Nexus 上での RADIUS を使用した ACS 制限付きユーザ アクセスの設定例

目次

概要

このドキュメントでは、Nexus ユーザに制限付きアクセスを付与する方法を説明します。これにより、Nexus ユーザは Cisco Secure Access Control Server（ACS）を RADIUS サーバとして使用して、限られたコマンドだけを入力できます。 たとえば、ユーザが特権モードまたはコンフィギュレーション モードでログインでき、ユーザに対してインターフェイス コマンドの実行だけを許可するとします。 このためには、使用する RADIUS サーバでそのユーザに対しカスタム ロールを作成する必要があります。

前提条件

要件

RADIUS サーバ（この例では ACS）と Nexus は、相互に通信し、認証を実行できる必要があります。

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.x

- Nexus 7000 スイッチ

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

Nexus でのカスタム ロールの設定

インターフェイス コマンドのみ読み取り/書き込みアクセス権だけを付与するロールを作成するため、次のように入力します。

```
switch(config)# role name Limited-Access
switch(config-role)# rule 1 permit read-write feature interface
```

追加の許可アクセス ルールが次の構文で定義されます。

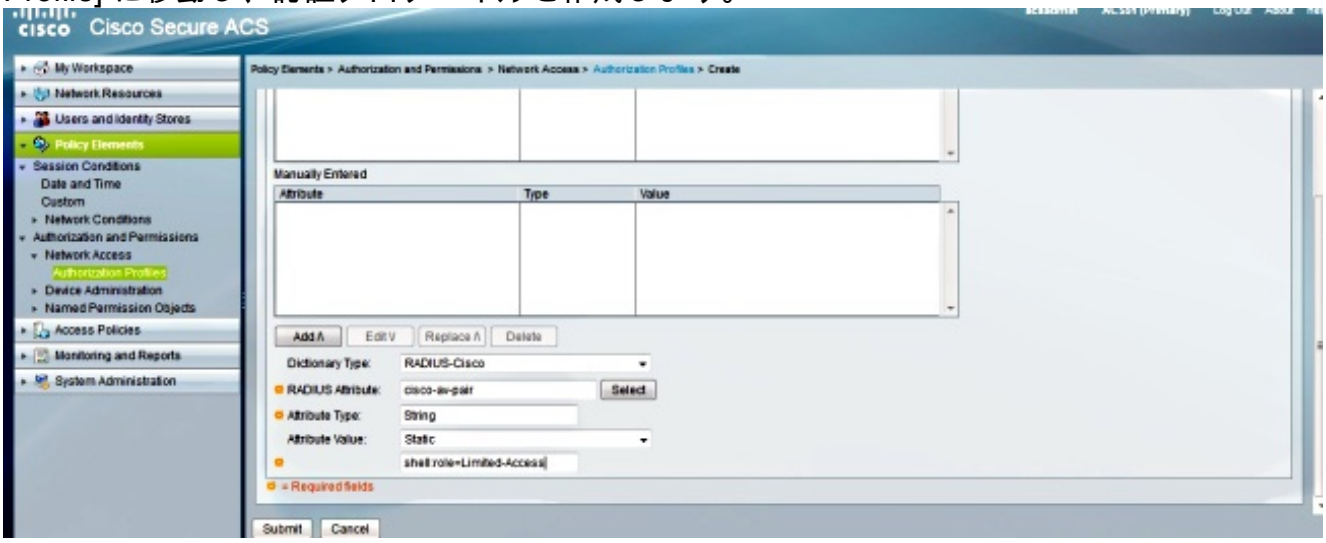
```
switch(config-role)# rule 1 permit read-write feature snmp
switch(config-role)# rule 2 permit read-write feature snmp
TargetParamsEntry
switch(config-role)# rule 3 permit read-write feature snmp
TargetAddrEntry
```

