

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、次のタスクを実行してください。

正常性チェック

アップグレードの前に Cisco ISE 展開の正常性チェックを実行して、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ます。詳細については、『*Cisco ISE Administrator Guide, Release 3.5*』にある「[Troubleshoot](#)」の章の「Health Check」を参照してください。

アップグレード期間の最適化

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するため、次のガイドラインに従ってください。これにより、全体的なダウンタイムが短縮できます。

- 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。



Note

以前の からアップグレードするときに、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。

- 実稼働システムに影響を与えることなく問題を特定して対処するために、ステージング環境でアップグレードをテストします。
- 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必要があります。



Note

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を実行していない場合、「**Upgrade cannot begin (アップグレードを開始できません)**」という警告メッセージが表示されます。これは、アップグレードがブロックされていることを意味します。アップグレードを開始する前に、すべてのノードに同じバージョンとパッチがインストールされていることを確認してください。

- Cisco ISE リリース 3.2 パッチ 3 より前の Cisco ISE リリースからアップグレードする場合は、次のガイドラインに従います。
 - 展開内の PSN の数や利用可能なスタッフに応じて、必要な最終バージョンの Cisco ISE をインストールし、最新のパッチを適用して、システムを使用できるようにします。
 - MnT ログを保持する場合は、MnT ノードに対してタスクを実行し、MnT ノードとして新しい展開に参加させます。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。

- 実稼働環境に影響を与えることなく、Cisco ISE のインストールをマルチノード展開で並行して実行できます。Cisco 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および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。
- 新しい展開に古いログを転送するのではなく、アーカイブすることをお勧めします。後で MnT ロールを変更した場合、MnT ノードで操作ログを復元しても、他のノードと同期されません。
- 完全に分散展開されているデータセンターが2つある場合は、最初にバックアップデータセンターをアップグレードします。その後、プライマリデータセンターをアップグレードする前にユースケースをテストします。
- 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。
- 現在最新の Cisco ISE リリースにアップグレードしている場合は、正常性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を開始する前に、URT を使用して、設定データ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、アップグレード中の設定データ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て問題を特定し、修正または報告します。URT は、セカンダリ PAN 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 URT の使用方法について説明します。
<https://video.cisco.com/detail/video/5797832452001>

Warning

プライマリ PAN で 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は、です。各ノードで生成されたシステムのタイムスタンプが表示されます。URT を使用するとアップグレードに余分の時間がかかる場合は、代わりに CLI を使用することを推奨します。
- 設定を変更する前に、ロードバランサをバックアップします。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。
- 既存のポリシーを確認し、古いルールや冗長な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。このウィンドウを表示するには、Cisco ISE GUI で[管理 (Administration)] > [システム (System)] > [ロギング (Logging)] > [収集フィルタ (Collection Filters)] に移動します。
- リモートロギングターゲットを作成するには、Cisco ISE GUI で[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 Targets)] に移動します。その後、Cisco ISE GUI で[システム (System)] > [ロギング (Logging)] > [ロギングカテゴリ (Logging categories)] に移動することで、各ロギングカテゴリを特定のロギングターゲットにルーティングできます。
- 繰り返し発生するアカウント更新を回避するには、[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、Cisco ISE GUI で [管理 (Administration)] > [システム (System)] > [設定 (Settings)] > [プロトコル (Protocols)] > [RADIUS] に移動します。
- 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、アップグレードに関連するオープンおよび修正済みの不具合を見つけます。 <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。

データの検証

Cisco ISE は URT を含みます。アップグレードプロセスを開始する前に、このツールを実行して、データアップグレードの問題を検出して解決できます。

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 を使用して、アップグレード前にデータを検証し、問題を特定してレポートし、可能な場合は問題を修正します。

URT は、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。ハイアベイラビリティと複数のノードの展開のサポートを実現するため、セカンダリ管理ノードを URT で実行します。または、単一ノード展開のスタンドアロンノードで URT を実行します。



Warning

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 CLI から URT を実行できます。URT は以下のことを実行します。

1. サポートされているバージョンの Cisco ISE で実行されているかどうかを確認します（サポートされているバージョンは、リリース 3.2、3.3、および 3.4）。
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. 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、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。
4. 次の前提条件がすべて満たされているかどうかをチェックします。
 - バージョンの互換性
 - ペルソナのチェック

