# Cisco ISE 3.2 アップグレードガイド：アップグレードの準備

## アップグレードの準備

アップグレードプロセスを開始する前に、次のタスクを必ず実行してください。

## ヘルス チェック

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

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

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

- アップグレードの開始前に、既存のバージョンで最新のパッチにアップグレードします。

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

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

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

- 展開内の PSN の数と人員の可用性に基づいて、アップグレードする必要がある Cisco ISE の最終バージョンをインストールし、最新のパッチを適用して、対応可能な状態に保つことができます。
- MnT ログを保持する場合は、MnT ノードに対して前述のタスクを実行し、MnT ノードとして新しい展開に参加します。ただし、操作ログを保持する必要がない場合は、MnT ノードを再イメージ化してこの手順をスキップできます。
- 実稼働環境に影響のないマルチノード展開がある場合、Cisco ISE のインストールを並行して実行できます。ISE サーバーを並列にインストールすると、特に以前のリリースのバックアップと復元を使用している場合、時間が節約されます。
- 新しい展開に PSN を追加して、PAN からの登録プロセス中に既存のポリシーをダウンロードすることができます。ISE の遅延と帯域幅の計算ツールを使用して、Cisco ISE の展開における遅延と帯域幅の要件を理解します。
- 古いログをアーカイブし、それらを新しい展開に転送しないことをお勧めします。これは、後で MnT ロールを変更する場合に、MnT で復元された操作ログが異なるノードに同期されないためです。
- 完全な分散型展開を使用する 2 つのデータセンター（DC）がある場合は、バックアップ DC をアップグレードし、プライマリ DC をアップグレードする前に使用例をテストします。

- アップグレード前にローカルリポジトリでアップグレードソフトウェアをダウンロードおよび保存し、プロセスを高速化します。
- 現在 Cisco ISE リリース 3.0 以降にアップグレードしている場合は、ヘルスチェックまたはアップグレード準備ツール（URT）を使用して、アップグレードプロセスを開始する前にシステム診断を実行できます。
- アップグレードプロセスの開始前にアップグレード準備ツール（URT）を使用し、設定データのアップグレードの問題を検出して修正します。ほとんどのアップグレードの障害は、設定データのアップグレードの問題が原因で発生します。URT は、可能な場合は、必ずアップグレード前にデータを検証し、問題を特定、報告、または修正します。URT は、セカンダリポリシー管理ノードまたはスタンドアロンノードで実行できる個別のダウンロード可能なバンドルとして利用できます。このツールを実行するのにダウンタイムは発

生しません。次のビデオでは、URT の使用方法について説明します。
https://www.cisco.com/c/en/us/td/docs/security/ise/videos/urt/v1-0/cisco-urt.html

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

- GUI を使用して Cisco ISE をアップグレードする場合、ノードあたりのプロセスのタイムアウトは 4 時間です。アップグレード所要時間が 4 時間を超えると、アップグレードは失敗します。アップグレード準備ツール（URT）のアップグレードに 4 時間以上かかる場合は、このプロセスに CLI を使用することをお勧めします。
- 設定を変更する前に、ロードバランサのバックアップを作成します。アップグレードウィンドウ中にロードバランサから PSN を削除し、アップグレード後に再び追加できます。
- 自動 PAN フェールオーバーを無効にして（設定されている場合）、アップグレード中に PAN 間のハートビートを無効にします。
- 既存のポリシーとルールを確認し、古くて、冗長な、更新されていないポリシーおよびルールを削除します。
- 不要なモニターリングログとエンドポイントデータを削除します。
- 設定と動作のログのバックアップを作成し、ネットワークに接続されていない一時的なサーバーで復元することができます。アップグレードウィンドウ中はリモートロギングターゲットを使用できます。

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

  - MnT コレクションフィルタ（このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして、**[管理（Administration）]**>**[システム（System）]**>**[ロギング（Logging）]**>**[コレクションフィルタ（Collection Filters）]**）を使用して、着信ログをフィルタリングし、AAA ログでエントリが重複しないようにします。
  - リモートロギングターゲット（このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして、**[管理（Administration）]**> **[システム（System）]**> **[ロギング（Logging）]**>**[リモートロギングターゲット（Remote Logging Target）]**）を作成し、個々のロギングカテゴリを特定のロギングターゲット（このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして、**[システム（System）]**>**[ロギング（Logging）]**> **[ロギングカテゴリ（Logging categories）]**）にルーティングできます。
  - [繰り返し発生する更新を無視（Ignore Repeated Updates）] オプションを有効にします。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして、[管理（Administration）]>[システム（System）]>[設定（Settings）]>[プロトコル（Protocols）]>[RADIUS] ウィンドウに移動して、繰り返し発生するアカウンティングの更新を回避します。

