ACS 5.4 との NCS 統合の設定例

目次

概要

このドキュメントでは、Cisco Prime Network Control System（NCS）リリース 1.1 上での TACACS+ 認証および認可の設定例について説明します。

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。

- NCS をアクセス コントロール システム（ACS）内のクライアントとして定義します。
- ACS と NCS 上の IP アドレスおよび同一の共有秘密キーを定義します。

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 バージョン 5.4
- NCS Prime リリース 1.1

このドキュメントの情報は、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、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく

必要があります。

設定

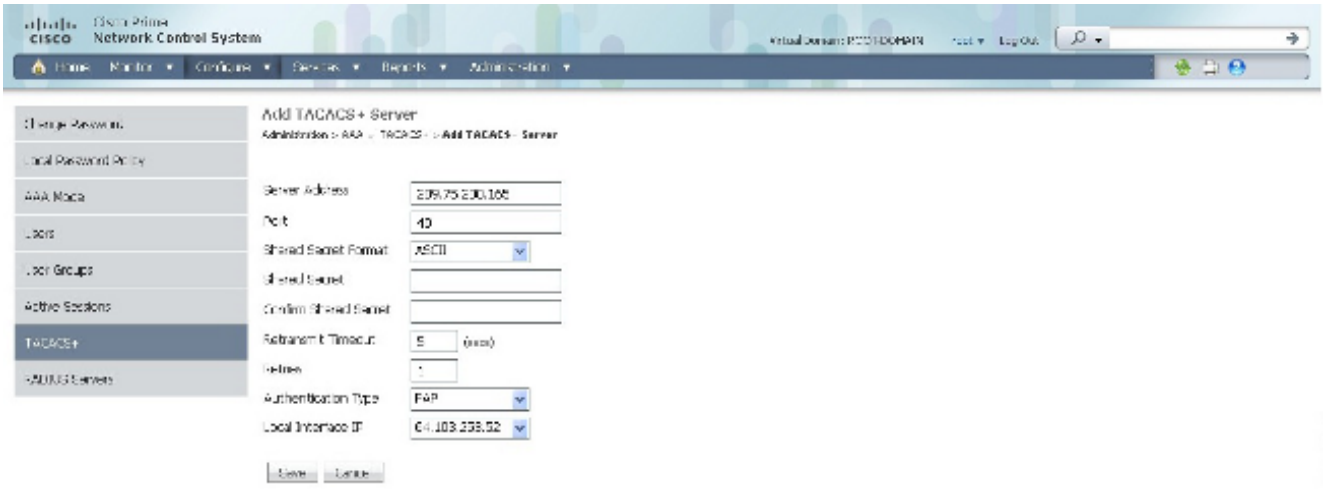
このセクションでは、このドキュメントで説明されている機能を設定するために使用される情報を提供します。

> **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。

TACACS サーバとしての ACS の追加

次の手順を実行して、ACS を TACACS サーバとして追加します。

1. [Administration] > [AAA] に移動します。
2. 左側のサイドバー メニューから [TACACS+] を選択すると、次の情報が表示されます。



[TACACS+] ページには、IP アドレス、ポート、再送信レート、および認証タイプが表示されます。

3. ACS サーバの IP アドレスを追加します。
4. ACS サーバで使用される TACACS+ 共有秘密を入力します。
5. [Confirm Shared Secret] テキスト ボックスに共有秘密を再度入力します。
6. 残りのフィールドはデフォルト設定のままにします。
7. [Submit] をクリックします。

AAA モードの設定

認証、認可、およびアカウンティング（AAA ）モードを選択するには、次の手順を実行します。

1. [Administration] > [AAA] に移動します。

2. 左側のサイドバー メニューから [AAA Mode] を選択すると、次の情報が表示されます。

3. [TACACS+] を選択します。

4. 外部の AAA サーバがダウンしたときに管理者にローカル データベースを使用させる場合は、[Enable Fallback to Local] チェックボックスをオンにします。 この設定は、TACACS+ サーバで障害が発生しても認証が実行されるようにするために推奨されています。 設定の内容を確認して作動したら、必要に応じて変更を加えることができます。