- ディスク容量

Note

必要なディスク容量で使用可能なディスクサイズを確認してください（『*Cisco ISE Installation Guide, Release 3.5*』の「[Cisco Secured Network Server Series Appliances and Virtual Machine Requirements](#)」の章を参照）。ディスクサイズを増やす必要がある場合は、Cisco 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。

Note

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予想されている動作です。

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が提示されます。

アップグレードが成功した場合、ツールは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、ツールは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。

URT のダウンロードと実行

URT はアップグレード前の設定データをチェックして、アップグレード失敗の原因となる可能性のある問題を特定します。

URT の実行中は、同時に実行しないでください。

- データをバックアップまたは復元する
- ペルソナに変更を加える

Step 1 [リポジトリを作成します。 , on page 5](#)

Step 2 [URT のインストール, on page 5](#)

リポジトリを作成します。

リポジトリを作成し、URT バンドルをコピーします。リポジトリの作成に関する詳細については、『*Cisco ISE Administrator Guide, Release 3.5*』にある「Maintain and Monitor」の章の「[Create repositories](#)」を参照してください。

パフォーマンスと信頼性を向上させるには、FTP を使用します。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。ノードに近いローカルリポジトリを選択してください。

リポジトリへの接続に十分な帯域幅があることを確認します。

Step 1 [Cisco ISE Download Software Center](#) から URT バンドルをダウンロードします (ise-urtbundle-3.5.0.<build#>-1.0.0.SPA.x86_64.tar.gz)。

Step 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-3.5.0.<build#>-1.0.0.SPA.x86_64.tar.gz disk:/
```

SFTP を使用してアップグレードバンドルをコピーするには、次の手順を実行します。

```
(Add the host key if it does not exist) crypto host_key add host mySftpserver
copy sftp://aaa.bbb.ccc.ddd/ ise-urtbundle-3.5.0.<build#>-1.0.0.SPA.x86_64.tar.gz disk:/
```

値「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-3.5.0.<build#>-1.0.0.SPA.x86_64.tar.gz」は URT バンドルの名前を表します。

URT のインストール

URT は、アップグレード失敗の原因となる可能性のあるデータの問題を特定します。可能な場合は、これらの問題を報告または修正します。URT をインストールするには、次の手順を実行します。

URT バンドルをローカルディスクに保存すると、インストールプロセスをより迅速に完了できます。

Step 1 次の コマンドを入力して、ツールをインストールします。

```
application install ise-urtbundle-3.5.0.<build#>-1.0.0.SPA.x86_64.tar.gz reponame
```



Note

アプリケーションが正常にインストールされていない場合、URT によってアップグレード失敗の理由が示されます。報告された問題を修正してから URT を再度インストールしてください。

Step 2 Cisco ISE リリース 3.5 にアップグレードする場合は、5G 属性を削除します。詳細については、『*Cisco ISE Administrator Guide, Release 3.5*』の「Secure Access」の章にある「[Configure Cisco Private 5G as a Service](#)」セクションを参照してください。



Note

5G 属性を削除しないと、次のエラーが表示されます。

```
Error Occurred while adding 5G field to access service
```

```
Error while applying changes in version: 3.5.0.100 class: com.cisco.cpm.acs.nsf.im.NetworkAccessUpgrade
```

```
com.cisco.cpm.infrastructure.upgrade.api.UpgradeFailureException:
com.cisco.cpm.nsf.api.exceptions.NSFEntityAttributeException: AccessService FIVEG
DuplicateAttributeException~AttributeName : FIVEG already exists as FIVEG
```

```
at
```

```

com.cisco.cpm.acs.nsf.im.NetworkAccessUpgrade.upgradeAllowFiveG(NetworkAccessUpgrade.java:2671)
    at com.cisco.cpm.acs.nsf.im.NetworkAccessUpgrade.upgrade(NetworkAccessUpgrade.java:585)
    at
com.cisco.cpm.infrastructure.upgrade.impl.UpgradeServiceRegistrar.UpgradeServices(UpgradeServiceRegistrar.java:132)
    at
com.cisco.cpm.infrastructure.upgrade.impl.UpgradeServiceRegistrar.main(UpgradeServiceRegistrar.java:185)

Caused by: com.cisco.cpm.nsf.api.exceptions.NSFEntityAttributeException: AccessService FIVEG
DuplicateAttributeException~AttributeName : FIVEG already exists as FIVEG

```

URT の削除

インストールに失敗した場合、またはインストールされているバージョンが古い場合は、URT をアンインストールします。URT をアンインストールするには、次の手順を実行します。

インストール済みプログラムのリストに URT が表示されていることを確認します。

Step 1 CLI で次のコマンドを入力します。

