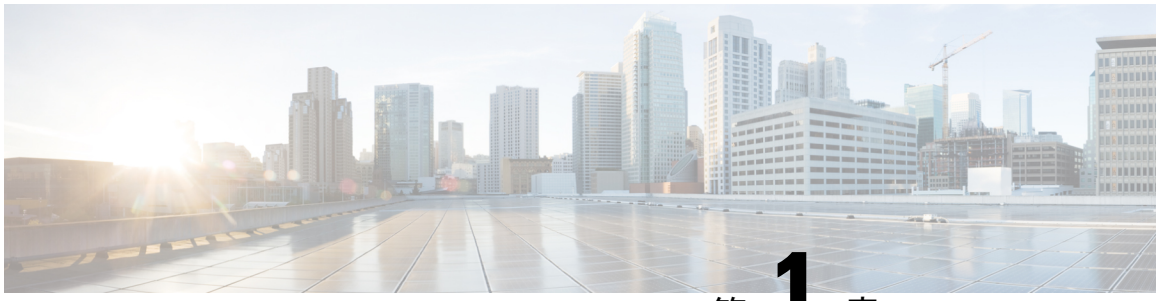
Cisco Identity Services Engine リリース 2.6 アップグレード ガイド

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 ISE 展開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。最小限のダウンタイムでのアップグレードを計画するには、このマニュアルで示されている推定所要時間を使用します。PSN グループに複数の PSN を含む展開では、ダウンタイムはありません。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あった場合は、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 アクセスが付与されます。

スタンドアロン展開または PSN が単一の展開の場合は、PSN のアップグレード中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。

次のリリースはすべて、リリース 2.6 に直接アップグレードできます。

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

（注） Cisco ISE リリース 2.3 以降では、すべてのネットワーク アクセス ポリシーとポリシー セットを置き換える、新しい拡張された [ポリシーセット（Policy Sets）] ページが提供されます。以前のリリースからリリース 2.3 以降にアップグレードすると、すべてのネットワーク アクセス ポリシーの設定（認証および承認の条件、ルール、ポリシー、プロファイル、および例外を含む）が ISE GUI の新しい [ポリシーセット（Policy Sets）] 領域に移行されます。変更の詳細については、新規ポリシー モデル （4 ページ） を参照してください。

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

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

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

Cisco ISE のこのリリースでは、GUI ベースおよび CLI ベース両方のアップグレードをサポートします。

GUI または CLI を使用してアップグレードするかどうかに関係なく、可能な限り最小のダウンタイムで、最大の復元力とロールバックの機能を提供しながら、展開をアップグレードするには、次の順序でアップグレードを実行することをお勧めします。

1. 必要に応じて手動で簡単にロールバックできるようにするため、アップグレード開始前に設定とモニタリングのすべてのデータをバックアップします。
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 モニタリング ノード
4. ポリシー サービス ノード

   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 （48 ページ）を参照）、新しい展開が期待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。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 モニタリング ノード
6. プライマリ管理ノード

（注） 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。

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（古い展開と同様）。

ライセンスの変更

デバイス管理ライセンス

Cisco ISE 2.3 以前のバージョンでは、展開でのデバイス管理ノードの数にかかわらず、展開ごとに Device Administration 永久ライセンスが必要です。Cisco ISE 2.4 以降、デバイス管理ライセンスの数は、展開でのデバイス管理ノード（デバイス管理サービス用に設定された PSN）の数と同じである必要があります。

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

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

VM ノードのライセンス

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

VM ライセンスは、小、中、大の 3 つのカテゴリで提供されます。たとえば、8 コアと 64 GB RAM を備えた 3595 相当の VM ノードを使用している場合に、VM で同じ機能をレプリケートするには、中カテゴリの VM ライセンスが必要になります。展開の要件に応じて、VM とそのリソースの数に基づいて、複数の VM ライセンスをインストールできます。

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

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

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

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

次の表は、VM 最小リソースをカテゴリ別に示しています。

VM カテゴリ	RAM の範囲	CPU の数
小	16 GB	12 個の CPU
中	64 GB	16 個の CPU
大	256 GB	16 個の CPU

ライセンスの詳細については、『*Cisco Identity Services Engine Administrator Guide*』の「Cisco ISE Licenses」の章を参照してください。

新規ポリシー モデル

認証、承認、例外を含め、すべてのネットワーク アクセス ポリシーおよびポリシーセットは、Cisco ISE 2.3 以降では [ポリシー（Policy）] > [ポリシーセット（Policy Sets）] からアクセスすることができる [ポリシーセット（Policy Sets）] エリアの下に統合されます。各ポリシー セットは、ポリシー階層の最上位レベルで定義されたコンテナであり、その下にそのセットのすべての関連する認証および許可ポリシーおよびポリシー例外ルールが設定されます。

すべて条件に基づいて、認証と許可の両方に複数のルールを定義できます。また、条件とその他の関連設定に簡単にアクセスして、新しいポリシー セット インターフェイスから直接再利用できるようになりました。ポリシーセットが照合される順序は、新しいインターフェイスに表示される順序によって決定され、[ポリシーセット（Policy Set）] テーブルの最初の行から開始され、一致が見つかるまでチェックが続行されます。一致するものが見つからない場合は、システムのデフォルト ポリシー セットが使用されます。同じ論理を使用して正しい認証ルールの照合と選択が行われ、次に正しい許可ルールの照合と選択が行われます。各テーブルの先頭から開始し一致が見つかるまで各ルールがチェックされます。一致する他のルールがない場合は、デフォルト ルールが使用されます。

新しいポリシー モデルは、古いユーザ インターフェイスを使用して以前のバージョンで追加された可能性のあるすべてのポリシーを表しますが、ネットワーク アクセスを論理的に管理できる大幅に簡素化された改良済みのインターフェイスが提供されます。

スタンドアロンの認証および許可ポリシーの変更

スタンドアロンの認証ルールを使用する場合、ISE 2.2 以下のバージョンからのルールは新しいポリシー モデルに変換されます。認証ルールに割り当てられている許可されたプロトコルに基づいて、2 つの個別のシナリオがあります。

1. システム内のすべての「外部パート」に、デフォルト パートを含む同じ許可されたプロトコルが割り当てられている場合、すべての元の認証ルールは次のように変換されます。

   すべての「外部パート」は、新しいポリシー モデルの単一のポリシー セットに変換されます。新しいポリシー セットはデフォルトと呼ばれ、ポリシー セット レベルでは条件が定義されず、統一された許可プロトコルが割り当てられます。すべての内部パートは、新しいデフォルト ポリシー セット内の認証ポリシーの一部としてルールに変換されます。

   次の表に、同じ許可されたプロトコルを使用する古いスタンドアロン認証ルールのセットの変換を示します（シナリオ 1）。この表では、各行の形式は次のとおりです。

名前（条件/結果）

たとえば認証外部パート 1（外部条件/許可されるプロトコル A）の場合：

- 名前：認証外部パート 1
- 条件：外部条件
- 結果：許可されるプロトコル A

表 *1*: 同じ許可されたプロトコルを使用したスタンドアロン認証ポリシー

Cisco ISE 2.3 より前：デフォルト認証	Cisco ISE 2.3 以降へのアップグレード後：ポリシー セット
1. 認証外部パート1（外部条件1/許可されるプロトコル A） **1.** 認証内部パート1.1（内部条件1.1/ID ストア A） **2.** 認証内部パート1.2（内部条件1.2/ID ストア A） **3.** 認証内部パート1.3（内部条件1.3/ID ストア A） **4.** 認証内部1デフォルト（条件なし/ID ストア B） **2.** 認証外部パート2（外部条件2/許可されるプロトコル A） **1.** 認証内部パート2.1（内部条件2.1/ID ストア A） **2.** 認証内部パート2.2（内部条件2.2/ID ストア A） **3.** 認証内部パート2.3（内部条件2.3/ID ストア A） **4.** 認証内部2デフォルト（条件なし/ID ストア B） **3.** 認証外部パート3（外部条件3/許可されるプロトコル A） **1.** 認証内部3デフォルト（条件なし/ID ストア B） **4.** デフォルト認証外部パート（条件なし/許可されるプロトコル A/デフォルト ID ストア） **5.** 例外 1 **6.** 許可ルール 1 **7.** 許可ルール 2	

