



# Cisco ISE-PIC のアップグレード

- [Cisco ISE-PIC アップグレードの概要 \(1 ページ\)](#)
- [アップグレードの失敗を防ぐためのデータの検証 \(3 ページ\)](#)
- [通信用に開く必要があるファイアウォールポート \(5 ページ\)](#)
- [プライマリ管理ノードからの Cisco ISE-PIC 設定および運用データのバックアップ \(6 ページ\)](#)
- [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 \(7 ページ\)](#)
- [証明書の有効性の確認 \(7 ページ\)](#)
- [証明書および秘密キーのエクスポート \(7 ページ\)](#)
- [スケジュールバックアップの無効化 \(8 ページ\)](#)
- [NTP サーバーの設定と可用性の確認 \(8 ページ\)](#)
- [2 ノード展開のアップグレード \(8 ページ\)](#)
- [スタンドアロンノードのアップグレード \(9 ページ\)](#)
- [アップグレードプロセスの確認 \(10 ページ\)](#)
- [アップグレードの障害からの回復 \(11 ページ\)](#)
- [以前のバージョンへのロールバック \(14 ページ\)](#)
- [アップグレード後のタスク \(15 ページ\)](#)
- [その他の参考資料 \(16 ページ\)](#)
- [通信、サービス、およびその他の情報 \(17 ページ\)](#)

## Cisco ISE-PIC アップグレードの概要

Cisco ISE-PIC 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。アップグレードには約 240 分、15 GB すべてのデータの場合はさらに 60 分かかります。

アップグレードの時間に影響する可能性のある要因には、次の項目の数があります。

- ネットワーク内のエンドポイント数とユーザー数
- プライマリ ノードのログ数

Cisco ISE-PIC をアップグレードするには、Cisco ISE アップグレードバンドルを使用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。

可能な限り最小のダウンタイムで、最大の復元力、ロールバックの機能、および最小限のエラー数を提供しながら、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すべての設定データをバックアップします。
2. 展開に応じてアップグレードプロセスを選択します。
  - スタンドアロン配置
    1. ノードをアップグレードします。 [スタンドアロンノードのアップグレード \(9 ページ\)](#) を参照してください。
    2. ノードのアップグレード後、アップグレードの検証テストとネットワークテストを実行します。次の情報を参照してください。  
[アップグレードプロセスの確認 \(10 ページ\)](#)。



(注) この手順の詳細については、次の項目を参照してください。

- [2 ノード展開のアップグレード \(8 ページ\)](#)
- [アップグレードプロセスの確認 \(10 ページ\)](#)

#### • ハイアベイラビリティ (2 ノード) の展開

1. 初回のアップグレードで失敗した場合にロールバックの PAN を使用できるように、最初にセカンダリ ノードをアップグレードし、セカンダリ ノードのアップグレードが確認されるまで以前のバージョンの PAN を保持しておきます。
2. セカンダリ ノードのアップグレード後、アップグレードの検証テストとネットワークテストを実行します。
3. PAN をアップグレードします。  
  
両方のノードのアップグレード後、セカンダリ管理ノードはアップグレードされたバージョンでインストールされた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アップグレードされたバージョンでインストールされたセカンダリ管理ノードになります。
4. 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。
5. 元のプライマリ ノードのアップグレードが完了したら (2 番目のアップグレード)、必要に応じて、現在のセカンダリ ノードの [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)。

## アップグレードの失敗を防ぐためのデータの検証

Cisco ISE-PIC 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、プライマリ管理ノードでは URT を実行しないでください。

Cisco ISE-PIC 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. URT がスタンドアロン Cisco ISE-PIC ノードまたはセカンダリ管理ノードで実行されているかどうかを確認します。
2. 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。
3. 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
- 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

4. 構成データベースを複製します。
5. 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。

6. 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行う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。

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 (4 ページ)

ステップ 2 アップグレード準備ツールの実行 (5 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。

ステップ 1 Cisco.com から URT バンドルをダウンロードします。Cisco ISE-PIC 用の Cisco ISE URT バンドルを使用する必要があります。

**ステップ 2** 必要に応じて、時間節約のために、Cisco ISE-PIC 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-2.7.0.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-2.7.0.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-2.7.0.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。

---

**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-filename 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。

---

## 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セカンダリ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間の通信用。
- TCP 443 : プライマリ管理ノードとセカンダリノード間の通信用。
- 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-PIC が使用するポートの完全なリストについては、「[Cisco ISE ポートリファレンス](#)」を参照してください。

# プライマリ管理ノードからの Cisco ISE-PIC 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) から Cisco ISE-PIC 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-PIC が VMware で実行されている場合、ISE-PIC 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-PIC 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-PIC 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-PIC データをバックアップすると、Cisco ISE-PIC サービスが停止します。ISE-PIC ノードを起動するには、再起動が必要です。