```
application remove urt
```

Step 2 プロンプトに対して、**Y** を入力します。

```
Continue with application removal? (y/n)
```

アンインストールが完了すると、次のメッセージが表示されます。

```
Application successfully uninstalled
```

What's next

アンインストールが成功したら、必要に応じて URT をインストールできます。

承認単純条件の名前を変更して、複合条件名の競合を避ける

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。以前の展開に、事前定義済み承認複合条件と同じ名前の承認単純条件がある場合、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、承認単純条件の名前を変更し、事前定義済み複合条件と名前が重複しないようにしてください。

アップグレードの失敗を防ぐために、アップグレード中に承認単純条件名と重複していない、事前定義済み承認複合条件名のリストを次に示します。

- 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 設定のアップデート

VMs の Cisco ISE ノードをアップグレードする場合は、以下の手順を実行します。

1. ゲスト OS を RHEL 7 に変更します。
2. VM の電源をオフにします。
3. ゲスト OS を RHEL 7 に変更にします。
4. VM の電源をオンにします。

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します。

スポンサーグループ名のアップデート

アップグレードの前に、非 ASCII 文字を含む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 では、スポンサーグループ名に非 ASCII 文字はサポートされません。

主要なファイアウォールポートの有効化

PAN と他のノードの間にファイアウォールを展開している場合、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: (PAN) とモニタリングノード間の通信用。
- TCP 443: (PAN) 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: PSN がノードグループの一部である場合、PSN グループのクラスタリングに必要です。

Cisco ISE が使用するすべてのポートのリストについては、『Cisco ISE Installation Guide, Release 3.5』の「[Cisco ISE Ports Reference](#)」の章を参照してください。

PAN からの Cisco ISE 設定および運用データのバックアップ

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 を使用して設定および運用データをバックアップするには、次のコマンドを入力します。

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

Note

Cisco ISE が VMware で実行されている場合、Cisco 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特定の時点で、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、すべてのノードが現在のデータベースと継続的にデータを同期します。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。データのアーカイブおよび復元には、Cisco ISE のバックアップ機能を使用します。

VMware スナップショットを使用して Cisco 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 ノードを復元するには、再起動します。

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。次のことを確認します。

- 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。
- データのバックアップにローカルリポジトリを使用していないこと。
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。
- CD-ROM、HTTP、HTTPS、または TFTP リポジトリを使用しないでください。これらのリポジトリは読み取り専用であるか、ファイルの一覧表示をサポートしていません。

Cisco ISE GUI からバックアップを取得するには、次の手順を実行します。

1. Cisco ISE GUI で、**[管理 (Administration)] > [メンテナンス (Maintenance)] > [バックアップと復元 (Backup and Restore)]** に移動します。
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。

ノードロールの変更または昇格は、バックアップが完了するまでお待ちください。バックアップ中にノード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、データの不整合が発生する可能性があります。

バックアップ後、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。Cisco ISE では、バックアップファイル名にタイムスタンプを付加し、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。



Note

Cisco ISE では、ある Cisco ISE ノード（A）からバックアップを取得して、別の Cisco 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。

PAN からのシステムログのバックアップ

CLI を使用して、PAN からシステムログのバックアップを取得します。次の CLI コマンドを使用します。

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

CA 証明書チェーン

Cisco ISE リリース 3.5 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。内部 CA 証明書が有効かどうかを確認するには、次の手順を実行します。

1. Cisco ISE GUI で、[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）]に移動します。
2. 展開内の各ノードについて、[フレンドリ名（Friendly Name）] フィールドに [証明書サービスエンドポイントサブ CA（Certificate Services Endpoint Sub CA）] というラベルの付いている証明書を選択します。
3. [View] をクリックします。
4. 「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。
5. Cisco ISE GUI で [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）] に移動して、破損した証明書チェーンを修正します。

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。

アップグレードする前に、次の手順に従って、信頼できる証明書の有効性を確認します。

1. Cisco ISE の GUI で、[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）]に移動します。
2. 証明書の有効期限（Expiration Date）を確認します。証明書の有効期限が切れているか、まもなく期限切れになる場合は、証明書を更新します。

同様に、次の手順に従ってシステム証明書の有効性を確認します。

1. Cisco ISE GUI で、[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）]に移動します。

2. 証明書の有効期限 (**Expiration Date**) を確認します。証明書の有効期限が切れているか、まもなく期限切れになる場合は、証明書を更新します。

証明書の更新

Cisco ISE リリース 3.5 にアップグレードする前に、管理サービスで使用されている SHA1 証明書を、SHA256 以上などの安全なアルゴリズムを使用した証明書に置き換えてください。最新の CiscoSSL セキュリティ要件の下では、SHA1 は管理サービスでサポートされなくなりました。管理サービスが正しく動作するように、これらの証明書を更新してください。管理サービスの SHA1 証明書ではなく、他のサービスの SHA1 証明書のみをインポートします。

証明書の削除

期限切れの証明書を削除するには、次の手順を実行します。

- Step 1** Cisco ISE の GUI で、[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)] に移動します。
- Step 2** 期限切れの証明書を特定して選択します。
- Step 3** [削除 (Delete)] をクリックして、選択した証明書を削除します。
- Step 4** Cisco ISE の GUI で、[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)] に移動します。