Cisco ISE 2.3 より前：デフォルト認証	Cisco ISE 2.3 以降へのアップグレード後：ポリシー セット
	1. デフォルト（条件なし/許可されるプロトコル A） 1. 認証ポリシー（コンテナ） 1. 認証外部パート 1：認証内部パート 1.1（外部条件 1 + 内部条件 1.1/ID ストア A） 2. 認証外部パート 1：認証内部パート 1.2（外部条件 1 + 内部条件 1.2/ID ストア A） 3. 認証外部パート 1：認証内部パート 1.3（外部条件 1 + 内部条件 1.3/ID ストア A） 4. 認証外部パート 1：認証内部 1 デフォルト（外部条件 1/ID ストア B） 5. 認証外部パート 2：認証内部パート 2.1（外部条件 2 + 内部条件 2.1/ID ストア A） 6. 認証外部パート 2：認証内部パート 2.2（外部条件 2 + 内部条件 2.2/ID ストア A） 7. 認証外部パート 2：認証内部パート 2.3（外部条件 2 + 内部条件 2.3/ID ストア A） 8. 認証外部パート 2：認証内部 2 デフォルト（外部条件 2/ID ストア B） 9. 認証外部パート 3：認証内部 3 デフォルト（外部条件 3/ID ストア B） 10. デフォルト認証外部パート（条件なし/デフォルト ID ストア） 2. 例外 1 3. 許可ポリシー（コンテナ）

Cisco ISE 2.3 より前：デフォルト認証	Cisco ISE 2.3 以降へのアップグレード後：ポリシー セット
	1. 許可ルール 1 2. 許可ルール 2

2. システム内の「外部パート」の少なくとも 1 つに、デフォルト パートなどの他の部分とは異なる許可されたプロトコルが割り当てられている場合、すべての元の認証ルールは次のように変換されます。

   各「外部パート」は、新しいポリシー モデルの個別のポリシー セットに変換されます。新しいポリシーセットは、その特定の新しいセットの元の外部パートの名前に基づいて名前が付けられます。各ポリシー セットのポリシー セット レベルでは、元の外部パートの条件と許可されたプロトコルが割り当てられます。各外部パートのすべての内部パートは、新しいポリシー セット内の認証ポリシーの一部として 1 対 1 で認証ルールに変換されます。

   次の表に、異なる許可されたプロトコルを使用する古いスタンドアロン認証ルールのセットの変換を示します（シナリオ 2）。この表では、各行の形式は次のとおりです。

   名前（条件/結果）

   たとえば認証外部パート 1（外部条件/許可されるプロトコル A）の場合：

   - 名前：認証外部パート 1
   - 条件：外部条件
   - 結果：許可されるプロトコル A

表 *2:* 異なる許可されたプロトコルを使用したスタンドアロン認証ポリシー

Cisco ISE 2.3 より前：デフォルト認証	Cisco ISE 2.3 以降へのアップグレード後：ポリシー セット
1. 認証外部パート 1（外部条件 1/許可されるプロトコル A） **1.** 認証内部パート 1.1（内部条件 1.1/ID ストア A） **2.** 認証内部パート 1.2（内部条件 1.2/ID ストア A） **3.** 認証内部パート 1.3（内部条件 1.3/ID ストア A） **4.** 認証内部 1 デフォルト（条件なし/ID ストア B） **2.** 認証外部パート 2（外部条件 2/許可されるプロトコル B） **1.** 認証内部パート 2.1（内部条件 2.1/ID ストア A） **2.** 認証内部パート 2.2（内部条件 2.2/ID ストア A） **3.** 認証内部パート 2.3（内部条件 2.3/ID ストア A） **4.** 認証内部 2 デフォルト（条件なし/ID ストア B） **3.** 認証外部パート 3（外部条件 3/許可されるプロトコル C） **1.** 認証内部 3 デフォルト（条件なし/ID ストア B） **4.** デフォルト認証外部パート（条件なし/許可されるプロトコル A/ID ストア C） **5.** 例外 1 **6.** 許可ルール 1 **7.** 許可ルール 2	

Cisco ISE 2.3 より前：デフォルト認証	Cisco ISE 2.3 以降へのアップグレード後：ポリシー セット
	1. デフォルト認証外部パート 1（外部条件 1/許可されるプロトコル A） 1. 認証ポリシー（コンテナ） 1. 認証内部パート 1.1（内部条件 1.1/ID ストア A） 2. 認証内部パート 1.2（内部条件 1.2/ID ストア A） 3. 認証内部パート 1.3（内部条件 1.3/ID ストア A） 4. 認証内部 1 デフォルト（条件なし/ID ストア B） 2. 例外 1 3. 許可ポリシー（コンテナ） 1. 許可ルール 1 2. 許可ルール 2 1. デフォルト認証外部パート 2（外部条件 2/許可されるプロトコル B） 1. 認証ポリシー（コンテナ） 1. 認証内部パート 2.1（内部条件 2.1/ID ストア A） 2. 認証内部パート 2.2（内部条件 2.2/ID ストア A） 3. 認証内部パート 2.3（内部条件 2.3/ID ストア A） 4. 認証内部 2 デフォルト（条件なし/ID ストア B） 2. 例外 1 3. 許可ポリシー（コンテナ） 1. 許可ルール 1 2. 許可ルール 2

Cisco ISE 2.3 より前：デフォルト認証	Cisco ISE 2.3 以降へのアップグレード後：ポリシー セット
	1. デフォルト認証外部パート 3（外部条件 3/許可されるプロトコル C） 1. 認証ポリシー（コンテナ） 1. 認証内部 3 デフォルト（条件なし/ID ストア B） 2. 例外 1 3. 許可ポリシー（コンテナ） 1. 許可ルール 1 2. 許可ルール 2 1. デフォルト（条件なし/許可されるプロトコル A） 1. 認証ポリシー（コンテナ） 1. デフォルト認証ルール（条件なし/ID ストア C） 2. 例外 1 3. 許可ポリシー（コンテナ） 1. 許可ルール 1 2. 許可ルール 2

ポリシー セットの変更

以前のバージョンから Cisco ISE 2.3 以降にアップグレードする場合、表示される新しいポリシーセットはここで説明する古いISEバージョンの場合とは異なりますが、動作はまったく同じままです。

