Cisco Secure ACS から Cisco ISE へのデータの移行

この章では、移行ツールを使用して、Cisco Secure ACS リリース 以降のデータを Cisco ISE リリース 3.0 システムにエクスポートおよびインポートする方法について説明します。

Cisco Secure ACS からのデータのエクスポート

移行ツールの起動後、次の手順を実行して、Cisco Secure ACS から移行ツールにデータをエクスポートします。

ステップ 1 [Cisco Secure ACS to Cisco ISE Migration Tool] ウィンドウで [設定（Settings）] をクリックして、移行に使用できるデータ オブジェクトのリストを表示します。

ステップ 2 （任意）移行を実行するために、依存関係処理を設定する必要はありません。従属データがない場合は、エクスポートするデータ オブジェクトのチェック ボックスをオンにして、[保存（Save）] をクリックします。

ステップ 3 [Cisco Secure ACS to Cisco ISE Migration Tool] ウィンドウで [移行（Migration）] をクリックし、[ACS からのエクスポート（Export from ACS）] をクリックします。

ステップ 4 Cisco Secure ACS リリース 5.5 以降のシステムの場合は Cisco Secure ACS のホスト名、ユーザー名、およびパスワード、[ACS5クレデンシャル（ACS5 Credentials）] ウィンドウで [接続（Connect）] をクリックします。

[Cisco Secure ACS to Cisco ISE Migration Tool] ウィンドウで移行プロセスをモニターできます。ウィンドウには、正常にエクスポートされた現在のオブジェクト数、および警告やエラーの原因となったオブジェクトが表示されます。

エクスポートプロセスで発生した警告またはエラーについて詳しい情報を取得するには、[移動（Migrations）] タブの [警告（Warnings）] または [エラー（Errors）] カラムで下線の付いた数字をクリックします。[オブジェクト エラーと警告の詳細（Object Errors and Warnings Details）] ウィンドウに、エクスポート中に発生した警告またはエラーの結果が表示されます。警告またはエラーのオブジェクト グループ、タイプ、および日時が示されます。

ステップ 5 スクロールして、選択したオブジェクトのエラーの詳細を表示し、[閉じる（Close）] をクリックします。

ステップ 6 データ エクスポート プロセスが完了したら、[Cisco Secure ACS to Cisco ISE Migration Tool] ウィンドウに、エクスポートが終了したときのエクスポートのステータスが表示されます。

ステップ 7 [エクスポート レポート（Export Report(s)）] をクリックして、エクスポート レポートの内容を表示します。

ステップ 8 Cisco Secure ACS と Cisco ISE 間のポリシー ギャップを分析するには、[ポリシー ギャップ分析レポート（Policy Gap Analysis Report）] をクリックします。

（注） 移行ツールは、エクスポートされたオブジェクトのキャッシュを保持し、その後のエクスポートのためにキャッシュを取得します。

エクスポート時のパスワードのコンプライアンス

移行ツールは、エクスポート プロセス中にパスワードのコンプライアンスを遵守します。

- **パスワードの複雑度**

  次に、ユーザーのパスワードがパスワードの複雑度要件を満たしていない場合にエクスポート プロセス中に発生するエラー メッセージの一覧を示します。

  「ユーザー：パスワードがパスワードの複雑度と一致しないためエクスポートできませんでした（*user: Failed to Export because its password does not match with the password Complexity*）」

  「パスワードの長さは *5* 文字以上にしてください。（*Password length should be minimum of '5' characters.*）」

  「パスワードには、「*cisco*」またはその文字の逆順は使用できません。（*Password should not contain 'cisco' or its characters in reverse.*）」

  「パスワードには、「*hello*」またはその文字の逆順は使用できません。（*Password should not contain 'hello' or its characters in reverse.*）」

  「パスワードには、*4* 回以上連続する繰り返し文字は使用できません。（*Password should not contain repeated characters four or more times consecutively.*）」