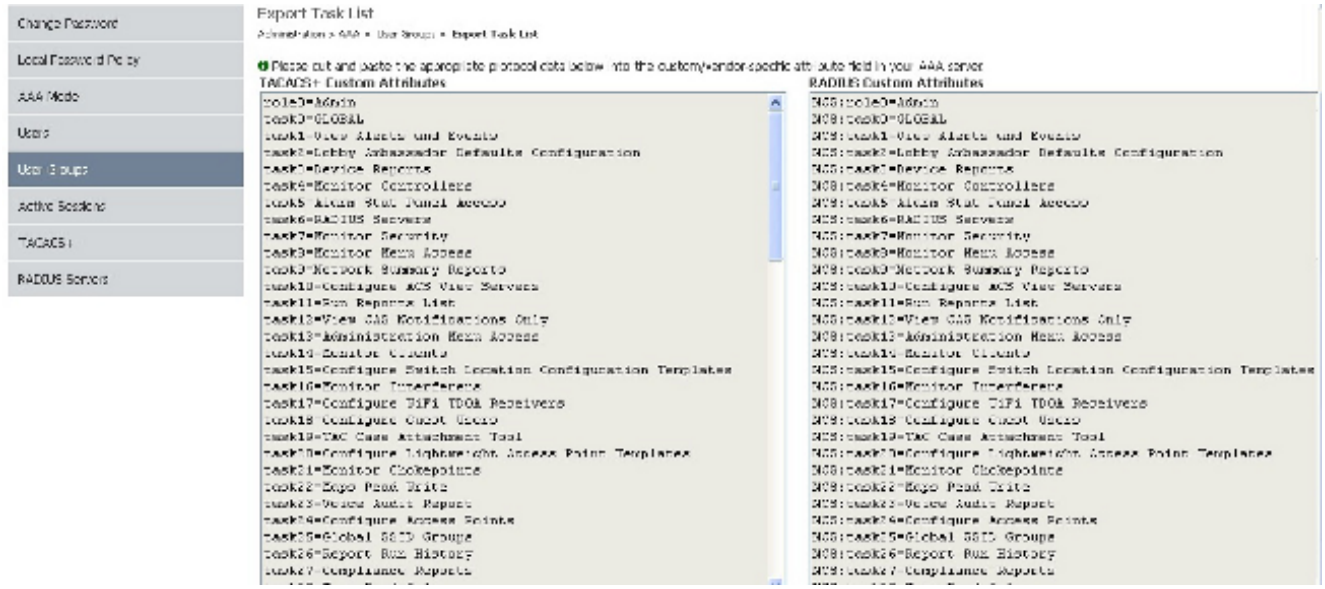
ASA バージョン 5.4 の設定

ACS バージョン 5.4 の設定では、ACS から NCS に属性を送信するために次の手順を実行する必要があります。

1. 属性を取得します。

   [Administration] > [AAA] > [User Groups] の順に移動します。

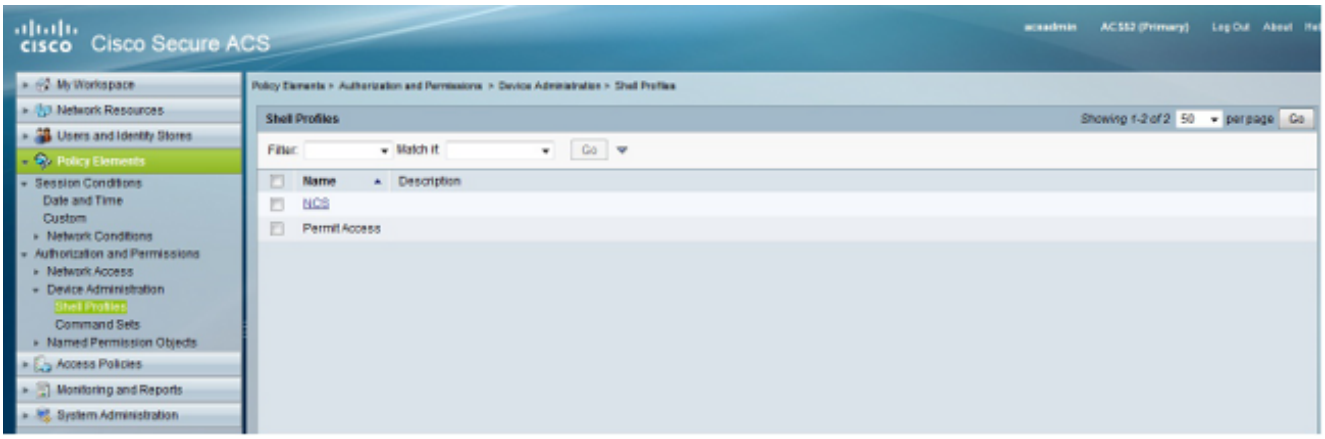
   次の例は、管理者の認証を示しています。 リストで [Admin Group Name] を探して、その右側にある [Task List] オプションをクリックします。



2. 属性をエクスポートしてデスクトップに保存します。

3. **ACS 管理者 GUI** にログインして、[Policy Elements] > [Authentication and Permissions] > [Device Administration] > [Shell Profiles] の順に移動し、シェル プロファイルを作成します。