次の図は、Cisco ISE 2.3 以降へのアップグレード後のポリシーセットの変更を示しています。

図 *1 : ISE 2.3* より前：ポリシー セット

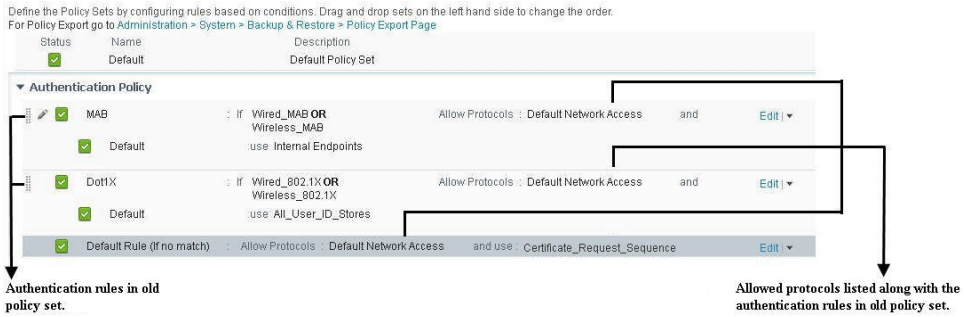
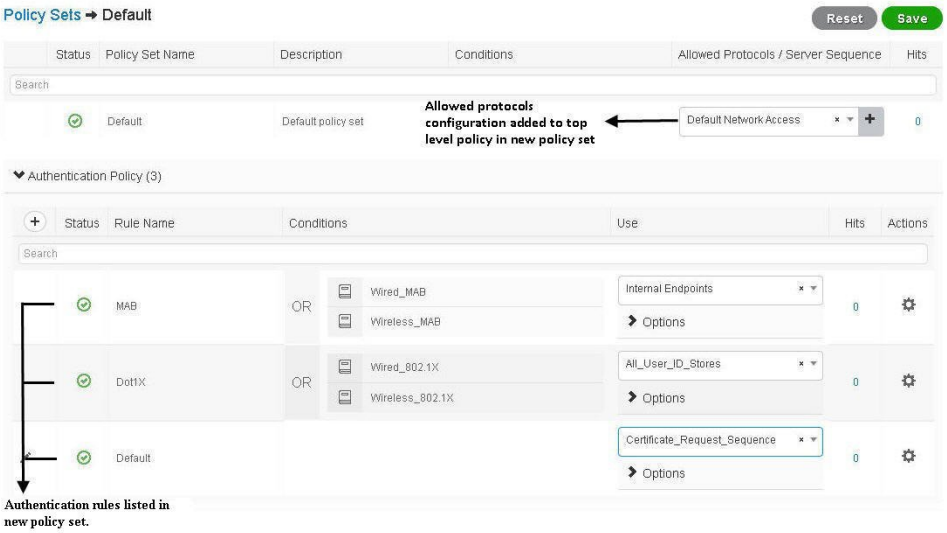


図 *2 : ISE 2.3* から：ポリシー セット



ISE 2.2 以下のバージョンからのポリシーは、新しいポリシー モデルに変換されます。認証ルールに割り当てられている許可されたプロトコルに基づいて、2 つの個別のシナリオがあります。

1. 単一のポリシー セット内のすべての「外部パート」に同じ許可されたプロトコルが割り当てられている場合、元のポリシー セットはすべて次のように変換されます。

   - すべての「外部パート」は、新しいポリシー モデルの単一のポリシー セットに変換されます。新しいポリシー セットは、元のポリシー セットと同じ名前になります。たとえば、古いモデルでポリシー セットの名前が「全従業員」になっている場合、新しいモデルでも「全従業員」と呼ばれます。

     次の表に、同じ許可されたプロトコルを使用する認証ルールを含む古いポリシー セットの変換を示します（シナリオ 1）。この表では、各行の形式は次のとおりです。

     名前（条件/結果）

たとえば認証外部パート 1（外部条件/許可されるプロトコル A）の場合：

- 名前：認証外部パート 1
- 条件：外部条件
- 結果：許可されるプロトコル A

表 *3 :* 同じ許可されたプロトコルを使用したポリシー セットの変換

Cisco ISE 2.2 以前からの古いポリシー セット	Cisco ISE 2.3 以降へのアップグレード後の新しいポリシー セット

Cisco ISE 2.2 以前からの古いポリシー セット	Cisco ISE 2.3 以降へのアップグレード後の新しいポリシー セット
1. ポリシー セット A（条件 A/結果なし） 1. 認証外部パート 1（外部条件 1/許可されるプロトコル A） 1. 認証内部パート 1.1（内部条件 1.1/ID ストア A） 2. 認証内部パート 1.2（内部条件 1.2/ID ストア A） 3. 認証内部パート 1.3（内部条件 1.3/ID ストア A） 4. 認証内部 1 デフォルト（条件なし/ID ストア B） 2. 認証外部パート 2（外部条件 2/許可されるプロトコル A） 1. 認証内部パート 2.1（内部条件 2.1/ID ストア A） 2. 認証内部パート 2.2（内部条件 2.2/ID ストア A） 3. 認証内部パート 2.3（内部条件 2.3/ID ストア A） 4. 認証内部 2 デフォルト（条件なし/ID ストア B） 3. 認証外部パート 3（外部条件 3/許可されるプロトコル A） 1. 認証内部 3 デフォルト（条件なし/ID ストア B） 4. デフォルト認証外部パート（条件なし/許可されるプロトコル A/ID ストア C） 5. 例外 1 6. 許可ルール 1 7. 許可ルール 2	

Cisco ISE 2.2 以前からの古いポリシー セット	Cisco ISE 2.3 以降へのアップグレード後の新しいポリシー セット
	1. ポリシー セット A（条件 A/許可されるプロトコル A） 1. 認証ポリシー（コンテナ） 1. 認証外部パート 1：認証内部パート 1.1（外部条件 1 + 内部条件 1.1/ID ストア A） 2. 認証外部パート 1：認証内部パート 1.2（外部条件 1 + 内部条件 1.2/ID ストア A） 3. 認証外部パート 1：認証内部パート 1.3（外部条件 1 + 内部条件 1.3/ID ストア A） 4. 認証外部パート 1：認証内部 1 デフォルト（外部条件 1/ID ストア B） 5. 認証外部パート 2：認証内部パート 2.1（外部条件 2 + 内部条件 2.1/ID ストア A） 6. 認証外部パート 2：認証内部パート 2.2（外部条件 2 + 内部条件 2.2/ID ストア A） 7. 認証外部パート 2：認証内部パート 2.3（外部条件 2 + 内部条件 2.3/ID ストア A） 8. 認証外部パート 2：認証内部 2 デフォルト（外部条件 2/ID ストア B） 9. 認証外部パート 3：認証内部 3 デフォルト（外部条件 3/ID ストア B） 10. デフォルト認証外部パート（条件なし/ID ストア C） 2. 例外 1 3. 許可ポリシー（コンテナ） 1. 許可ルール 1

Cisco ISE 2.2 以前からの古いポリシー セット	Cisco ISE 2.3 以降へのアップグレード後の新しいポリシー セット
	2. 許可ルール 2

- 新しくアップグレードされたポリシー セットには、元のポリシー セットからの外部条件と内部条件を組み合わせて変換される認証ルールのリストが含まれています。変換中に作成されるそれぞれの新しい認証ルールは、内部パートの名前を含むサフィックス付きの古い外部パートの名前に基づいて名前が付けられます。たとえば、上記の表のように、古いポリシーセットが「ポリシーセットA」と呼ばれ、その認証の「外部パート」の 1 つが外部パート 1 と呼ばれ、認証の「内部パート」の 1 つが内部パート 1 と呼ばれている場合、新しく作成された認証ルールは、ポリシー セット A 内で「外部パート 1：内部パート 1」と呼ばれます。同様に、古いポリシー セットが「全従業員」ポリシーセットと呼ばれ、その認証の「外部パート」の 1 つがロンドンと呼ばれ、認証の「内部パート」の 1 つが「有線 MAB」と呼ばれている場合、新しく作成された認証ルールは「全従業員」ポリシー セット内で「ロンドン：有線 MAB」と呼ばれます。認証ポリシーのデフォルトの外部パートは、デフォルトの認証ルールとして変換されます。システムのデフォルト ポリシー ルールは、作成または変換された他のルールに関係なく、認証テーブル全体の最後のルールとして表示され、このルールは移動または削除できません。
- 外部パートに定義された条件（それに基づいて認証ルールが照合されます）は、内部パートの条件（認証に使用される ID ストアを示す）と組み合わされます。新しい結合条件は、新しいモデルのポリシーセット内の単一の認証ルールで設定されます。ポリシー セット内の新しい個別ルールは、古いポリシー セットの個別の外部パートごとに作成されます。

2. ポリシーセット内の「外部パート」に対して 2 つ以上の許可されたプロトコルが選択されている場合、元のポリシー セットはすべて次のように変換されます。
   - 古いポリシーセット内の各認証ルールの各「外部パート」は、新しいモデルで新しい個別のポリシー セットに変換されます。この新しいポリシー セットは、新しいポリシー モデルの [認証ポリシー（Authentication Policy）] セクションの下にある同じ元の「外部パート」から「条件」を配置します。