また、Cisco ISE-PIC 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。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-PIC 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、指定されたり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-PIC 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-PIC では、ある ISE-PIC ノード (A) からバックアップを取得して、別の ISE-PIC 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-PIC 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 ([管理 (Administration)] > [システム (System)] > [証明書 (Certificates)] > [証明書の管理 (Certificate Management)]) 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 ([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)]) 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。

## スケジュールバックアップの無効化

Cisco ISE-PIC 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。

- 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-PIC 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-PIC 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、『[Microsoft Windows での ISE および NTP サーバーの同期失敗のトラブルシューティング](#)』を参照してください。

## 2 ノード展開のアップグレード

`application upgrade prepare <upgrade bundle name> <repository name>` コマンドおよび `proceed` コマンドを使用して、2 ノード展開をアップグレードします。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、プライマリノードをアップグレードします。

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。



---

**ステップ 1** CLI からセカンダリノードをアップグレードします。

アップグレードプロセスで、自動的に元のセカンダリノードが展開から削除され、アップグレードされま  
す。元のセカンダリノードは再起動すると、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** アップグレード元のプライマリノード。

アップグレードプロセスで、自動的に元のプライマリノードが展開に登録され、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、セカンダリノード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 \(10 ページ\)](#)

## スタンドアロンノードのアップグレード

**application upgrade <upgrade bundle name> <repository name>** コマンドを直接使用したり、  
**application upgrade prepare <upgrade bundle name> <repository name>** および **application upgrade  
proceed** コマンドを指定された順番に使用してスタンドアロンノードをアップグレードするこ  
ともできます。

このコマンドを直接実行する場合は、コマンドを実行する前にリモートリポジトリから Cisco  
ISE-PIC ノードのローカルディスクにアップグレードバンドルをコピーして、アップグレード  
の時間を短縮することを推奨します。

代わりに、**application upgrade prepare <upgrade bundle name> <repository name>** コマンドと  
**application upgrade proceed** コマンドを使用することもできます。**application upgrade prepare  
<upgrade bundle name> <repository name>** コマンドを使用すると、アップグレードバンドルが  
ダウンロードされ、ローカルに抽出されます。このコマンドはリモートリポジトリから Cisco  
ISE-PIC 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なら、**application upgrade proceed** コマンドを実行してアップグレー  
ドを正常に完了します。

以下で説明する **application upgrade prepare <upgrade bundle name> <repository name>** および  
**application upgrade proceed** コマンドを実行することをお勧めします。

## 始める前に

「[アップグレードの準備](#)」の項の手順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-PIC コマンドラインインターフェイス (CLI) から、**application upgrade prepare <upgrade bundle name> <repository name>** コマンドを入力します。

このコマンドは、アップグレードバンドルを前の手順で作成したローカルリポジトリ「upgrade」にコピーし、MD5 と SHA256 チェックサムを一覧表示します。

**ステップ 3** (注) アップグレード後、SSH 経由でログインし、**show application status ise** コマンドを使用することで、アップグレードの進行状況を表示できます。次のメッセージが表示されます。「%NOTICE: Identity Services Engine upgrade is in progress...」

Cisco ISE-PIC 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 \(10 ページ\)](#)

## アップグレードプロセスの確認

展開が期待どおりに機能すること、およびユーザーがアクセスできることを確認するためのネットワークテストを実行することを推奨します。

構成データベースの問題でアップグレードが失敗すると、変更された内容が自動的にロールバックされます。

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-PIC CLI から次のコマンドを入力します：**show logging system ade/ADE.log.?**

STEP の **grep** でアップグレードの進行状況を表示できます。

- `info:[application:install:upgrade:preinstall.sh] STEP 0: Running pre-checks`
- `info:[application:operation:preinstall.sh] STEP 1: Stopping ISE application...`

- info:[application:operation:preinstall.sh] STEP 2: Verifying files in bundle...
  - info:[application:operation:isedbupgrade-newmodel.sh] STEP 3: Validating data before upgrade...
  - info:[application:operation:isedbupgrade-newmodel.sh] STEP 4: De-registering node from current deployment.
  - info:[application:operation:isedbupgrade-newmodel.sh] STEP 5: Taking backup of the configuration data...
  - info:[application:operation:isedbupgrade-newmodel.sh] STEP 6: Registering this node to primary of new deployment...
  - info:[application:operation:isedbupgrade-newmodel.sh] STEP 7: Downloading configuration data from primary of new deployment...
  - info:[application:operation:isedbupgrade-newmodel.sh] STEP 8: Importing configuration data...
  - info:[application:operation:isedbupgrade-newmodel.sh] STEP 9: Running ISE configuration data upgrade for node specific data...
  - info:[application:operation:isedbupgrade-newmodel.sh] STEP 10: Running ISE M&T database upgrade...
  - info:[application:install:upgrade:post-osupgrade.sh] POST ADEOS UPGRADE STEP 1: Upgrading Identity Services Engine software...
  - info:[application:operation:post-osupgrade.sh] POST ADEOS UPGRADE STEP 2: Importing upgraded data to 64 bit database...
- この文字列を検索して、アップグレードが成功したことを確認します。
- ```
Upgrade of Identity Services Engine completed
successfully.
```
- **show version** コマンドを実行し、ビルドバージョンを検証します。
  - **show application status ise** コマンドを入力して、すべてのサービスが実行されていることを確認します。