- アップグレードの最新のアップグレードバンドルをダウンロードして使用します。バグ検索ツールで次のクエリを使用して、アップグレードを探し、オープンで修正済みの関連不具合をアップグレードします。http://cs.co/ise-upgrade-bugsearch
- ユーザー数を減らした新しい展開ですべての使用例をテストし、サービスの継続性を確保します。

# アップグレードの失敗を防ぐためのデータの検証

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

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

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

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

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

1. サポートされているバージョンの Cisco ISE で URT が実行されているかどうかをチェックします。サポートされているバージョンは、リリース 2.4、2.6 および 2.7 です。
2. URT がスタンドアロン Cisco ISE ノードまたはセカンダリポリシー管理ノード（セカンダリ PAN）で実行されているかどうかを確認します。
3. URT バンドルの使用開始日から 45 日未満であるかどうかをチェックします。このチェックは、最新の URT バンドルを使用していることを確認するために行われます。
4. すべての前提条件が満たされているかどうかをチェックします。

   次の前提条件が URT によって確認されます。

   - バージョンの互換性
   - ペルソナのチェック
   - ディスク容量

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

- NTP サーバー
- メモリ
- システムと信頼できる証明書の検証

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

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

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

## アップグレード準備ツールのダウンロードと実行

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

### 始める前に

URT の実行中は、同時に実行しないようにします。：

- データをバックアップまたは復元する
- ペルソナ変更の実行

手順

**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 （6 ページ）

**ステップ 2** アップグレード準備ツールの実行 （6 ページ）

## リポジトリの作成および URT バンドルのコピー

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

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

### 始める前に

リポジトリとの帯域幅接続が良好であることを確認してください。

手順

**ステップ 1** Cisco.com から URT バンドルをダウンロードします（ise-urtbundle-3.2.xxx-1.0.0.SPA.x86_64.tar.gz）。

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

```
copy repository_url/path/ise-urtbundle-3.2.xxx-1.0.0.SPA.x86_64.tar.gz disk:/
```

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

```
(Add the host key if it does not exist) crypto host_key add host mySftpserver
copy sftp://aaa.bbb.ccc.ddd/ ise-urtbundle-3.2.xxx-1.0.0.SPA.x86_64.tar.gz disk:/
```

aaa.bbb.ccc.ddd は SFTP サーバーの IP アドレスまたはホスト名、ise-urtbundle-3.2.*xxx*-1.0.0.SPA.x86_64.tar.gz は URT バンドルの名前です。

## アップグレード準備ツールの実行

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

### 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。

手順

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

```
application install ise-urtbundle-3.2.0.x.SPA.x86_64.tar.gz reponame
```

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

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

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（ユーザー定義された）承認単純条件が事前定義済み承認複合条件と同じ名前である場合、アップグレードプロセスは失敗します。アップグレードする前に、次の事前定義済み承認複合条件名のいずれかと名前が同じ承認単純条件は名前を変更する必要があります。

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

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

仮想マシンの Cisco ISE ノードをアップグレードする場合は、ゲスト オペレーティング システムを Red Hat Enterprise Linux（RHEL）のサポートされるバージョンに変更してあることを確認

します。これを行うには、VM の電源をオフにし、ゲスト オペレーティング システムを更新し、変更後に VM の電源をオンにする必要があります。

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

# スポンサーグループ名から 非 ASCII 文字を削除する

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

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

# 通信用に開く必要があるファイアウォールポート

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

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

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

Cisco ISE が使用するポートの完全なリストについては、「Cisco ISE Ports Reference」を参照してください。

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

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

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

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

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

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

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

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

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

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

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

# プライマリ管理ノードからのシステムログのバックアップ

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

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

# CA 証明書チェーン

Cisco ISE 3.2 にアップグレードする前に、内部 CA 証明書チェーンが有効であることを確認します。

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

# 証明書の有効性の確認

アップグレードプロセスは、Cisco ISE の信頼できる証明書またはシステム証明書ストアの証明書の期限が切れていると、失敗します。アップグレードの前に、[信頼できる証明書（Trusted Certificates）] と [システム証明書（System Certificates）] ウィンドウ（このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして、[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [証明書の管理（Certificate Managemen）]を選択）の [有効期限（Expiration Date）] の有効性を確認し、必要に応じて更新してください。

また、アップグレードの前に、[CA 証明書（CA Certificates）] ウィンドウ（このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして、[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [証明書機関（Certificate Authority）] > [証明書機関の証明書（Certificate Authority Certificates）]を選択）内の証明書の [有効期限（Expiration Date）] の有効性を確認し、必要に応じて更新してください。

