Cisco ISE 2.7 アップグレードガイド：アップグレード後のタスク

初版：2023 年 2 月 21 日

最終更新：2023 年 2 月 21 日

アップグレード後の設定と構成

Cisco ISE のアップグレード後に、次のタスクを実行します。

仮想マシンの設定の確認

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（64 ビット）または Red Hat Enterprise Linux（RHEL）6（64 ビット）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、サポートされる RHEL バージョンにゲスト 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。

ESXi 5.x サーバー（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 ユーザー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。

  - 内部管理者アカウントを使用して Cisco ISE ユーザー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「Cisco ISE への管理アクセス」を参照してください。

  - 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ーを識別します。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（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（Comment）]：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 サーバー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。

証明書の復元

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。

プライマリ管理ノードのルート CA 証明書を復元するには、新しい Cisco ISE ルート CA 証明書チェーンを生成します。**[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き換え（Replace ISE Root CA certificate chain）]**を選択します を選択します。

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。これにより、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。

Cisco ISE CA 証明書およびキーのバックアップと復元

ルート CA チェーンの再生成

特定のアップグレードシナリオでは、アップグレードプロセスの完了後にルート CA チェーンを再生成する必要があります。次の手順に従って、ルート CA チェーンを再生成します。

1. Cisco ISE メインメニューから、**[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）]** の順に選択します。
2. [証明書署名要求（CSR）の生成（Generate Certificate Signing Request (CSR)）] をクリックします。
3. [証明書の使用先（Certificate(s) will be used for）] ドロップダウンリストで [ISE ルート CA（ISE Root CA）] を選択します。
4. [ISE ルート CA 証明書チェーンの置き換え（Replace ISE Root CA Certificate Chain）] をクリックします。

表 *1:* ルート *CA* チェーンの再生シナリオ

アップグレードのシナリオ	モード	ルート CA チェーンの再生成
フルアップグレードプロセス	展開	アップグレードプロセス中に展開が変更されないため、ルート CA の再生成は必要ありません。
分割アップグレードプロセス	展開	ルート CA チェーンの再生成
構成データベースの復元プロセス	スタンドアロン	ルート CA チェーンの再生成
ノードの昇格：分割アップグレードプロセス後に、セカンダリ PAN をプライマリ PAN に昇格する	展開	ルート CA チェーンの再生成
Cisco ISE ノードのドメイン名またはホスト名の変更	スタンドアロンと展開	ルート CA チェーンの再生成

アップグレードプロセス後、次のイベントが発生する可能性があります。

1. ライブログにデータがない。
2. キューリンクエラー。
3. ヘルスステータスが使用不可。
4. 一部のノードのシステム概要に利用できる日付がない。

キューリンクエラーを解決し、情報を復元するには、MnT Database をリセット し、ISE ルート CA 証明書チェーンを置き換える必要があります。

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、

「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：

手順

ステップ 1 **[管理（Administration）] > [フィード サービス（FeedService）] > [プロファイラ（Profiler）]** を選択します。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。

ステップ 2 Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして、**[管理（Administration）] > [フィードサービス（FeedService）] > [プロファイラ（Profiler）]**を選択します。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。

ステップ 3 [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

手順

ステップ 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。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 [シスコ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。

ステップ 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。

ステップ 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

手順

ステップ 1 [追加（Add）] をクリックします。

ステップ 2 [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。

ステップ 3 [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（Allowed Protocols）] の設定を更新してください。

手順

ステップ 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。

ステップ 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。

ステップ 3 [送信（Submit）] をクリックします。

関連トピック

Cisco Identity Services Engine リリースノート
Cisco Identity Services Engine ネットワークコンポーネントの互換性

モニター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。

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 管理者ガイド』の「」「」「」「バックアップ/復元操作」「」「」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。

- `no cts role-based enforcement`
- `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。

プロファイラエンドポイント所有権の同期/レプリケーション

Cisco ISE 2.7 以降のバージョンにアップグレードすると、JEDIS フレームワークの一部として、ポート 6379 を展開内のすべてのノード間で開いて双方向通信を行う必要があります。

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。