     次の表に、ISE 2.2 以前のバージョンから ISE 2.3 以降への古いポリシー セットの変換を示します（シナリオ 2）。

表 *4 :* 異なる許可されたプロトコルを使用したポリシー セットの変換

Cisco ISE 2.2 以前からの古いポリシー セット	**Cisco ISE 2.3** 以降へのアップグレード後の新しいポリシー セット

Cisco ISE 2.2 以前からの古いポリシー セット	Cisco ISE 2.3 以降へのアップグレード後の新しいポリシー セット
1. ポリシー セット A（条件 A/結果なし） 1. 認証外部パート 1（外部条件 1/許可されるプロトコル A） 1. 認証内部パート 1.1（内部条件 1.1/ID ストア A） 2. 認証内部パート 1.2（内部条件 1.2/ID ストア A） 3. 認証内部パート 1.3（内部条件 1.3/ID ストア A） 4. 認証内部 1 デフォルト（条件なし/ID ストア B） 2. 認証外部パート 2（外部条件 2/許可されるプロトコル B） 1. 認証内部パート 2.1（内部条件 2.1/ID ストア A） 2. 認証内部パート 2.2（内部条件 2.2/ID ストア A） 3. 認証内部パート 2.3（内部条件 2.3/ID ストア A） 4. 認証内部 2 デフォルト（条件なし/ID ストア B） 3. 認証外部パート 3（外部条件 3/許可されるプロトコル C） 1. 認証内部 3 デフォルト（条件なし/ID ストア B） 4. デフォルト認証外部パート（条件なし/許可されるプロトコル A/ID ストア C） 5. 例外 1 6. 許可ルール 1 7. 許可ルール 2	

Cisco ISE 2.2 以前からの古いポリシー セット	Cisco ISE 2.3 以降へのアップグレード後の新しいポリシー セット
	1. ポリシー セット A：認証外部パート 1（条件 A + 外部条件 1/許可されるプロトコル A） 1. 認証ポリシー（コンテナ） 1. 認証内部パート 1.1（内部条件 1.1/ID ストア A） 2. 認証内部パート 1.2（内部条件 1.2/ID ストア A） 3. 認証内部パート 1.3（内部条件 1.3/ID ストア A） 4. 認証内部 1 デフォルト（条件なし/ID ストア B） 2. 例外 1 3. 許可ポリシー（コンテナ） 1. 許可ルール 1 2. 許可ルール 2 1. ポリシー セット A：認証外部パート 2（条件 A + 外部条件 2/許可されるプロトコル B） 1. 認証ポリシー（コンテナ） 1. 認証内部パート 2.1（内部条件 2.1/ID ストア A） 2. 認証内部パート 2.2（内部条件 2.2/ID ストア A） 3. 認証内部パート 2.3（内部条件 2.3/ID ストア A） 4. 認証内部 2 デフォルト（条件なし/ID ストア B） 2. 例外 1 3. 許可ポリシー（コンテナ） 1. 許可ルール 1

Cisco ISE 2.2 以前からの古いポリシー セット	Cisco ISE 2.3 以降へのアップグレード後の新しいポリシー セット
	2. 許可ルール 2 1. ポリシー セット A：デフォルト認証外部パート 3（条件 A＋外部条件 3/許可されるプロトコル C） 1. 認証ポリシー（コンテナ） 1. 認証内部 3 デフォルト（条件なし/ID ストア B） 2. 例外 1 3. 許可ポリシー（コンテナ） 1. 許可ルール 1 2. 許可ルール 2 1. ポリシー セット A：デフォルト（条件 A/許可されるプロトコル A） 1. 認証ポリシー（コンテナ） 1. デフォルト認証ルール（条件なし/ID ストア C） 2. 例外 1 3. 許可ポリシー（コンテナ） 1. 許可ルール 1 2. 許可ルール 2

- 変換時に作成される新しいポリシーセットは、外部パート名を含むサフィックスを使用して抽出された古いポリシーセットの名前に基づいて名前が付けられます。たとえば、上記の表のように、古いポリシーセットが「ポリシーセットA」と呼ばれ、その認証の「外部パート」の 1 つが外部パート 1 と呼ばれている場合、新しく作成されたポリシー セットは「ポリシーセットA：外部パート1」と呼ばれます。同じように、古いポリシーセットが「ロンドン」と呼ばれ、その認証の「外部パート」の1つが有線 MAB と呼ばれている場合、新しく作成されたポリシー セットは「ロンドン：有線 MAB」と呼ばれます。

古い各ポリシーセットのデフォルトの外部パートも、「ロンドン：デフォルト」などのように、他のすべての外部パートと同様に新しいポリシーセットに変換されます。システム デフォルト ポリシー セットは、作成または変換された他のポリシー セットに関係なく、テーブル全体の最後のポリシーセットとして表示され、移動または削除できません。

- 古いポリシーセットの最上位レベルで定義された条件は、許可された正しいプロトコルを選択するように設計された外部認証パート条件と組み合わされます。新しい結合条件は、新しいモデルの新しいポリシーセットごとに最上位レベルのルールで構成されます。古い各ポリシー セットの各外部パートごとに新しい個別のポリシー セットが作成されます。

許可ルール/例外の変更

グローバル例外とローカル例外だけでなく、許可ルールもポリシーセット内から維持されるようになりました。古いポリシー セット内のすべての許可ルールおよび例外は、認証ポリシー ルールの変換の結果として生じるすべての新しいポリシーセットにも適用されます。許可ポリシーの変更は、外部パートに設定されている許可されたプロトコルに関係なく、アップグレードされるすべてのポリシー セットに適用されます。

ポリシー セットの評価

新しいインターフェイスでポリシー セットは、[ポリシー セット（Policy Set）] テーブルに表示される順序に従って一致の有無がチェックされます。たとえば、古い「ロンドン」ポリシーセットに、変換前にステータスが異なる 3 つの外部パートがあり、古い「ニューヨーク」セットにデフォルトの外部パートのみが含まれている場合、新しいポリシー セット インターフェイスのテーブルには新しいポリシー セットとシステムのデフォルト ポリシー セットが次の順序で表示されます。

ポリシー セット名
ロンドン：有線 MAB
ロンドン：ワイヤレス MAB
ロンドン：デフォルト
ニューヨーク：デフォルト
デフォルト

最初の 2 つのセットが一致しない場合、システムは「ロンドン：デフォルト」をチェックします。「ロンドン：デフォルト」が一致しない場合、システムは次に「ニューヨーク：デフォルト」をチェックします。「ニューヨーク：デフォルト」も一致しない場合、システムはポリシーとして「デフォルト」のみを使用します。

同じ論理を使用して正しい認証ルールの照合と選択が行われ、次に正しい許可ルールの照合と選択が行われます。各テーブルの先頭から開始し一致が見つかるまで各ルールがチェックされます。一致する他のルールがない場合は、デフォルト ルールが使用されます。

新しく変換されたポリシー セットのステータス

認証ルールに異なる許可されたプロトコルを使用するポリシーセットを変換する際に、新しく変換されたポリシーセットのステータスは、古いポリシーセットのステータスと古いポリシーセットの「外部パート」のステータスに基づいて次のように決定されます。

古いポリシー セットのステータス	古いポリシー セットの「外部パート」のステータス	新しいポリシー セットのステータス
無効（Disable）	無効（Disable）	無効（Disable）
無効（Disable）	モニタ（Monitor）	無効（Disable）
無効（Disable）	有効（Enable）	無効
モニタ（Monitor）	無効（Disable）	無効（Disable）
モニタ（Monitor）	モニタ（Monitor）	モニタ（Monitor）
モニタ（Monitor）	有効（Enable）	モニタ（Monitor）
有効（Enable）	無効	無効（Disable）
有効（Enable）	モニタ（Monitor）	モニタ（Monitor）
有効（Enable）	有効（Enable）	有効（Enable）

新しく変換された認証ルールのステータス

認証ルールに同じ許可されたプロトコルを使用するポリシーセットを変換する際に、新しく変換された認証ルールのステータスは、古い認証ルールの「外部パート」のステータスと対応する古い認証ルールの「内部パート」のステータスに基づいて次のように決定されます。