# 証明書を削除する

期限切れの証明書を削除するには、次の手順を実行します。

**手順**

**ステップ 1** Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [証明書の管理（Certificate Management）] > [システム証明書（System Certificates）]**を選択します。

**ステップ 2** 期限切れの証明書を選択します。

**ステップ 3** [削除（Delete）] をクリックします。

**ステップ 4** Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [証明書の管理（Certificate Management）] > [信頼できる証明書（Trusted Certificates）] を選択します。

**ステップ 5** 期限切れの証明書を選択します。

**ステップ 6** [削除（Delete）] をクリックします。

**ステップ 7** [管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [認証局（Certificate Authority）] > [認証局証明書（Certificate Authority Certificates）] の順に選択します。

**ステップ 8** 期限切れの証明書を選択します。

**ステップ 9** [削除（Delete）] をクリックします。

# 証明書および秘密キーのエクスポート

次の項目をエクスポートすることを推奨します。

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

手順

**ステップ 1** Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [証明書の管理（Certificate Management）] > [システム証明書（System Certificates）] を選択します。

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

**ステップ 3** [証明書および秘密キーをエクスポート（Export Certificates and Private Keys）] ラジオボタンを選択します。

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

**ステップ 5** [エクスポート（Export）] をクリックします。

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

手順

**ステップ 1** Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [証明書の管理（Certificate Management）] > [システム証明書（System Certificates）]** を選択します。

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

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

**ステップ 4** Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [認証局（Certificate Authority）] > [認証局証明書（Certificate Authority Certificates）] を選択します。

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

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

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

**ステップ 8** [エクスポート（Export）] をクリックします。

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

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

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

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

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

# NTP サーバーの設定と可用性の確認

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

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

Cisco ISE リリース 2.7 以降では、Network Time Protocol デーモン（ntpd）の代わりに chrony が使用されます。ntpd はルート分散が最大 10 秒のサーバーと同期しますが、chrony はルート分散が 3 秒未満のサーバーと同期します。したがって、NTP サービスの中断を回避するために、Cisco ISE リリース 2.7 以降にアップグレードする前に、ルート分散が低い NTP サーバーを使用することを推奨します。詳細については、『Troubleshoot ISE and NTP Server Synchronization Failures on Microsoft Windows』を参照してください。

# 仮想マシンのアップグレード

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

各OVAファイルは、VMを記述するために使用されるファイルを含むパッケージであり、Cisco ISE ソフトウェアをインストールするためにアプライアンスに必要なハードウェアリソースを確保します。

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

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

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

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

# プロファイラ設定の記録

プロファイラサービスを使用する場合、管理者ポータルから、各ポリシーサービスノードのプロファイラ構成を必ず記録してください（このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして、[管理（Administration）] > [システム（System）] > [展開（Deployment）] > <ノード> > を選択します）。ノードを選択して、[ノードの編集（Edit Node）] をクリックします。[ノードの編集（Edit Node）] ページで、[プロファイリング設定（Profiling Configuration）] タブに移動します。構成情報をメモするか、スクリーンショットを取得できます。

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

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

# アップグレード前の MDM ベンダーのアクティベート

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

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

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

# リポジトリの作成およびアップグレードバンドルのコピー

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

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

リポジトリとのインターネット接続が良好であることを確認します。

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

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

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

アップグレードバンドルは Cisco.com からダウンロードします。

リリース 3.2 にアップグレードするには、このアップグレードバンドルを使用します。
ise-upgradebundle-2.x-to-3.2.0.*xxx*.SPA.x86_64.tar.gz

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

**copy** *repository_url/path/ise-upgradebundle-2.x-to-3.2.0.xxx.SPA.x86_64.tar.gz* **disk:/**

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

1. （ホストキーが存在しない場合は追加します）**crypto host_key add host** *mySftpserver*
2. **copy sftp:**//*aaa.bbb.ccc.ddd/ise-upgradebundle-2.x-to-3.2.0.xxx.SPA.x86_64.tar.gz* **disk:/**

   *aaa.bbb.ccc.ddd* は SFTP サーバーの IP アドレスまたはホスト名、*ise-upgradebundle-2.x-to-3.2.0.xxx.SPA.x86_64.tar.gz* はアップグレードバンドルの名前です。

# 利用可能なディスクサイズの確認

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

# ロードバランサ構成の確認

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

# ログの保持と MnT ハードディスクのサイズ変更

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

また、Cisco ISE MnT に負荷をかける可能性があるさまざまなデバイスからの不要なログについては、アクティブなコレクションフィルタ（このウィンドウを表示するには、[メニュー（Menu）]アイコン（☰）をクリックして、**[管理（Administration）]**>**[システム（System）]**>**[ロギング（Logging）]**>**[コレクションフィルタ（Collection filters）]**を選択します）を使用することもできます。

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

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

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。