- Step 5** 期限切れの証明書を選択します。
- Step 6** [削除 (Delete)] をクリックします。
- Step 7** Cisco ISE GUI で、[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)] に移動します。
- Step 8** 期限切れの証明書を選択します。
- Step 9** [削除 (Delete)] をクリックします。

すべてのノードからの証明書のエクスポート

すべてのローカル証明書とその秘密キーを展開内のすべてのノードから安全な場所にエクスポートします。各証明書の設定 (証明書を使用するサービスを含む) を記録します。

- Step 1** Cisco ISE の GUI で、[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)] に移動します。
- Step 2** 証明書を選択し、[エクスポート (Export)] をクリックします。
- Step 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。
- Step 4** [秘密キーのパスワード (Private Key Password)] を設定し、[パスワードの確認 (Confirm Password)] をします。
- Step 5** [エクスポート (Export)] をクリックします。

ローカル証明書とその秘密キーがシステムにダウンロードされます。

信頼できる証明書ストアからの証明書のエクスポート

PAN 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。各証明書の設定（証明書を使用するサービスを含む）を記録します。

Step 1 Cisco ISE GUI で、[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）]に移動します。

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

アップグレードのためのスケジュールバックアップと自動フェールオーバーの無効化

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。アップグレードをスムーズに行うため、自動設定を無効化してください。Cisco ISE をアップグレードする前に、次の設定を無効化する必要があります。

- [PANの自動フェールオーバー（PAN Automatic Failover）]: Cisco ISE をアップグレードする前に、PAN でこのオプションを無効化します。
- [スケジュールバックアップ（Scheduled backups）]: アップグレード前に、すべてのバックアップスケジュールを無効化します。アップグレード後、バックアップスケジュールを変更して再作成します。

1回実行するようにスケジュールされたバックアップは、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。1回のみ実行するように設定されたバックアップスケジュールがある場合は、アップグレード前に無効化してください。

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、PAN からデータを移行、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、アップグレードプロセス全体を通して到達可能で、応答性があり、同期していることを確認します。

Cisco ISE の以前のバージョンでは、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、必須の Cisco ISE バージョン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。

VM のアップグレード

Cisco ISE ソフトウェアは、UCS ハードウェアの最新の CPU またはメモリリソース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の両方と同期している必要があります。

Cisco ISE のバージョンが進むにつれ、次のことが起こります。

- 旧型のハードウェアのサポートが段階的に廃止されます。
- 新型のハードウェアが導入されます。

パフォーマンスを向上するには、VM キャパシティをアップグレードすることを推奨します。

VM アップグレードを計画する場合は、OVA ファイルを使用して、ソフトウェアを効率的にインストールしてください。各 OVA ファイルは、VM を記述するパッケージであり、アプライアンスに Cisco ISE ソフトウェアをインストールするために必要なハードウェアリソースを確保します。

VM およびハードウェアの要件の詳細については、『*Cisco ISE Installation Guide, Release 3.5*』にある「[Cisco Secured Network Server Series Appliances and Virtual Machine Requirements](#)」の章の「Hardware and Virtual Appliance Requirements for Cisco ISE」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。Cisco ISE VM には、パフォーマンスと拡張性を確保するために、ハードウェアアプライアンスと比較して十分な数の CPU コアが含まれています。

VM インフラストラクチャでリソースを共有すると、パフォーマンスに悪影響を与える可能性があります。CPU 使用率の上昇、ユーザー認証と登録の遅延、ログのドロップ、レポート処理の速度低下、ダッシュボードの応答性低下を引き起こす可能性があります。

Note

パフォーマンスの問題を回避するため、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します。

新しいバージョンの Cisco ISE では、ローカルディスク割り当てが 29 GB に増加しました。そのため、Cisco ISE には各 VM ごとに 300 GB 以上のディスクサイズが必要です。

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 PSN のプロファイラ構成を記録してください。

プロファイラ構成情報を検索するには、次の手順を実行します。

1. Cisco ISE GUI で、[管理 (Administration)] > [システム (System)] > [展開 (Deployment)] に移動します。
2. ノードを選択します。
3. [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。
4. 設定情報をメモするか、スクリーンショットをキャプチャします。

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 (AD) を使用する場合は、AD のクレデンシャルと有効な内部管理者アカウントを用意してください。アップグレード後に、AD 接続が失われることがあります。その場合、管理者ポータルにログインするために Cisco ISE 内部管理者アカウントを使用し、Cisco ISE と AD を再接続するために Active Directory のクレデンシャルを使用してください。

モバイルデバイス管理ベンダーの有効化

展開がサードパーティのモバイルデバイス管理 (MDM) ソリューションと連携する場合は、アップグレード前に MDM ベンダーのステータスが有効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、次のいずれかを実行できます。

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。詳細については、『Cisco ISE Administrator Guide, Release 3.5』にある「[Maintain and Monitor](#)」の章の「Create Repositories」を参照してください。

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

1. アップグレードプロセス時の時間を短縮するために、アップグレードバンドルをローカルディスクに配置します。この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。

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



Note

- リポジトリとの接続が高速で安定していることを確認します。ノードにアップグレードバンドル（約 14 GB）をダウンロードするのに 35 分以上かかる場合、プロセスがタイムアウトします。
- 構成ファイルをローカルディスクに保存している場合、アップグレード時に構成ファイルが削除されます。Cisco ISE リポジトリを作成し、リポジトリにコピーして、ファイルを保持してください。
- 低速な WAN リンク上のリポジトリではなく、ノードの近くのローカルリポジトリを選択してください。FTP を使用すると、パフォーマンスと信頼性が向上します。

2. アップグレードバンドルは [Cisco.com](https://www.cisco.com) からダウンロードします。

Cisco ISE リリース 3.5 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-3.2.x-3.4.x-to-3.5.0.<build#>.SPA.x86_64.tar.gz
```