古い認証ルールの「外部パート」のステータス	対応する古い認証ルールの「内部パート」のステータス	変換された認証ルールのステータス
無効（Disable）	無効（Disable）	無効（Disable）
無効（Disable）	モニタ（Monitor）	無効（Disable）
無効（Disable）	有効（Enable）	無効
モニタ（Monitor）	無効（Disable）	無効（Disable）
モニタ（Monitor）	モニタ（Monitor）	モニタ（Monitor）
モニタ（Monitor）	有効（Enable）	モニタ（Monitor）
有効（Enable）	無効	無効（Disable）
有効（Enable）	モニタ（Monitor）	モニタ（Monitor）

古い認証ルールの「外部パート」のステータス	対応する古い認証ルールの「内部パート」のステータス	変換された認証ルールのステータス
有効（Enable）	有効（Enable）	有効（Enable）

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

- アップグレードの開始前に、既存のバージョンで最新のパッチにアップグレードします。
- 実稼働ネットワークのアップグレード前に、ステージング環境でアップグレードをテストし、アップグレードの問題を特定して修正することができます。
- アップグレード前にローカル リポジトリでアップグレード ソフトウェアをダウンロードおよび保存し、プロセスを高速化します。
- アップグレード プロセスの開始前にアップグレード準備ツール（URT）を使用し、設定データのアップグレードの問題を検出して修正します。ほとんどのアップグレードの障害は、設定データのアップグレードの問題が原因で発生します。URTは、可能な場合は、必ずアップグレード前にデータを検証し、問題を特定、報告、または修正します。URTは、セカンダリ ポリシー管理ノードまたはスタンドアロン ノードで実行できる個別のダウンロード可能なバンドルとして利用できます。このツールを実行するのに必要なダウンタイムはありません。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

（注） 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。

- UI を使用して ISE をアップグレードする場合、プロセスのタイムアウトは 4 時間です。プロセスに4時間以上かかる場合、アップグレードは失敗です。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することができます。

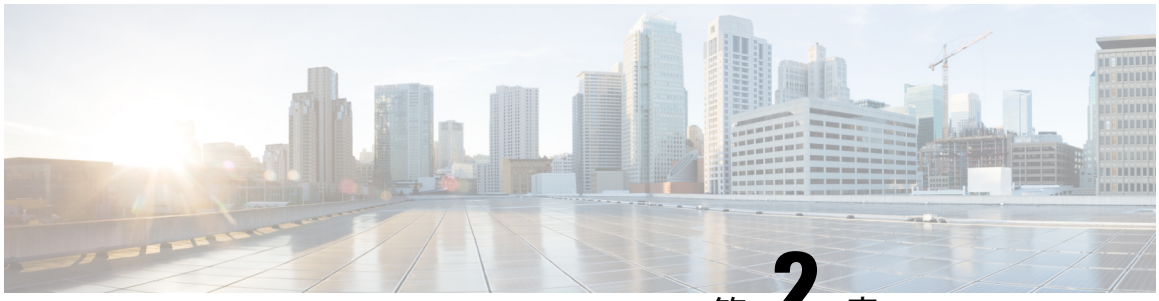
  - MnT コレクション フィルタ（[システム（System）] > [ロギング（Logging）] > [コレクションフィルタ（Collection Filters）]）を使用して、着信ログをフィルタリングし、AAA ログでエントリが重複しないようにします。
  - リモート ロギング ターゲット（[システム（System）] > [ロギング（Logging）] > [リモートロギングターゲット（Remote Logging Target）]）を作成し、個々のロギング カテゴリを特定のロギング ターゲット（[システム（System）] > [ロギング（Logging）] > [ロギングカテゴリ（Logging categories）]）にルーティングできます。
  - [管理（Administration）] > [システム（System）] > [設定（Settings）] > [プロトコル（Protocols）] > [RADIUS] ウィンドウで [繰り返し発生する更新を無視（Ignore Repeated Updates）] オプションを有効にして、繰り返し発生するアカウン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：
  https://bst.cloudapps.cisco.com/bugsearch/search?kw=%20ISE%20upgrade&pf=prdNm&sb=anfr&mDt=4&sts=open&bt=custV

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

リリース 2.6 は、Red Hat Enterprise Linux（RHEL）7.0 をサポートしています。

VMware 仮想マシンの Cisco ISE ノードをアップグレードする場合は、アップグレードの完了後に、Red Hat Enterprise Linux（RHEL）7 にゲスト オペレーティング システムを変更します。これを行うには、VM の電源をオフにし、RHEL 7 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。



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。

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

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

アップグレード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。

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

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

1. サポートされているバージョンの Cisco ISE で URT が実行されているかどうかをチェックします。サポートされているバージョンは、リリース 2.1、2.2、2.3、および 2.4 です。
2. URT がスタンドアロン Cisco ISE ノードまたはセカンダリ ポリシー管理ノード（セカンダリ PAN）で実行されているかどうかを確認します。
3. URT バンドルの使用開始日が 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） ディスク要件のサイズ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する必要があります。

- NTP サーバ
- 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。
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。
8.
   - （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。

始める前に

URT の実行中は、：

- データをバックアップまたは復元する
- ペルソナ変更の実行

ステップ 1 リポジトリの作成および URT バンドルのコピー （30 ページ）
ステップ 2 アップグレード準備ツールの実行 （30 ページ）

リポジトリの作成および URT バンドルのコピー

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

始める前に

リポジトリとの帯域幅接続が良好であることを確認してください。

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

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

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

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

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

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

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。

アップグレード準備ツールの実行

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

始める前に

ローカル ディスクに URT バンドルを置くと、時間を短縮できます。

---

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

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

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

Cisco ISE にはいくつかの事前定義された承認複合条件が付属しています。古い展開内の（ユーザ定義された）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、Red Hat Enterprise Linux（RHEL）7 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、RHEL 7 にゲスト オペレーティング システムを変更し、変更後に VM の電源をオンにする必要があります。RHEL 7 は E1000 および VMXNET3 ネットワーク アダプタのみをサポートします。アップグレードする前に、ネットワーク アダプタのタイプを変更する必要があります。

スポンサー グループ名から英語以外の文字を削除する

リリース 2.2 より前に、英語以外の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、英語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、英語以外の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の間にファイアウォールを導入している場合、次の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 モニタリング ノードのローカル リポジトリで、モニタリング データをバックアップすることはできません。次のリポジトリ タイプはサポートされていません。CD-ROM、HTTP、HTTPS、または TFTP。これは、これらのリポジトリ タイプが読み取り専用であるか、またはプロトコルでファイルのリストがサポートされないためです。

1. [管理（Administration）] > [メンテナンス（Maintenance）] > [バックアップと復元（Backup and Restore）] を選択します。
2. [すぐにバックアップ（Backup Now）] をクリックします。

3. バックアップを実行するために必要な値を入力します。
4. [OK] をクリックします。
5. バックアップが正常に完了したことを確認します。

   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。

   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。

（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*

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、信頼できる証明書とシステム証明書ストアの証明書の有効性を確認し、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。
- 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。

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。アップグレードの前に、次の設定を無効にした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、アップグレードの前に、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。

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 サーバ ノードのプロファイラ構成を必ず記録してください（[管理（Administration）] > [システム（System）] > [展開（Deployment）] > *<node>* > [プロファイル設定（Profiling Configuration）]）。設定をメモするか、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 サーバ名が承認ポリシーで使用され、対応する MDM サーバが無効の場合は、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 サーバを有効にします。
2. 承認ポリシーから MDM サーバ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。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。

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

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

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

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

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** 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。

