

アップグレード後の作業

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。

新しいライセンスタイプへの変換

新しいライセンスタイプに変換するには、次の手順を実行します。

1. Cisco Smart Software Manager (CSSM) を使用して、古いライセンスを新しいライセンスタイプに変換します。
2. Cisco ISE 管理者ポータルで新しいライセンスを有効にします。

詳細については、『Cisco ISE Administrator Guide, Release 3.5』の「[Licensing](#)」の章にある「Cisco ISE Licenses」を参照してください。

VM 設定の確認

VM の Cisco ISE ノードをアップグレードする場合は、ゲスト OS を変更します。Cisco ISE リリース 3.1 〜 Cisco ISE リリース 3.5 のゲストオペレーティングシステムとして RHEL 8 を使用します。操作内容

1. VM の電源をオフにします。
2. ゲスト OS をサポートされている RHEL バージョンに変更してから、
3. VM の電源をオンにします。

RHEL 7 以降は、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。

ブラウザのセットアップ

Cisco ISE 展開をアップグレードした後、以下を実行する必要があります。

1. ブラウザのキャッシュをクリア。
2. ブラウザを閉じる。
3. (サポートされているブラウザで) 新しいブラウザセッションを開き、Cisco ISE 管理ポータルにアクセスします。

Note

サポートされるブラウザのリストについては、リリースノートを参照してください。 <https://www.cisco.com/c/en/us/support/security/identity-services-engine/products-release-notes-list.html>

Active Directory の再参加

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。

管理アクセスに対して証明書ベースの認証を使用していて、Active Directory がアイデンティティソースである場合、アップグレード後にログインページにアクセスできません。これは、アップグレード中に Active Directory (AD) への結合が失われるためです。

外部アイデンティティソースとして Active Directory (AD) を使用しているときに、接続が失われた場合は、以下の手順を実行します。

1. 次のコマンドを入力して、Cisco ISE をセーフモードで起動します。

application start ise safe

2. 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。



Note

Cisco ISE 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た場合は、『*Cisco ISE Administrator Guide, Release 3.5*』の「[Administrator Access to Cisco ISE](#)」の章を参照してください。

3. Cisco ISE を Active Directory (AD) に再結合します。
4. 外部アイデンティティソースのワークフローを実行して、ノードに参加した後に接続が復元されていることを確認します。

Active Directory (AD) で使用される証明書属性

Cisco ISE 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 と CN の両方が使用される場合、sAMAccountName 属性が一意でないと、Cisco ISE は CN 属性値も比較します。

AD 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. Cisco ISE GUI で、[管理 (Administration)] > [ID管理 (Identity Management)] > [外部IDソース (External Identity Sources)] > [Active Directory] を選択します。
2. [拡張ツール (Advanced Tools)] をクリックします。
3. [高度な調整 (Advanced Tuning)] を選択し、次の詳細を入力します。
 - [ISE ノード (ISE Node)]: Active Directory に接続される Cisco 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 Cisco 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 (「デフォルト動作を SAM および CN に変更」など)。

4. [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たら、メッセージを読み、変更を承認します。Cisco ISE の AD コネクタサービスが自動的に再起動します。

逆引き DNS ルックアップ

各 DNS サーバーに、分散展開のすべての Cisco ISE ノードの逆引き DNS ルックアップを設定します。逆引き DNS ルックアップを設定しない場合、アップグレード後に展開関連の問題が発生する可能性があります。

証明書の復元

このセクションでは、アップグレード中に発生する可能性のある認証エラーを防ぐために、Cisco ISE 管理ノードで証明書とキーを復元する方法について詳しく説明しています。

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、PAN 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。

- SAN は新しい展開で PAN に昇格されている。
- セッション サービスが SAN で無効になっている。

証明書がストアにない場合は、認証エラーが発生し、次のエラーメッセージ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。

PAN 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。Cisco ISE GUI で、[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)] に移動します。

証明書とキーの SAN への復元

SAN を使用している場合は、PAN から Cisco ISE CA 証明書およびキーのバックアップを取得し、SAN で復元します。これにより、プライマリ PAN に障害が発生し、SAN を PAN に昇格する場合に、SAN 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。

詳細については、『Cisco ISE Administrator Guide, Release 3.5』にある「[Basic Setup](#)」の章の「Backup and restoration of Cisco ISE CA certificates and keys」を参照してください。

