移行計画

この章では、移行計画に必要な情報を提供します。移行を注意深く計画することで、移行がスムーズに行われ、移行が失敗するリスクが軽減されます。

前提条件

ここでは、移行プロセスを実行するための前提条件について説明します。

移行インターフェイスの有効化

移行プロセスを開始する前に、Cisco Secure ACS および Cisco ISE サーバーでデータ移行に使用するインターフェイスを有効にする必要があります。移行プロセスが完了した後、両方のサーバーの移行インターフェイスを無効にすることをお勧めします。

ステップ 1 Cisco Secure ACS CLI で次のコマンドを入力して、Cisco Secure ACS マシンの移行インターフェイスを有効にします。

acs config-web-interface migration enable

ステップ 2 Cisco ISE サーバーで移行インターフェイスを有効にします。

a) Cisco ISE CLI で、**application configure ise** と入力します。

b) ACS の移行を有効または無効にするには、**11** と入力します。

c) **Y** と入力します。

（注） 移行プロセスが完了した後で、コマンド **acs config-web-interface migration disable** を使用して、Cisco Secure ACS マシン上の移行インターフェイスを無効にします。

（注） 移行プロセスが完了したら、Cisco ISE サーバー上の移行インターフェイスを無効にします。

移行ツールでの信頼できる証明書の有効化

始める前に

Cisco Secure ACS サーバーから移行ツールにデータをエクスポートできるようにするために、Cisco Secure ACS CA 証明書または Cisco Secure ACS 管理証明書を信頼することができます。

移行ツールから Cisco ISE サーバーへのデータのインポートを有効にするために、Cisco ISE CA 証明書または Cisco ISE 管理証明書を信頼することができます。

移行ツールで信頼できる証明書を有効にするには、次の手順を実行します。

- Cisco Secure ACS で、サーバー証明書が **[システム管理（System Administration）] > [設定（Configuration）] > [ローカル サーバー証明書（Local Server Certificates）] > [ローカル証明書（Local Certificates）]** ページにあることを確認します。証明書内の共通名（[サブジェクト（Subject）] フィールドの CN 属性）または DNS 名（[サブジェクト代替名（Subject Alternative Name）] フィールド内）は、接続の確立と Cisco Secure ACS からのデータのエクスポートのために [ACS5 クレデンシャル（ACS5 Credentials）] ダイアログボックスで使用されます。
- Cisco ISE で、サーバー証明書が **[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [証明書管理（Certificate Management）] > [システム証明書（System Certificates）]** ページにあることを確認します。共通名（[サブジェクト（Subject）] フィールドの CN 属性）または DNS 名（[サブジェクト代替名（Subject Alternative Name）] フィールド内）は、接続の確立と移行ツールから Cisco ISE へのデータのインポートのために [ISE クレデンシャル（ISE Credentials）] ダイアログボックスで使用されます。

ステップ 1 [Cisco Secure ACS to Cisco ISE Migration Tool] ウィンドウで、**[設定（Settings）] > [信頼できる証明書（Trusted Certificates）] > [追加（Add）]** を選択して、信頼できる通信を有効にする Cisco Secure ACS および Cisco ISE 証明書を追加します。

移行ツールで証明書を表示または削除できます。

ステップ 2 [開く（Open）] ダイアログボックスで、信頼できるルート証明書が格納されているフォルダを選択し、[開く（Open）] をクリックして、選択した Cisco ISE 証明書を移行ツールに追加します。

ステップ 3 前の手順を繰り返して、Cisco Secure ACS 証明書を追加します。

（注） Cisco Secure ACS および Cisco ISE のホスト名が IP アドレスに解決可能であることを確認します。

データ移行の推定時間

移行ツールは、次の構成を移行するのに約 5 時間稼働する可能性があります。

- 10,000 の内部ユーザー
- 4 個の ID グループ
- 16,000 台のネットワーク デバイス
- 512 個のネットワーク デバイス グループ
- 2 個の許可プロファイル（ポリシー セットの有無にかかわらず）
- 1 個のコマンド セット
- 42 個のシェル プロファイル
- 9 個のアクセス サービス（25 個の許可ルールを含む）

Cisco Secure ACS リリース 5.5 または 以降からの移行の準備

Cisco Secure ACS から正常に移行した後に簡易モードに変更しないことを推奨します。Cisco ISE に移行されたすべてのポリシーが失われる可能性があるからです。それらの移行されたポリシーを取得することはできませんが、簡易モードからポリシー セット モードに切替えることができます。

Cisco Secure ACS データを Cisco ISE に移行し始める前に、次のことを考慮してください。

- Cisco Secure ACS リリース 5.5 以降のデータは、Cisco ISE リリース 3.0 のポリシーセット モードでのみ移行します。
- サービス選択ポリシー（SSP）の有効なルールごとに1つのポリシーセットを生成し、SSP ルールの順序に従って順序付けします。

（注） SSP のデフォルトルールの結果であるサービスは、Cisco ISE リリース 3.0 のデフォルトポリシーセットになります。移行プロセスで作成されたすべてのポリシーセットで、最初の一致ポリシー セットが一致タイプになります。

ポリシー サービスの移行ガイドライン

Cisco Secure ACS から Cisco ISE へのポリシー サービスの移行中、次の点を確認してください。

- サービス選択ポリシー（SSP）に、Cisco Secure ACS リリース 5.5 以降で無効になっているか、またはモニターされている SSP ルールが含まれている場合、それらは Cisco ISE に移行されません。
- サービス選択ポリシー（SSP）に、Cisco Secure ACS リリース 5.5 以降で有効な SSP ルールが含まれている場合は、次のようになります。
  - サービスを要求していて、そこにグループ マッピング ポリシーが含まれている場合、Cisco ISE に移行されません。Cisco ISE は、グループ マッピング ポリシーをサポートしません。

    特定のアクセス サービスにグループ マッピングが含まれている場合、移行ツールはそれをポリシー ギャップ分析レポートに警告として表示し、そのアクセス サービスに関連する許可ルールを移行します。
  - サービスを要求し、その ID ポリシーにルールが含まれ、それが RADIUS ID サーバーになる場合、Cisco ISE に移行されません（Cisco ISE はこれとは異なり、認証に RADIUS ID サーバーを使用します）。
  - サービスを要求し、そこに Cisco ISE でサポートされていない属性またはポリシー要素を使用するポリシーが含まれている場合、Cisco ISE に移行されません。

Cisco Secure ACS ポリシー ルールの移行ガイドライン

ルールを移行できない場合、データ整合性だけでなくセキュリティ面からも、ポリシーモデル全体を移行できません。ポリシーのギャップ分析レポートで問題のあるルールの詳細情報を表示できます。サポート対象外のルールを修正または削除しなかった場合、ポリシーは Cisco ISE へ移行されません。

一般に、Cisco Secure ACS リリース 5.5 以降から Cisco ISE リリース 3.0 にデータを移行する際は、次のルールを考慮する必要があります。

- enum 型の属性（RADIUS、VSA、ID、およびホスト）は、使用可能な値を持つ整数として移行される。
- （属性のデータ型に関係なく）すべてのエンドポイント属性は String データ型として移行される。

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。