CLI メソッドを使用して Cisco ISE をアップグレードする前に、次の点を考慮する必要があります。

- CLI を使用して Cisco ISE をアップグレードするには、技術的な専門分野と更なる作業時間が必要です。
- 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

スタンドアロン ノードをアップグレードするには、次の 2 つの手順のいずれかを実行します。

- 次のコマンドを直接入力します。

```
application upgrade <upgrade bundle name> <repository name>
```

- 次の 2 つのコマンドを指定された順序で入力します。

```
application upgrade prepare <upgrade bundle name> <repository name>
```

```
application upgrade proceed
```

管理、ポリシーサービス、pxGrid、およびモニタ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。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ます。アップグレードバンドルをローカルディスクに保存すると、アップグレードに必要な時間が短縮されます。

また、次の手順を実行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。

- 次のコマンドを実行して、アップグレードバンドルをダウンロードし、ローカルに抽出します。

```
application upgrade prepare <upgrade bundle name> <repository name>
```

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。

- プロセスを正常に完了するには、アップグレード用のノードの準備後に次のコマンドを実行します。

```
application upgrade proceed
```

このセクションで説明するとおりに **application upgrade prepare <upgrade bundle name> <repository name>**、および **application upgrade proceed** コマンドを実行します。

「Prepare for Upgrade」の項の手順を必ず読んでください。

**Step 1** 次のコマンドを CLI に入力します。

```
application upgrade prepare <upgrade bundle name> <repository name>
```

**Step 2** SSH経由でログインし、 **show application status ise** コマンドを使用してアップグレードの進行状況を表示します。

次のメッセージが表示されます。「% NOTICE: Identity Services Engine upgrade is in progress...」

**Step 3** **application upgrade proceed** コマンドを入力します。

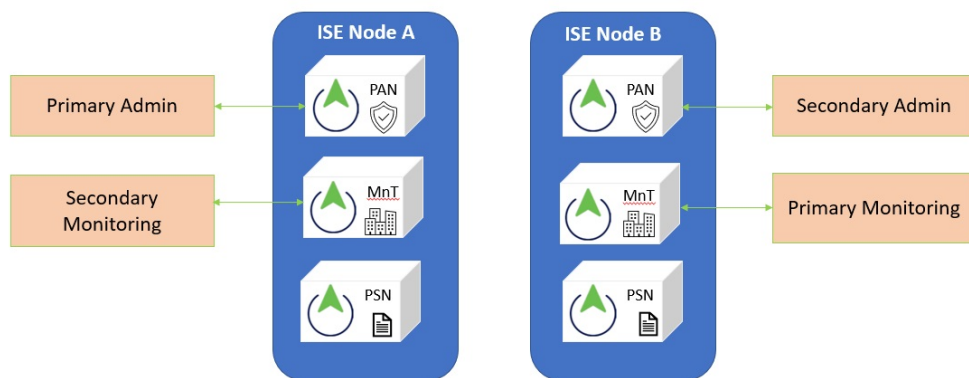
## 2 ノード展開のアップグレード

次の 2 つの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。

1. `application upgrade prepare <upgrade bundle name> <repository name>`
2. `proceed`

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、新しい展開に追加します。2 ノード展開をアップグレードする場合は、まず SAN（ノード B）のみをアップグレードします。セカンダリノードのアップグレードを完了した後、プライマリノード（ノード A）をアップグレードします。こ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 1: Cisco ISE 2 ノード管理展開**



- PAN から設定および運用データの手動バックアップを実行します。
- 管理とモニタリングのペルソナを、展開の両方のノードで有効にします。

PAN でのみ管理ペルソナが有効になっている場合は、セカンダリノードで管理ペルソナを有効にします。最初に SAN をアップグレードする必要があります。

2 ノード展開に管理ノードが 1 つのみの場合は、セカンダリノードの登録を解除します。各ノードはスタンドアロンノードとして動作します。各スタンドアロンノードをアップグレードし、アップグレード後に展開を再度設定します。