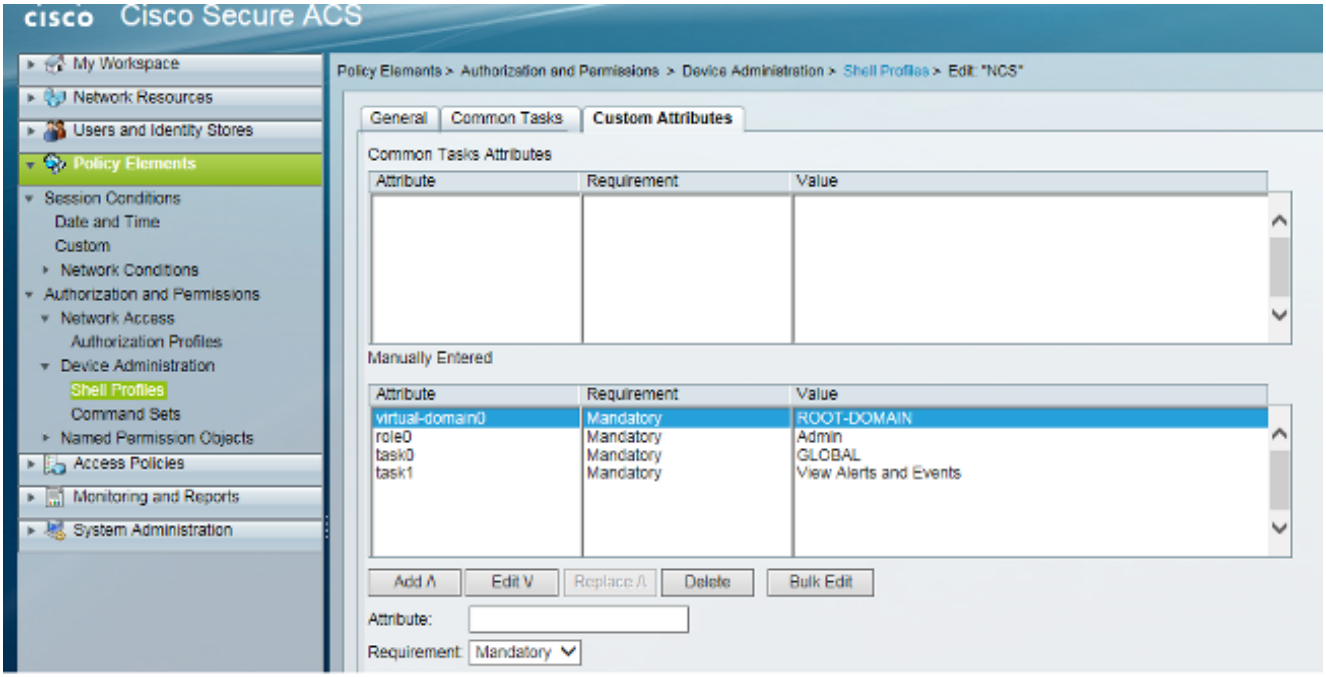
4. プロファイルに **NCS** という名前を付けます。



5. [Custom Attributes] タブで、次の値を入力します。

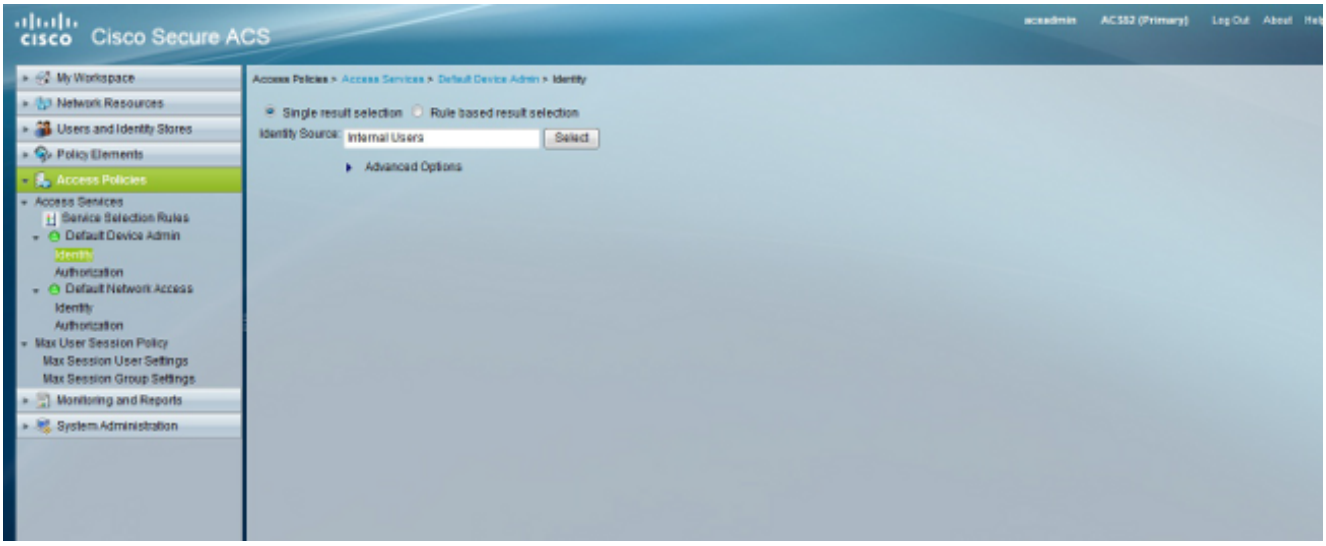
```
Attribute          Requirement    Value
-----------------------------------------------------
role0               Mandatory     Admin
task0               Mandatory     GLOBAL
task1               Mandatory     View Alerts and Events
Virtual-domain0     Mandatory     ROOT-DOMAIN
```