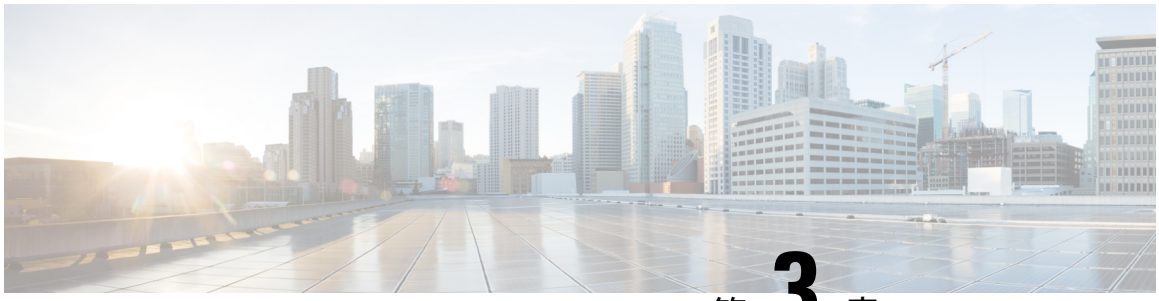
（注） リポジトリとの帯域幅接続が良好であることを確認してください。リポジトリからノードにアップグレード バンドルをダウンロードする場合、ダウンロードが完了するまでに 35 分以上かかるとダウンロードがタイムアウトします。

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 Installation Guide』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。



第 3 章

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さらに簡素化され、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。

[アップグレードの概要（Upgrade Overview）]ページには、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。

さまざまなタイプの展開

- スタンドアロン ノード：管理、ポリシー サービスおよびモニタリングのペルソナを担当する単一の Cisco ISE ノード
- マルチノード展開：複数の ISE ノードによる分散展開。分散展開をアップグレードする手順については、下記で詳しく説明します。

> ISE コミュニティ リソース
>
> ネットワークが ISE 展開への準備ができているかどうかを評価する方法については、ISE Deployment Assistant（IDA）を参照してください。

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

管理者ポータルから Cisco ISE 展開のすべてのノードをアップグレードできます。

（注） GUI ベースのアップグレードは、リリース 2.0 以降からそれよりも新しいリリースにアップグレードする場合、または Cisco ISE 2.0 以降の限定提供リリースを一般提供リリースにアップグレードする場合にのみ適用できます。

始める前に

アップグレードする前に、次の作業が完了していることを確認します。

- ISE の設定および運用データのバックアップを取得します。
- システム ログのバックアップを取得します。
- スケジュールしたバックアップを無効にします。展開のアップグレードが完了したら、バックアップ スケジュールを再設定します。
- 証明書および秘密キーをエクスポートします。
- リポジトリを設定します。アップグレードバンドルをダウンロードし、このリポジトリに格納します。
- Active Directory の参加クレデンシャルと RSA SecurID ノード秘密のメモを取ります（該当する場合）。この情報は、アップグレード後に Active Directory または RSA SecurID サーバに接続するために必要です。
- アップグレードのパフォーマンスを向上させるために、運用データを消去します。

ステップ 1 管理者ポータルの [アップグレード（Upgrade）] タブをクリックします。

ステップ 2 [続行（Proceed）] をクリックします。

[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 3 [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。

[バンドルのノードへのダウンロード（Download Bundle to Nodes）] ウィンドウが表示されます。

ステップ 4 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。

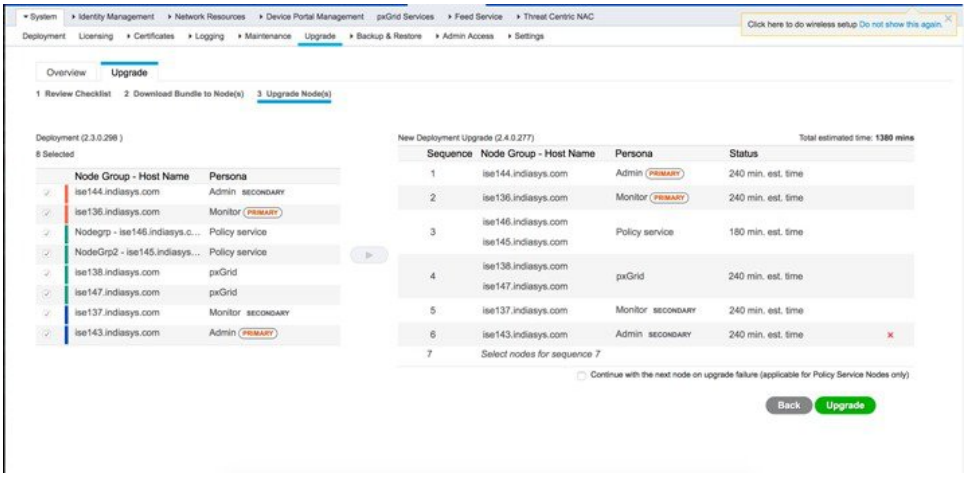
d) アップグレードに使用するバンドルの隣にあるチェックボックスをオンにします。
e) [確認（Confirm）] をクリックします。

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 5 [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 *3*：現在の展開と新しい展開を表示するアップグレード ウィンドウ



ステップ 6 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。

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

現在の展開内のノード ペルソナ	アップグレードの順序
セカンダリ管理/プライマリ モニタリング ノード、ポリシー サービス ノード、プライマリ管理/セカンダリ モニタリング ノード	1. セカンダリ管理/プライマリ モニタリング ノード 2. ポリシー サービス ノード 3. プライマリ管理/セカンダリ モニタリング ノード
セカンダリ管理/セカンダリ モニタリング ノード、ポリシー サービス ノード、プライマリ管理/プライマリ モニタリング ノード	1. セカンダリ管理/セカンダリ モニタリング ノード 2. ポリシー サービス ノード 3. プライマリ管理/プライマリ モニタリング ノード
セカンダリ管理ノード、プライマリ モニタリング ノード、ポリシー サービス ノード、プライマリ管理/セカンダリ モニタリング ノード	1. セカンダリ管理ノード 2. プライマリ モニタリング ノード 3. ポリシー サービス ノード 4. プライマリ管理/セカンダリ モニタリング ノード
セカンダリ管理ノード、セカンダリ モニタリング ノード、ポリシー サービス ノード、プライマリ管理/プライマリ モニタリング ノード	1. セカンダリ管理ノード 2. セカンダリ モニタリング ノード 3. ポリシー サービス ノード 4. プライマリ管理/プライマリ モニタリング ノード
セカンダリ管理/プライマリ モニタリング ノード、ポリシー サービス ノード、セカンダリ モニタリング 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 モニタリング ノード 4. プライマリ管理ノード

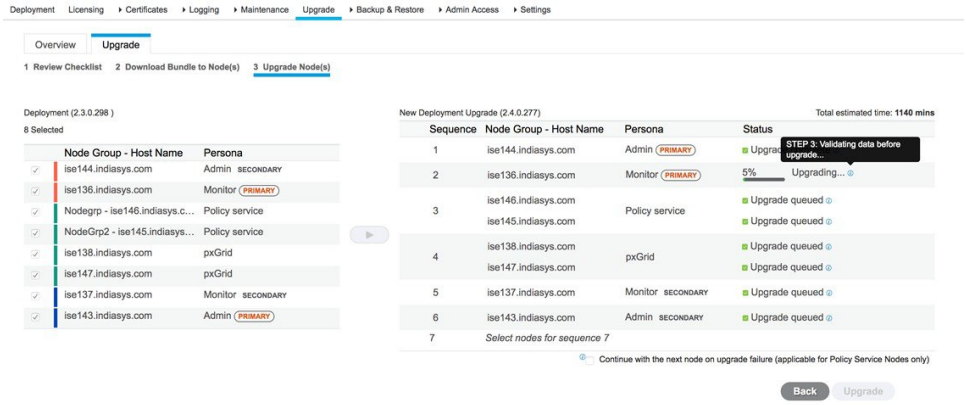
ステップ 7 アップグレードがアップグレード順序のいずれかのポリシーサービス ノードで失敗した場合でもアップグレードを続行するには、[失敗時でもアップグレードを続行する（Continue with upgrade on failure）] チェックボックスをオンにします。

このオプションは、セカンダリ管理ノードおよびプライマリ モニタリング 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 8 [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。