- モニタリングペルソナが 1 つのノードのみで有効になっている場合は、次に進む前に他のノードのモニタリングペルソナを有効にします。

**Step 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。

**Step 2** 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。

**Step 3** 新しい展開で、ノード A をプライマリノードに昇格させます。

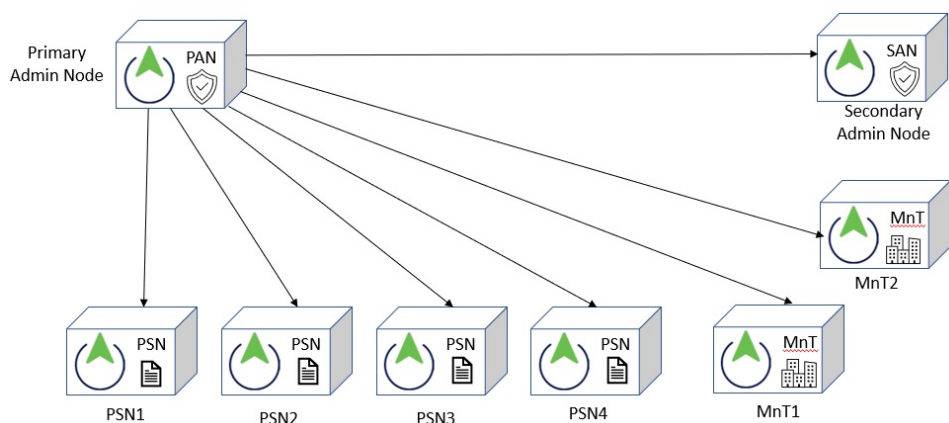
アップグレードが完了した後、ノードに古いモニタリングログが含まれる場合、これらのノード上でコマンドを実行し、5（データベースの統計情報の更新）を選択します。

```
application configure ise
```

## 分散展開のアップグレード

初めに、SAN を新しいリリースにアップグレードする必要があります。たとえば、この図に示すように、1 つの PAN、1 つの SAN、4 つの PSN、1 つのプライマリ モニタリング ノード（MnT1）、および 1 つのセカンダリ モニタリング ノード（MnT2）を含む展開がセットアップされている場合、このアップグレード手順に進むことができます。

**Figure 2:** 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。次の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。

1. `application upgrade prepare <upgrade bundle name> <repository name>`
2. `proceed`

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。アップグレード前にノードの登録を手動で解除する場合は、アップグレードを開始する前に PAN ライセンスファイルがあることを確認してください。このファイルがない場合（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など）、Cisco Technical Assistance Center（TAC）に連絡してください。

展開の完全性を維持し、ダウンタイムを最小限に抑えてスムーズにアップグレードするには、次の手順を実行します。

- 展開に SAN がない場合は、アップグレードプロセスを開始する前に、SAN にする PSN を 1 つ設定します。
- このガイド（『Cisco ISE アップグレードジャーニー、リリース 3.5』）の「[アップグレードの準備](#)」の章に記載されている手順を読み、その手順に従っていることを確認します。
- 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。

## Step 1 CLI からSANをアップグレード

- SAN ノードの CLI からアップグレードを開始します。
- アップグレードプロセスで、自動的に SAN が以前の展開から登録解除され、アップグレードされます。
- 再起動時に、SAN が新しい展開のプライマリノードになります。
- 各展開には少なくとも 1 つのモニタリングノードが必要です。そのため、アップグレードにより、以前に有効化されていなかった場合でも SAN でモニタリングペルソナが有効になります。
- ポリシーサービスペルソナが以前の展開の SAN で有効であった場合、アップグレード後も維持されます。

## Step 2 モニタリングノード（MnT1 および MnT2）をアップグレード

- モニタリングノードの 1 つを新しい展開にアップグレードします。
- 以前の展開で PAN がプライマリ モニタリング ノードとしても機能している場合、セカンダリ モニタリング ノードの前にプライマリ モニタリング ノードをアップグレードすることはできません。それ以外の場合は、最初にプライマリ モニタリング ノードをアップグレードします。
- プライマリ モニタリング ノードは、PAN ダッシュボードからアクセスできる新しい展開からログの収集を開始します。
- 以前の展開にモニタリングノードが 1 つだけ存在する場合は、アップグレード前に PAN でモニタリングペルソナを有効にします。