3. アップグレードを実行するには、このコマンドを使用してアップグレードバンドルを Cisco ISE ノードのローカルディスクにコピーします。

```
copy repository_url/path/ise-upgradebundle-3.2.x-3.4.x-to-3.5.0.<build#>.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-3.2.x-3.4.x-to-3.5.0.<build#>.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-3.2.x-3.4.x-to-3.5.0.<build#>.SPA.x86_64.tar.gz はアップグレードバンドルの名前です。

使用可能なディスク容量の確認

仮想マシン（VM）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, Release 3.5*』の「[Cisco Secured Network Server Series Appliances and Virtual Machine Requirements](#)」の章にある「Disk space requirements for VMs in a Cisco ISE deployment」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、Cisco 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。

ロード バランサ構成の確認

PAN と PSN 間でロードバランサを使用している場合は、アップグレードプロセスが中断されないように、ロードバランサのセッションタイムアウトを十分長く設定してください。セッションタイムアウトが短すぎると、PSN でアップグレードが中断される可能性があります。たとえば、PAN から PSN へのデータベース転送中にセッションが終了すると、PSN でのアップグレードが失敗します。

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。ログが常にキャパシティに達し、追加のハードウェアリソースが必要な場合は、ログ保持のニーズに基づいて MnT ハードディスクサイズを計画します。ログ保持キャパシティは、直近のCisco ISE リリースで大幅に増加しました。

コレクションフィルタを有効にして、さまざまなデバイスから不要なログを削除できます。過剰なログは、Cisco ISE MnT に負荷をかける可能性があります。

Cisco ISE の GUI で、**[管理（Administration）]>[システム（System）]>[ロギング（Logging）]>[収集フィルタ（Collection Filters）]**に移動します。

[Cisco 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に関する情報が示されています。ログの保持は、TACACS+ と RADIUS で個別に計算してください。

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。