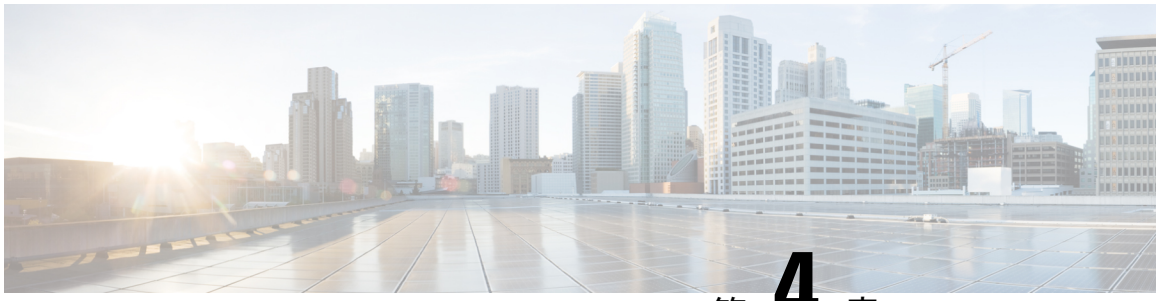
図 *4*:アップグレードの進行状況を表示するアップグレード ウィンドウ



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。

（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またはノードの新しい展開への登録中に、[管理（Administration）] > [システム（System）] > [設定（Settings）] > [ポスチャ（Posture）] > [更新（Updates）] ページから、ポスチャの自動更新機能を無効にすることができます。



第 4 章

CLI からの Cisco ISE 展開のアップグレード

アップグレード プロセス

スタンドアロン ノードのアップグレード

application upgrade コマンドを直接使用したり、アプリケーション アップグレード **prepare** および **proceed** コマンドを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** 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、**application upgrade** 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** 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** 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** および **proceed** コマンドを実行することをお勧めします。

始める前に

アップグレードの準備に関する章の説明を必ず読んでください。

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

例：

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

ステップ 2 Cisco ISE コマンドライン インターフェイス（CLI）から、 **application upgrade prepare** 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 （48 ページ）

2 ノード展開のアップグレード

application upgrade prepare 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 *5 : 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 （48 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（ノードA）、1つのセカンダリ管理ノード（ノードB）、および4つのポリシー サービス ノード（PSN）（ノードC、ノードD、ノードE、およびノードF）、1つのプライマリ モニタリング ノード（ノードG）、および1つのセカンダリ モニタリング ノード（ノードI）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 *6 :* 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** 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。
- アップグレード前の注意事項に関する章で指定されている手順をすでに読んで完了し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 からセカンダリ管理ノード（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が展開から登録解除され、アップグレードされます。再起動すると、ノードBは、新しい展開のプライマリ ノードになります。各展開でモニタリング 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イネーブルになってい

なくても、ノード B のモニタリング ペルソナをイネーブルにします。ポリシー サービス ペルソナが古い展開のノード B でイネーブルであった場合、この設定は新しい展開へのアップグレード後も維持されます。

ステップ 2 モニタリング ノードの 1 つ（ノード G）を新規展開にアップグレードします。

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ノード A のモニタリング 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。ノード A が再起動するまで待ちます。新規展開にモニタリング 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リング ペルソナを持たない場合、モニタリング 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 ノード（ノード C、D、E、F）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。

PSN がノード グループ クラスタの一部である場合、PSN を PAN から登録解除し、スタンドアロン ノードとしてアップグレードし、新規展開の PAN に登録する必要があります。

アップグレード後に、新規展開のプライマリ ノード（ノード B）に PSN が登録され、プライマリ ノード（ノード B）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 （展開に IPN ノードがある場合）プライマリ管理ノードから IPN ノードの登録を解除します。

Cisco ISE、リリース 2.0 以降は、IPN ノードはサポートしていません。

ステップ 5 古い展開に 2 番目のモニタリング ノード（ノード I）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 ノードであるノード A のモニタリング ペルソナをイネーブルにします。

展開でモニタリング 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 モニタリング ノード（ノード I）を古い展開から新しい展開にアップグレードします。

プライマリ管理ノード（ノード A）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 6 最後に、プライマリ管理ノード（ノード A）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（ノード A）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。

例

次のタスク

アップグレード プロセスの確認 （48 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、変更は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。

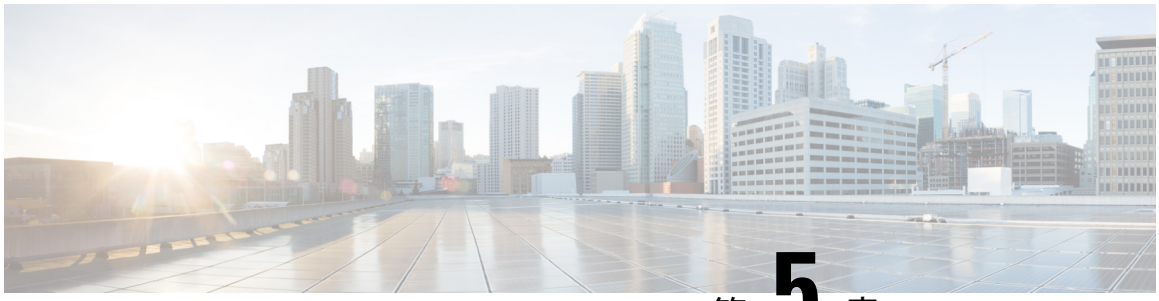
- ade.log ファイルでアップグレードプロセスを確認します。ade.log ファイルを表示するには、Cisco ISE CLI から次のコマンドを入力します：**show logging system ade/ADE.log**
- **show version** コマンドを実行し、ビルド バージョンを検証します。
- **show application status ise** コマンドを入力して、すべてのサービスが実行されていることを確認します。

ISO イメージの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 設定およびモニタリング データをバックアップすることをお勧めします。バックアップおよびアップグレード プロセスの詳細については、Cisco ISE アップグレードの概要 （1 ページ）を参照してください。

設定およびモニタ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、設定およびモニタリング データを復元（モニタリング 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、リモート リポジトリにサポート バンドルを配置します。



第 5 章

アップグレード後の作業

展開のアップグレード後に、この章にリストされているタスクを実行します。

アップグレード後の作業

Cisco ISE リリース 2.3 以降では、すべてのネットワーク アクセス ポリシーとポリシー セットを置き換える、新しい拡張された [ポリシーセット（Policy Sets）] ページが提供されます。以前のリリースからアップグレードすると、すべてのネットワーク アクセス ポリシーの設定（認証および承認の条件、ルール、ポリシー、プロファイル、および例外を含む）が ISE GUI の新しい [ポリシーセット（Policy Sets）] 領域に移行されます。ポリシー変更の詳細については、新規ポリシー モデル （4 ページ）を参照してください。

これらのタスクの詳細については、「Administrators Guide for your version of ISE」を参照してください。

- **VM 設定の確認**

  VMware 仮想マシンのゲスト オペレーティング システムが Red Hat Enterprise Linux（RHEL）7 に設定され、ネットワーク アダプタが E1000 または VMXNET3 に設定されていることを確認します。

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

- **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 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。

  1. 内部管理者アカウントを使用して Cisco ISE ユーザ 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「Administrator Access to Cisco ISE」を参照してください。

  2. 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**：ユーザを識別するために 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**：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。

- **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（古い展開のプライマリ管理ノード）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。

  回避策として、新しい展開でプライマリ管理ノードになるようにセカンダリ管理ノードを昇格した後に、管理者用ポータルから新しい ISE ルート CA 証明書チェーンを作成します

（**[管理（Administration）] > [証明書（Certificates）] > [証明書署名要求（Certificate Signing Requests）] > [ISEルートCA証明書チェーンの置換（Replace ISE Root CA certificate chain）]** の順に選択）。

- **証明書とキーをセカンダリ管理ノードで復元する**

  セカンダリ管理ノードを使用している場合は、プライマリ管理ノードから Cisco ISE CA 証明書およびキーのバックアップを取得し、セカンダリ管理ノードで復元します。この操作により、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。