  「パスワードには、小文字が少なくとも *1* 文字含まれている必要があります。（*Password should contain at least one Lower case character.*）」

「パスワードには、大文字が少なくとも *1* 文字含まれている必要があります。（*Password should contain at least one Upper case character.*）」

「パスワードには、数字が少なくとも *1* 文字含まれている必要があります。（*Password should contain at least one Numeric Character.*）」

「パスワードには、英数字以外の文字が少なくとも *1* 文字含まれている必要があります。（*Password should contain at least one non alphanumeric characters.*）」

- **パスワード ハッシュ**

  Cisco Secure ACS で内部ユーザーのパスワード ハッシュを有効にして内部ユーザーをエクスポートしようとすると、移行ツールに次のエラー メッセージが表示されます。

  「ユーザー：*ISE* でサポートされていないパスワード ハッシュで設定されているためエクスポートできませんでした。この設定を *ACS* で無効にしてから、再度エクスポートしてください。（*user: Failed to Export because its configured with Password Hash which is not supported by ISE, disable this configuration in ACS and export again.*）」

Cisco ISE へのデータのインポート

ステップ 1 [Cisco Secure ACS to Cisco ISE Migration Tool] ウィンドウで、[ISE へのインポート（Import To ISE）] をクリックします。

ステップ 2 データを Cisco ISE へインポートする前に、LDAP ID ストアに属性を追加するようプロンプトが表示されたら、[OK] をクリックします。

ステップ 3 [LDAP IDストア（LDAP Identity Store）] ドロップダウン リストから、属性を追加する ID ストアを選択し、[属性の追加（Add Attribute）] をクリックします。

ステップ 4 [属性名（Attribute Name）] フィールドに名前を入力し、[属性タイプ（Attribute Type）] ドロップダウン リストから属性タイプを選択します。[デフォルト値（Default Value）] フィールドに値を入力して [保存して終了（Save & Exit）] をクリックします。

ステップ 5 属性を追加したら、[ISE へのインポート（Import To ISE）] をクリックし、[ISE クレデンシャル（ISE Credentials）] ウィンドウに Cisco ISE の完全修飾ドメイン名（FQDN）、ユーザー名、およびパスワードを入力して [接続（Connect）] をクリックします。

ステップ 6 データ インポート プロセスが完了したら、[Cisco Secure ACS to Cisco ISE Migration Tool] ウィンドウに、**インポートが終了**したときのインポートのステータスが表示されます。

ステップ 7 インポートされたデータの詳細レポートを表示するには、[インポート レポート（Import Report(s)）] をクリックします。

ステップ 8 インポートプロセスで発生した警告またはエラーについて詳しい情報を取得するには、[移行（Migrations）] タブの [警告（Warnings）] または [エラー（Errors）] カラムで下線の付いた数字をクリックします。

ステップ 9 Cisco Secure ACS と Cisco ISE 間のポリシー ギャップを分析するには、[ポリシー ギャップ分析レポート（Policy Gap Analysis Report）] をクリックします。

ステップ 10 [ログ コンソールの表示（View Log Console）] をクリックすると、エクスポートまたはインポート処理のリアルタイム ビューを表示できます。

Cisco ISE での移行されたデータの検証

Cisco Secure ACS 5.5 以降のデータが Cisco ISE 3.0 に移行されたことを確認するには、Cisco ISE にログインし、さまざまな Cisco Secure ACS オブジェクトを表示できることを確認します。

失敗したデータ移行の再開

移行ツールは、インポート操作またはエクスポート操作の各段階でチェックポイントを保持します。これは、インポートまたはエクスポートプロセスが失敗しても、プロセスを最初から再起動する必要がないことを意味します。障害発生前の最後のチェックポイントから開始できます。