## アップグレードの障害からの回復

この項では、アップグレードの障害からの回復時に必要な作業について説明します。

まれに、イメージを再作成し、新規インストールを実行して、データを復元することが必要になる場合があります。アップグレードを開始する前に、Cisco ISE-PIC の設定データのバックアップが存在することが重要です。構成データベースの障害発生時には自動的に変更内容のロールバックが試みられますが、コンフィギュレーションデータをバックアップしておくことが重要です。

## アップグレードの障害

このセクションでは、既知のエラーの一部とそのエラーからの回復手順を説明します。



(注) CLIからアップグレードのログ、コンソールからアップグレードのステータスを確認することができます。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-PIC ノードのコンソールを表示します。Cisco ISE-PIC CLI で **show logging application** コマンドを使用して、次のログを表示することができます（サンプルファイル名を括弧内に示します）。

- DB データアップグレードログ (*dbupgrade-data-global-20160308-154724.log*)
- DB スキーマログ (*dbupgrade-schema-20160308-151626.log*)
- OS アップグレード後のログ (*upgrade-postosupgrade-20160308-170605.log*)

### 構成とデータのアップグレードエラー

アップグレード中、構成データベーススキーマとデータアップグレードの障害は自動的にロールバックされます。システムは、最後の既知の正常な状態に戻ります。この場合、次のメッセージがコンソールとログに表示されます。

```
% Warning: The node has been reverted back to its pre-upgrade state.
error: %post(CSCOcpm-os-1.4.0-205.i386) scriptlet failed, exit status 1
% Application upgrade failed. Please check logs for more details or contact Cisco Technical
Assistance Center for support.
```

### 修復エラー

アップグレードの障害を修復し、ノードを元の状態に戻す必要がある場合は、コンソールに次のメッセージが表示されます。詳細についてはログを確認してください。

```
% Warning: Do the following steps to revert node to its pre-upgrade state."
error: %post(CSCOcpm-os-1.4.0-205.i386) scriptlet failed, exit status 1
% Application upgrade failed. Please check logs for more details or contact Cisco Technical
Assistance Center for support.
```

### 検証エラー

検証エラーは、実際にアップグレードが失敗したわけではありません。検証エラーが発生する場合があります。たとえば、セカンダリ PAN をアップグレードする前に PSN をアップグレードしようとした場合や、次のエラーが表示されることがあります。システムは、最後の既知の正常な状態に戻ります。このエラーが発生した場合は、このドキュメントで説明されているアップグレードを実行します。

```
STEP 1: Stopping ISE application...
% Warning: Cannot upgrade this node until the standby PAP node is upgraded and running.
If standbyPAP is already upgraded
and reachable ensure that this node is in SYNC from current Primary UI.
Starting application after rollback...

% Warning: The node has been reverted back to its pre-upgrade state.
error: %post(CSCOcpm-os-1.4.0-205.i386) scriptlet failed, exit status 1
% Application upgrade failed. Please check logs for more details or contact Cisco Technical
Assistance Center for support.
```

## アプリケーションバイナリアップグレードエラー

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は、再起動後に CLI から **show application status ise** コマンドを実行すると、次のメッセージが表示されます。設定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。

```
% WARNING: An Identity Services Engine upgrade had failed. Please consult logs. You have to reimage and restore to previous version.
```

## その他のタイプのエラー

その他のタイプのすべての障害（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）の場合、元のノードで有効にしていたペルソナに応じて、バックアップ。

## 再イメージ化

再イメージ化という用語は、Cisco ISE-PIC の新規インストールを示しています。再イメージ化する前に、失敗の原因を確認するために、**backup-logs** CLI コマンドを実行することによってサポートバンドルを生成し、リモートリポジトリ内にサポートバンドルを配置します。ノードペルソナ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。
- プライマリ管理ノード：PAN 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、新しい展開と同様のペルソナを有効にすることができます。

## 失敗後のアップグレード

アップグレードに失敗した場合、アップグレードを再試行する前に、次の操作を実行してください。

- ログを分析します。エラーがないかサポートバンドルを検査します。
- 生成したサポートバンドルを Cisco Technical Assistance Center (TAC) に送信して、問題を特定および解決します。