注: NCS の最新リリースを使用する場合は、仮想ドメインがリストに含まれています。 ユーザ仮想ドメインを定義する必要があります。

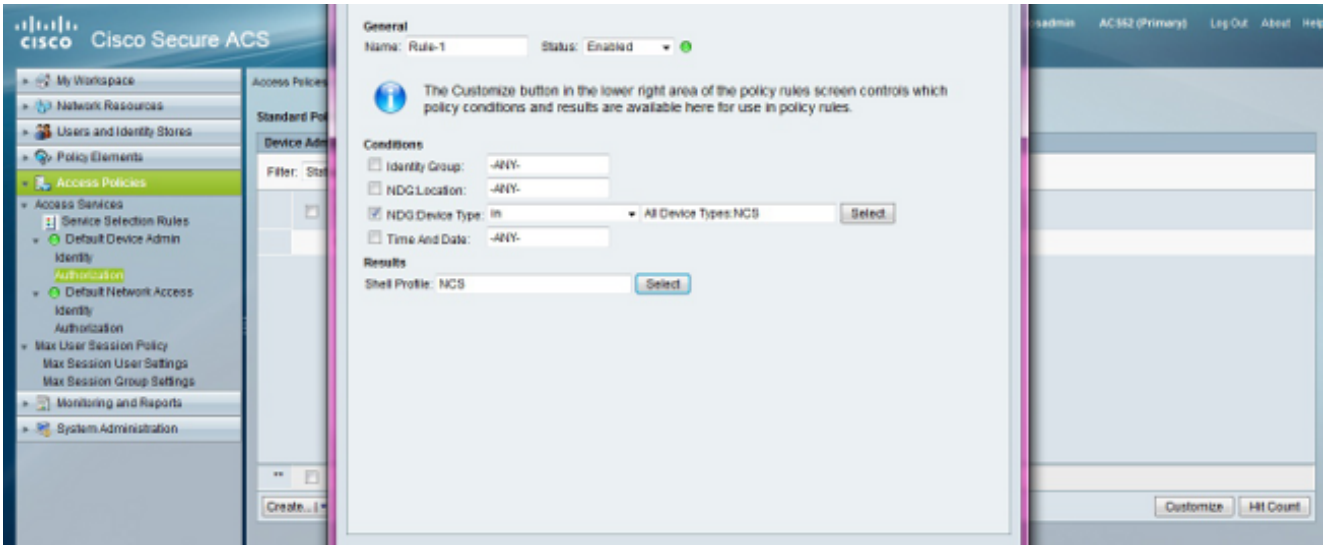


6. NCS の属性ベースのロールを作成するために変更を送信します。

7. [Access Policies] > [Access Services] > [Default Device Admin] > [Identity] の順に移動して、[Identity Source] に対して [Internal Users] を選択します。



8. 新しい認可ルールを作成するか、正しいアクセス ポリシー内にすでに存在するルールを編集します。 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。



9. [Conditions] 領域で、該当する条件を選択します。 [Results] 領域で、[Shell Profile] に対して [NCS] を選択します。

10. [OK] をクリックします。

確認

NCS にログインして、**管理者**ロールが付与されていることを確認します。

トラブルシューティング

NCS にログインできない場合は、ACS GUI にログインして、[Monitoring and Reports] > [Catalog] > [AAA Protocols] > [TACACS+ Authentication] の順に移動します。 失敗した認証を選択して [Details] を選択し、認証が失敗した理由または拒否された理由を確認します。