ACS 5.2 との Nexus 統合の設定例

目次

概要

この資料は Nexus スイッチで TACACS+ 認証設定の例を提供したものです。 デフォルトで Access Control Server （ ACS ）によって認証するために Nexus スイッチを設定すれば読み取り専用アクセスを提供するネットワーク オペレータ/vdc オペレータ ロールに自動的に置かれます。 ネットワーク admin/vdc admin ロールに置かれるために、ACS 5.2 のシェルを作成する必要があります。 この資料はそのプロセスを説明したものです。

前提条件

要件

この設定を行う前に、次の要件が満たされていることを確認します。

- ACS のクライアントと Nexus スイッチを定義して下さい。
- ACS および Nexus の IP アドレスおよび同一の共有秘密キーを定義して下さい。

注: 変更を行なう前に Nexus のチェックポイントかバックアップを作成して下さい。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- ACS 5.2
- Nexus 5000、5.2(1)N1(1)

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

設定

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

注: このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

ACS 5.2 設定の認証 および 権限のための Nexus デバイス

次の手順を実行します。

1. フォールバックのための完全な特権で Nexus スイッチのローカルユーザを作成して下さい:

```
username admin privilege 15 password 0 cisco123!
```

2. TACACS+ を有効に し、そして TACACS+ サーバ（ACS）の IP アドレスを提供して下さい:

```
feature tacacs+


tacacs-server hostIP-ADDRESS key KEY


tacacs-server key KEY


tacacs-server directed-request


aaa group server tacacs+ ACS


server IP-ADDRESS


use-vrf management


source-interface mgmt0
```

注: キーはこの Nexus デバイスのための ACS で設定される共有秘密を一致する必要があり

ます。
3. TACACSサーバ アベイラビリティをテストして下さい:

```
test aaa group group-name username password
```

テスト認証はサーバからのリジェクト メッセージとサーバが設定されなかったので失敗する必要があります。 このリジェクト メッセージは TACACS+ サーバが到達可能であることを確認します。
4. ログイン認証を設定して下さい:

```
aaa authentication login default group ACS


aaa authentication login console group ACS


aaa accounting default group ACS


aaa authentication login error-enable


aaa authorization commands default local


aaa authorization config-commands default local
```

注: Nexus は認証サーバが到達不能である場合ローカル認証を使用します。

ACS 5.x の設定

次の手順を実行します。

1. **ポリシー要素 > 認証**へのナビゲート**および権限 > デバイス Administration > シェル プロファイル** シェル プロファイルを作成するため。
2. プロファイル名を入力します。
3. [Custom Attributes] タブで次の値を入力します。[Attribute]： cisco-av-pair要件： Mandatory[Value]： シェル： roles* "ネットワーク admin vdc admin」
4. Nexus スイッチの属性ベースのロールを作成するため、変更内容を送信します。
5. 新しい承認規則を作成するか、または正しいアクセスポリシーの既存のルールを、編集して下さい。 デフォルトで、TACACS+ 要求は **Default Device Admin** アクセス ポリシーによって処理されます。
6. [Conditions] 領域で、該当する条件を選択します。 結果エリアで、Nexus OS シェル プロファイルを選択して下さい。
7. [OK] をクリックします。

確認

ここでは、設定が正常に動作していることを確認します。

Output Interpreter Tool（OIT）（登録ユーザ専用）では、特定の **show** コマンドがサポートされています。 OIT を使用して、**show** コマンド出力の解析を表示できます。

- **TACACS+ —**表示します TACACS+ 統計情報を**示して下さい**。
- **show running-config は TACACS+ —** 実行コンフィギュレーションの TACACS+ 設定を表示します。
- **show startup-config は TACACS+ —** スタートアップ コンフィギュレーションの TACACS+ 設定を表示します。
- **tacacs-server —**表示しますすべての設定された TACACS+ サーバ パラメータを**示して下さい**。

関連情報

- **テクニカル サポートとドキュメント – Cisco Systems**