ルート CA チェーンの再生成

展開が特定のアップグレードシナリオに一致する場合、アップグレードの完了後にルート CA チェーンを再生成する必要があります。

ルート CA チェーンを再生成するには、次の手順を実行します。

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)] > [証明書署名要求 (Certificate Signing Request)] に移動します。
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。

次の表に、さまざまなルート CA チェーン再生成シナリオを定義します。

Table 1: ルート CA チェーンの再生成シナリオ

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	展開とスタンドアロン	アップグレード中に展開が変更されない場合、ルート CA を再生成する必要はありません。
分割アップグレードプロセス	展開とスタンドアロン	ルート CA チェーンは、アップグレードプロセス中にシステムによって自動的に再生成されます。
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 チェーンは、復元中にシステムによって自動的に再生成されます。
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。

- データはライブログで使用できない場合があります。
- キューリンクエラーが発生する場合があります。
- システムは、正常性ステータスを使用不可と表示する場合があります。
- システム概要に一部のノードのデータが表示されない場合があります。

キューリンクエラーを解決し、システム情報を復元するには、次の手順を実行します。

- MnT データベースをリセットする。

- ISE ルート CA 証明書チェーンを置き換える。

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。Cisco 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します。アダプタを選択し、[再起動 (Restart)] をクリックします。

SNMP 発信元ポリシーサービスノードを設定する

SNMP の設定で、手動で元のポリシーサービスノード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 設定を再設定して、SNMP 機能を復元してください。

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 サービスを更新して、最新の組織固有識別子 (OUI) がインストールされているようにします。

プロファイラ フィード サービスを更新するには、次の手順を実行します。

- Step 1** Cisco ISE GUI で、[管理 (Administration)] > [フィードサービス (FeedService)] > [プロファイラ (Profiler)] に移動します。
- Step 2** プロファイラ フィード サービスが有効なことを確認します。
- Step 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 リソースを更新する前に、次の考慮事項を確認してください。

- クライアント プロビジョニング ポリシーで使用するネイティブ サプリカント プロファイルを確認します。
- ワイヤレス SSID が正しいことを確認してください。
- 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。

クライアント プロビジョニング リソースを更新するには、次の手順を実行します。

オンライン更新

- Step 1** Cisco ISE GUI で、[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)] に移動して、クライアント プロビジョニング リソースを設定します。
- Step 2** [追加 (Add)] をクリックします。
- Step 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。

- Step 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。
- Step 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

- Step 1** Cisco ISE GUI で、[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)] に移動して、クライアントプロビジョニングリソースを設定します。
- Step 2** [追加 (Add)] をクリックしてリソースを追加します。
- Step 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。
- Step 4** [カテゴリ (Category)] ドロップダウンリストから、[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

非推奨の暗号方式を使用したレガシーデバイスの認証は、Cisco ISE への接続時に失敗する可能性があります。

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、次の手順を実行して [許可されているプロトコル (Allowed Protocols)] の設定を更新します。

- Step 1** Cisco ISE GUI で、[ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [結果 (Results)] > [認証 (Authentication)] > [許可されるプロトコル (Allowed Protocols)] に移動します。
- Step 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。
- Step 3** [送信 (Submit)] をクリックします。

モニターとトラブルシューティング

モニターおよびトラブルシューティングするには、次の手順を検討してください。

- 電子メール設定を再構成します。
- お気に入りレポートを更新します。
- データ削除設定を変更します。
- 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。



Note

デフォルトで、すべてのアラームはアップグレード後に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。



Note

前回の展開時にレポートをカスタマイズした場合、その変更はアップグレード時に置き換えられます。

更新前に作成した MnT バックアップを復元します。

Trustsec NAD に対するポリシーの更新

次のコマンドを実行して、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`

サブリカント 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、サブリカント プロビジョニング ウィザード (SPW) は更新されません。SPW を手動で更新する必要があります。その後、新しい SPW を参照する新しいネイティブ サブリカント プロファイルと新しいクライアント プロビジョニング ポリシーを作成します。Cisco ISE のダウンロードページで新しい SPW を検索できます。詳細については、Cisco ソフトウェアのダウンロードサイトを参照してください。

プロファイラエンドポイント所有権の同期またはレプリケーション

アップグレード中、JEDIS フレームワークは、双方向の通信を可能にするために、ポート 6379 を展開内のすべてのノード間で開いている必要があります。

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。