移行プロセスが失敗すると、移行ツールはプロセスを終了します。障害の後で移行ツールを再起動すると、ダイアログボックスが表示され、以前のインポートまたはエクスポートを再開するか、または、以前のプロセスを破棄し、新しい移行プロセスを開始するか選択できます。前のプロセスを再開することを選択した場合、移行プロセスは最後のチェックポイントから再開されます。障害が発生した時点から再開する場合、前のプロセスから実行するためにレポートも再開されます。

シングル Cisco Secure ACS アプライアンスからのデータの移行

始める前に

Cisco Secure ACS リリース 5.5 移行のデータを Cisco ISE リリース 3.0 に移行する準備ができたら、それがスタンドアロンの Cisco ISE ノードであることを確認します。移行が正常に終了した後に、何らかの展開設定（Administrator ISE や Policy Service ISE のペルソナの設定など）を開始することができます。

移行のインポート フェーズは、サポートされているハードウェア アプライアンス上で、Cisco ISE ソフトウェアの新しい「クリーンな」インストールにおいて実行する必要があります。サポートされるハードウェアアプライアンスの一覧については、『*Cisco Identity Services Engine Hardware Installation Guide, Release 3.0*』を参照してください。

ご使用の環境内にシングル Cisco Secure ACS アプライアンスがある場合（または複数の Cisco Secure ACS アプライアンスがあるが、分散した設定内にない場合）は、移行ツールを Cisco Secure ACS アプライアンスに対して実行します。

Cisco Secure ACS および Cisco ISE が同じハードウェア（CSACS-1121 アプライアンス）を使用している場合は、移行ツールと次の移行手順を使用できます。

ステップ 1 スタンドアロンの Windows または Linux マシンに移行ツールをインストールします。

ステップ 2 Cisco Secure ACS-1121 ハードウェア アプライアンスから、データベースを持つセキュアな外部サーバーへ Cisco Secure ACS リリース 5.5 以降のデータをエクスポートします。

ステップ 3 Cisco Secure ACS のデータをバックアップします。

ステップ 4 サポートされている Cisco ISE アプライアンスと同じ物理ハードウェアを持つ Cisco Secure ACS-1121 ハードウェアアプライアンスのイメージを、Cisco ISE リリース 3.0 ソフトウェアで再適用します。

ステップ 5 変換された Cisco Secure ACS のデータを、セキュアな外部サーバーから Cisco ISE にインポートします。

分散環境からのデータの移行

始める前に

大規模な内部データベースがある場合、シスコではスタンドアロンのプライマリアプライアンスから移行を実行し、複数のセカンダリアプライアンスに接続されているプライマリアプライアンスからの移行は実行しないことを推奨しています。移行プロセスの完了後、セカンダリアプライアンスを登録できます。

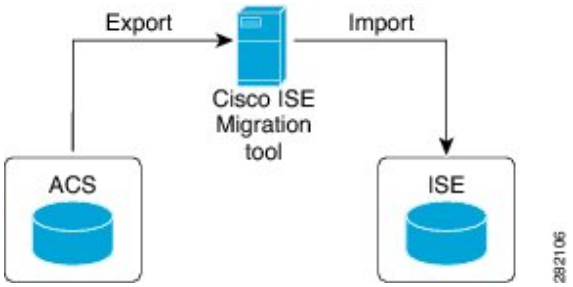
分散環境では、1 つのプライマリ Cisco Secure ACS アプライアンス、およびこのプライマリ アプライアンスと相互運用する 1 つ以上のセカンダリ Cisco Secure ACS アプライアンスがあります。

分散環境で Cisco Secure ACS を実行する場合は、以下のようにする必要があります。

ステップ 1 プライマリ Cisco Secure ACS アプライアンスをバックアップし、それを移行マシン上で復元します。

ステップ 2 プライマリ Cisco Secure ACS アプライアンスに対して移行ツールを実行します。

図 *1*：異なるアプライアンスにインストールされている *Cisco Secure ACS* および *Cisco ISE*



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。