### Note

ノードのペルソナを変更すると、Cisco ISE アプリケーションが再起動します。続行する前に、ノードがオンラインに戻るまで待機してください。

- 運用データの移行のため、モニタリングノードのアップグレードには時間がかかります。
- 新しい展開の PAN で以前にモニタリングペルソナが有効になっていない場合は、そのノードで無効になります。これにより、アプリケーションの再起動もトリガーされます。

## Step 3 PSNのアップグレード

- 次に、PSN をアップグレードします。
- 複数の PSN を並行してアップグレードできますが、すべてを同時にアップグレードするとネットワークのダウンタイムを引き起こす場合があります。

- アップグレード後、PSN は新しい展開のプライマリノード（SAN）に登録されます。
- PSN ではそのペルソナ、ノードグループ情報、およびブローブのプロファイリング設定が維持されます。

#### Step 4 セカンダリ モニタリング ノードをアップグレード（該当する場合）

- セカンダリ モニタリング ノードが以前の展開に存在する場合は、次の手順を実行します。
  - 以前の展開のプライマリノードである PAN のモニタリングペルソナを有効にします。各展開には少なくとも1つのモニタリングノードが必要なため、これは必須です。ペルソナの変更により、アプリケーションが再起動します。ノードがオンラインに戻るまで待機してください。
  - セカンダリ モニタリング ノードを以前の展開から新しい展開にアップグレードします。
  - この手順の前に、PAN を除くすべてのノードがアップグレードされていることを確認してください。

#### Step 5 PAN をアップグレード

- 最後に PAN をアップグレードします。
- アップグレード後、PAN は SAN として新しい展開に参加します。
- 必要に応じて、この SAN をプライマリノードに昇格できます。
- アップグレード後、モニタリングノードに以前のログが含まれている場合は、次のコマンドを実行します。  
**application configure ise**
- それらのノードでオプション 5（データベース統計の更新）を選択します。

#### アップグレードプロセスの確認

アップグレードが完了したら、展開が正しく機能していることを確認することが重要です。ネットワークテストを実行して、想定どおりに 認証およびアクセスできることを確認します。

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、システムは自動的に変更をロールバックします。

アップグレードが成功したことを確認するには、以下の手順を使用します。

#### Step 1 ade.log ファイルを確認して、アップグレードの進行状況を確認します。ログを表示するには、Cisco ISE CLI から次のコマンドを使用します。

```
show logging system ade/ADE.log.?
```

キーワード STEP を使用して、アップグレード手順のログをフィルタ処理できます。ログには次のような進行状況が表示されます。

- 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...
- 次の文字列のログを検索して、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.

**Step 2** 次のコマンドを入力して、ビルドバージョンを確認します。

**show version**

**Step 3** 次のコマンドを入力して、すべての Cisco ISE サービスが実行されていることを確認します。

**show application status ise**

## 以前のバージョンへのロールバック

Cisco ISE アプライアンスを再イメージ化する必要があるまれなケースでは、以前の 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必要があります。データを復元したら、以前の展開にアプライアンスを登録できます。以前の展開と同じ状態になるように、ペルソナを有効にします。アップグレードプロセスを開始する前に、Cisco ISE 設定およびモニタリングデータをバックアップすることが重要です。

設定およびモニタリングデータベースの問題が原因で、アップグレードが失敗することがあります。このような場合、システムは自動的にロールバックされません。こうなった場合、システムにはデータベースがロールバックされなかったことを示す通知が表示され、アップグレード失敗メッセージが示されます。そうしたら、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、設定データおよびモニタリングデータ（モニタリングペルソナが有効な場合）を復元する必要があります。

ロールバックまたは回復を実行する前に、**backup-logs** コマンドを使用してサポートバンドルを生成し、リモートリポジトリに保存します。このサポートバンドルは、障害対応に使用でき、必要に応じて Cisco Technical Assistance Center (TAC) に送信できます。

## 翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。