  Backup and Restore of Cisco ISE CA Certificates and Keys

- **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、以下を参照してください。

  「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：

  1. **[管理（Administration）] > [フィードサービス（FeedService）] > [プロファイラ（Profiler）]** の順に選択します。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。
  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

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。
2. [追加（Add）] をクリックします。
3. [Cisco 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。
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。
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

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。
2. [追加（Add）] をクリックします。
3. [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。
4. [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**の設定を更新してください。

1. 管理者用ポータルから、**[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [認証（Authentication）] > [許可されているプロトコル（Allowed Protocols）]** を選択します。
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。
3. [送信（Submit）] をクリックします。

サポート対象の暗号スイートの完全なリストについては、次のマニュアルを参照してください。

Cisco Identity Services Engine のリリース ノート

Cisco Identity Services Engine Network Component Compatibility

- **モニタ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。

  バックアップと復元の実行に失敗すると、[RADIUSディスク使用率上昇アラーム（High RADIUS Disk Usage Alarm）] がトリガーされる場合があります。アップグレード中、最大サイズの MnT データベース ファイルが正常に更新されず、データベース ファイルが一杯になるためです。

  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 Administrator Guide』の「Backup and Restore Operations 」を参照してください。

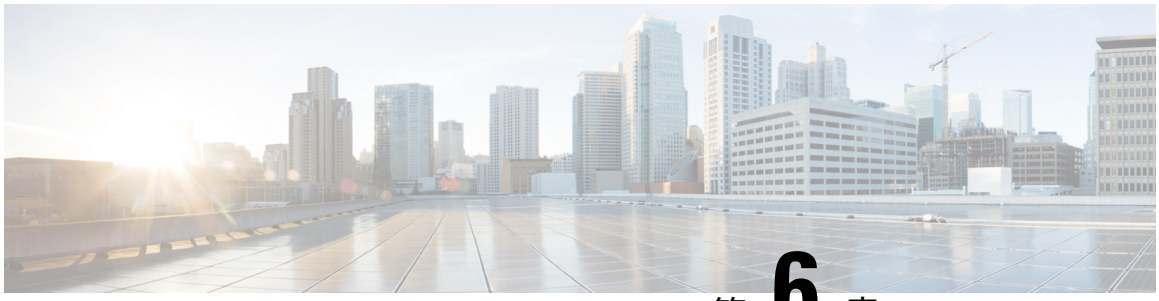
- **Trustsec NAD に対するポリシーの更新**

  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。

  1. no cts role-based enforcement
  2. 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。



第 6 章

アップグレードの障害に関する FAQ

アップグレードの障害に関する FAQ

GUI タイムアウトを使用してバンドル ダウンロードをアップグレードする理由

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。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。

次のアップグレード エラー メッセージが表示された場合の操作：`error: % Warning: The node has been reverted back to its pre-upgrade state`

[アップグレード（Upgrade）] ウィンドウで、[詳細（Details）] リンクをクリックします。[アップグレードの失敗の詳細（Upgrade Failure Details）] ウィンドウに記載されている問題を解決します。すべての問題を解決した後、[アップグレード（Upgrade）] をクリックして、アップグレードを再起動します。

次のノード アップグレード ステータス メッセージが表示された場合の操作：`Upgrade cannot begin…`

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。この問題は、展開のすべてのノードのバージョンが同じでないときに発生する可能性があります。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。

次のエラー メッセージが表示された場合の操作：`No Secondary Administration Node in the Deployment`

このエラーは次の場合に発生します。

- 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（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。

アップグレードの障害に関する FAQ

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。

次のメッセージが表示される理由：`Upgrade timed out after minutes: x`

このエラー メッセージが表示された場合は、Cisco ISE ノードの CLI にログインし、アップグレードのステータスを確認します。通常、このエラーメッセージは、アップグレードプロセスに問題が発生したことを示します。ただし、この時点では、誤ったアラームである可能性があります。

この問題が事実の場合は、該当する次のいずれかのタスクを実行します。

- アップグレードに成功し、このエラーメッセージが表示されるノードが古い展開からのセカンダリ管理ノードである場合は、残りのノードをCLIからアップグレードできます。
- 管理者用ポータルの [アップグレード（Upgrade）] ウィンドウからセカンダリ管理ノードを削除した場合、GUI からアップグレードを続行できません。この場合、残りのノードについては CLI からアップグレードを続行することを推奨します。
- このエラーメッセージが表示されるノードが非セカンダリ管理ノードである場合は、管理者用ポータルの [アップグレード（Upgrade）] ウィンドウからそのノードを削除し、残りのノードのアップグレードを GUI から続行します。

古い展開内のプライマリ管理ノードで登録中にアップグレードが失敗した場合は、どうなりますか?

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。

ISE ノードのアップグレードに特定の順序はありますか?

はい。次の順序でアップグレードを実行することをお勧めします。

1. セカンダリ管理ノード

（注） 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。

2. プライマリ モニタリング ノード

アップグレードの障害に関する FAQ

3. ポリシー サービス ノード

（注） 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」を参照）、新しい展開が期待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。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。

4. セカンダリ モニタリング ノード

5. プライマリ管理ノード

まれに、以前のバージョンの ISO イメージを使用して Cisco ISE アプライアンスのイメージを再作成し、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、アップグレードのプロセスを開始する前に、Cisco ISE の構成およびモニタリング データをバックアップすることをお勧めします。

構成およびモニタリング 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。このような場合では、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、構成およびモニタリング データを復元（モニタリング ペルソナが有効な場合）する必要があります。

アップグレード ログはどのように確認しますか?

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

ADE-OS またはアプリケーション バイナリ アップグレードが失敗するとどうなりますか?

Cisco Application Deployment Engine（ADE）オペレーティング システム（ADE-OS）またはアプリケーション バイナリ アップグレードが失敗した場合、再起動後に CLI から **show application status ise** コマンドを実行すると、アップグレード失敗メッセージが表示されます。

構成と運用のバックアップを再イメージ化し、復元する必要があります。

アップグレードのキャンセル、コンソールセッションの切断、電源障害など、その他のタイプのすべての障害の場合、元のノードで有効にしていたペルソナに応じて、設定と運用のバックアップ イメージを再作成し、復元する必要があります。

アップグレードの障害に関する FAQ

アップグレードに失敗したらイメージを再作成する必要がありますか?

モニタリングデータベースのアップグレード（スキーマとデータ）エラーの場合は、設定と運用のバックアップを再イメージ化して復元する必要があります。再イメージ化する前に、失敗の原因を分析するために、**backup-logs** コマンドを実行し、リモート リポジトリ内にサポート バンドルを格納することによって、サポート バンドルを生成します。

ノードペルソナに基づいて、旧バージョンまたは新バージョンに再イメージ化する必要があります。

- セカンダリ管理ノード：旧バージョンに再イメージ化し、設定と運用バックアップを復元します。
- モニタリング ノード：ノードが既存の展開から登録解除されている場合は、新バージョンに再イメージ化し、新しい展開に再登録して、モニタリングペルソナを有効にします。
- その他のすべてのノード：その他のノードにアップグレード障害が発生した場合は、通常、システムは最後の既知の正常な状態に戻ります。システムが旧バージョンにロールバックしない場合は、新バージョンに再イメージ化して、新しい展開に登録し、旧展開と同様のペルソナを有効にすることができます。

アップグレードがバイナリのインストール中に失敗した場合はどうなりますか?

アプリケーションバイナリのアップグレードはデータベースのアップグレード後に発生します。バイナリのアップグレードで障害が発生すると、コンソールと ADE.log に次のメッセージが表示されます。

```
% システムでアプリケーションのインストール/アップグレードが失敗しました。破損したインストールを削除します（% Application install/upgrade failed with system removing the corrupted install）
```

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、リモート リポジトリにサポート バンドルを配置します。

ロール バックするには、以前のバージョンの ISO イメージを使用して Cisco ISE アプライアンスのイメージを再作成し、バックアップ ファイルからデータを復元します。アップグレードを再試行するには、毎回新しいアップグレード バンドルが必要です。