- (注) 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...」

## アップグレードがバイナリのインストール中に失敗する

**問題** 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。

```
% Application install/upgrade failed with system removing the corrupted install
```

**解決法** 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 ISO イメージを使用して Cisco ISE-PIC 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。

- ログを分析します。エラーがないかサポートバンドルを検査します。
- 生成したサポートバンドルを Cisco Technical Assistance Center (TAC) に送信して、問題を特定および解決します。

## 以前のバージョンへのロールバック

まれに、以前のバージョンの ISO イメージを使用し、バックアップファイルからデータを復元することで、Cisco ISE-PIC 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-PIC 設定データをバックアップすることをお勧めします。

設定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ることがあります。これが発生すると、データベースがロールバックされないことを示す通知を、アップグレードの失敗メッセージと共に受け取ります。このようなシナリオでは、手動でシステムのイメージを再作成し、Cisco ISE をインストールして、設定およびモニターリングデータ。

ロールバックまたは回復を行う前に、**backup-logs** コマンドを使用してサポートバンドルを生成し、そのサポートバンドルをリモートリポジトリに配置します。

# アップグレード後のタスク

次のタスクの詳細については、『*Identity Services Engine Passive Identity Connector (ISE-PIC) Administrator Guide*』を参照してください。

## VMware 仮想マシンのゲスト オペレーティング システムの設定

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。



- (注) ESXi 5.x サーバー (5.1 U2 以上) でリリース 2.7 にアップグレードする場合は、RHEL 7 をゲスト OS として選択する前に、VMware ハードウェアのバージョンを 9 にアップグレードする必要があります。

## ブラウザのキャッシュのクリア

アップグレード後、Cisco ISE-PIC 管理者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。

サポート対象のブラウザは次のとおりです。

- Mozilla Firefox 79 以前のバージョン
- Mozilla Firefox ESR 60.9 以前のバージョン
- Google Chrome 84 以前のバージョン

## Active Directory の結合ポイントの再設定

Active Directory の結合ポイントは、アップグレード中に失われる可能性があります。管理ポータルにログインして移動し、結合ポイントを再設定する必要があるかどうかを確認します。

## Active Directory アイデンティティ検索属性の設定

Cisco ISE-PIC は、属性 SAM、CN、またはその両方を使用し、sAMAccountName 属性をデフォルト属性として使用して、ユーザーを識別します。

実際の環境で必要な場合、SAM と CN のいずれか、または両方を使用するように Cisco ISE-PIC を設定できます。SAM および CN が使用され、sAMAccountName 属性の値が一意でない場合、Cisco ISE-PIC 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. [プロバイダ (Providers)] > [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 (Value) ] : ユーザーを識別するために 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 ルックアップの設定

DNS サーバーからの 2 ノード展開のすべての Cisco ISE-PIC 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。

### Cisco CA 証明書とキーの復元

プライマリ管理ノードから Cisco ISE-PIC 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。これにより、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。

### 必須の ISE-PIC システム設定の再設定

- 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。

## その他の参考資料

次のリンクには、Cisco ISE で作業するときを使用できる追加のリソースが含まれています。  
[https://www.cisco.com/c/en/us/td/docs/security/ise/end-user-documentation/Cisco\\_ISE\\_End\\_User\\_Documentation.html](https://www.cisco.com/c/en/us/td/docs/security/ise/end-user-documentation/Cisco_ISE_End_User_Documentation.html)



## 通信、サービス、およびその他の情報

- シスコからタイムリーな関連情報を受け取るには、[Cisco Profile Manager](#) でサインアップしてください。
- 重要な技術によりビジネスに必要な影響を与えるには、[シスコサービス](#)にアクセスしてください。
- サービス リクエストを送信するには、[シスコサポート](#)にアクセスしてください。
- 安全で検証済みのエンタープライズクラスのアプリケーション、製品、ソリューション、およびサービスを探して参照するには、[Cisco DevNet](#)にアクセスしてください。
- 一般的なネットワーク、トレーニング、認定関連の出版物を入手するには、[Cisco Press](#) にアクセスしてください。
- 特定の製品または製品ファミリの保証情報を探すには、[Cisco Warranty Finder](#) にアクセスしてください。

## Cisco バグ検索ツール

[シスコバグ検索ツール](#) (BST) は、シスコ製品とソフトウェアの障害と脆弱性の包括的なリストを管理するシスコバグ追跡システムへのゲートウェイです。BSTは、製品とソフトウェアに関する詳細な障害情報を提供します。

## マニュアルに関するフィードバック

シスコのテクニカルドキュメントに関するフィードバックを提供するには、それぞれのオンラインドキュメントの右側のペインにあるフィードバックフォームを使用してください。



## 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。