認証および認可のための Nexus の設定

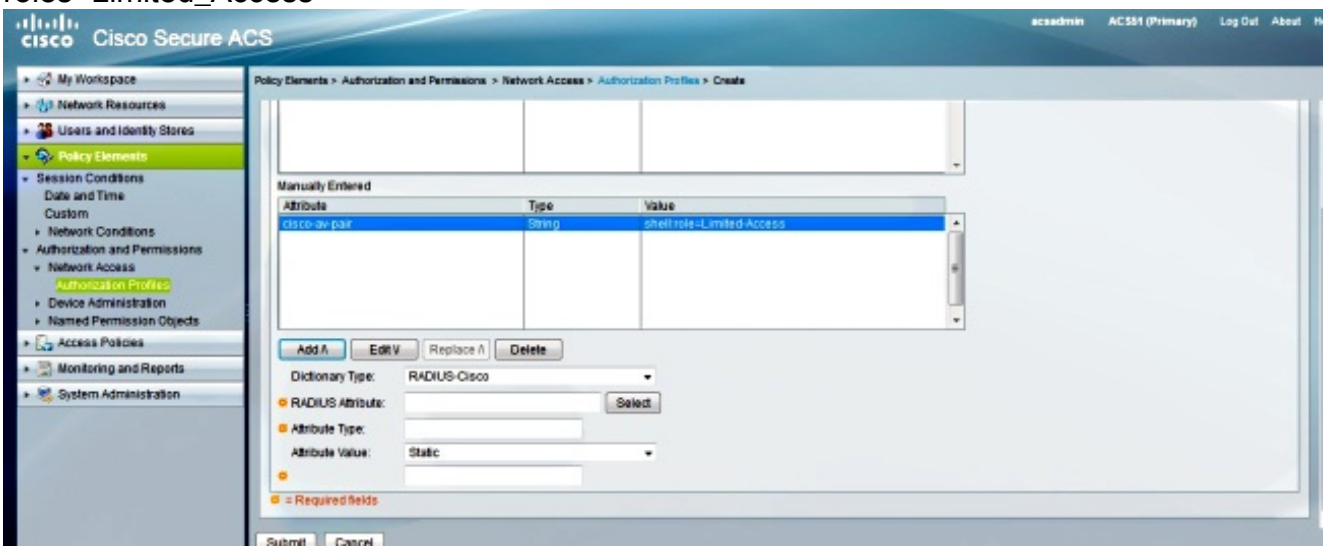
1. フォールバックのすべての特権を持つローカル ユーザをスイッチ上で作成するには、**username コマンド**を入力します。
   `Switch(config)#username admin privilege 15 password 0 cisco123!`
2. RADIUS サーバ（ACS）の IP アドレスを指定するため、次のように入力します。
   ```
   switch# conf terminal
   switch(config)# Radius-server host 10.10.1.1 key cisco123
   authenticationaccounting
   switch(config)# aaa group server radius RadServer
   switch(config-radius)#server 10.10.1.1
   switch(config-radius)# use-vrf Management
   ```
   注: このキーは、この Nexus デバイスのために RADIUS サーバで設定されている共有秘密と一致する必要があります。
3. RADIUS サーバの可用性をテストするため、**test aaa コマンド**を入力します。
   `switch# test aaa server Radius 10.10.1.1 user1 Ur2Gd2BH`まだ設定されていないため、テスト認証はサーバからの拒否で失敗するはずです。 ただし、サーバが到達可能であることが確認されます。
4. ログイン認証を設定するため、次のように入力します。`Switch(config)#aaa authentication login default group Radserver`
   `Switch(config)#aaa accounting default group Radserver`
   `Switch(config)#aaa authentication login error-enable`RADIUS サーバが使用できない場合、Nexus はそれ自体のローカルにフォールバックするため、ローカル フォールバック方法について心配する必要はありません。

ACS の設定

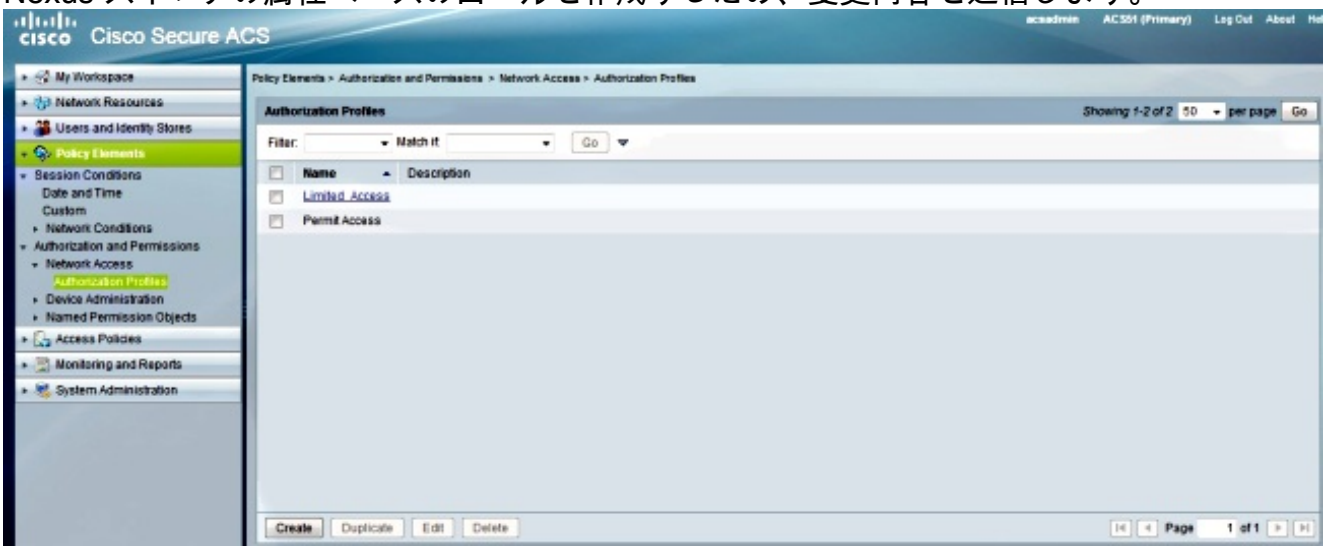
1. [Policy Elements] > [Authentication and Permissions] > [Network Access] > [Authorization Profile] に移動し、認証プロファイルを作成します。



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。
   ディクショナリ タイプ： Radius-Cisco[Attribute]： cisco-av-pair要件： Mandatory[Value]：シェル：
   roles=Limited_Access



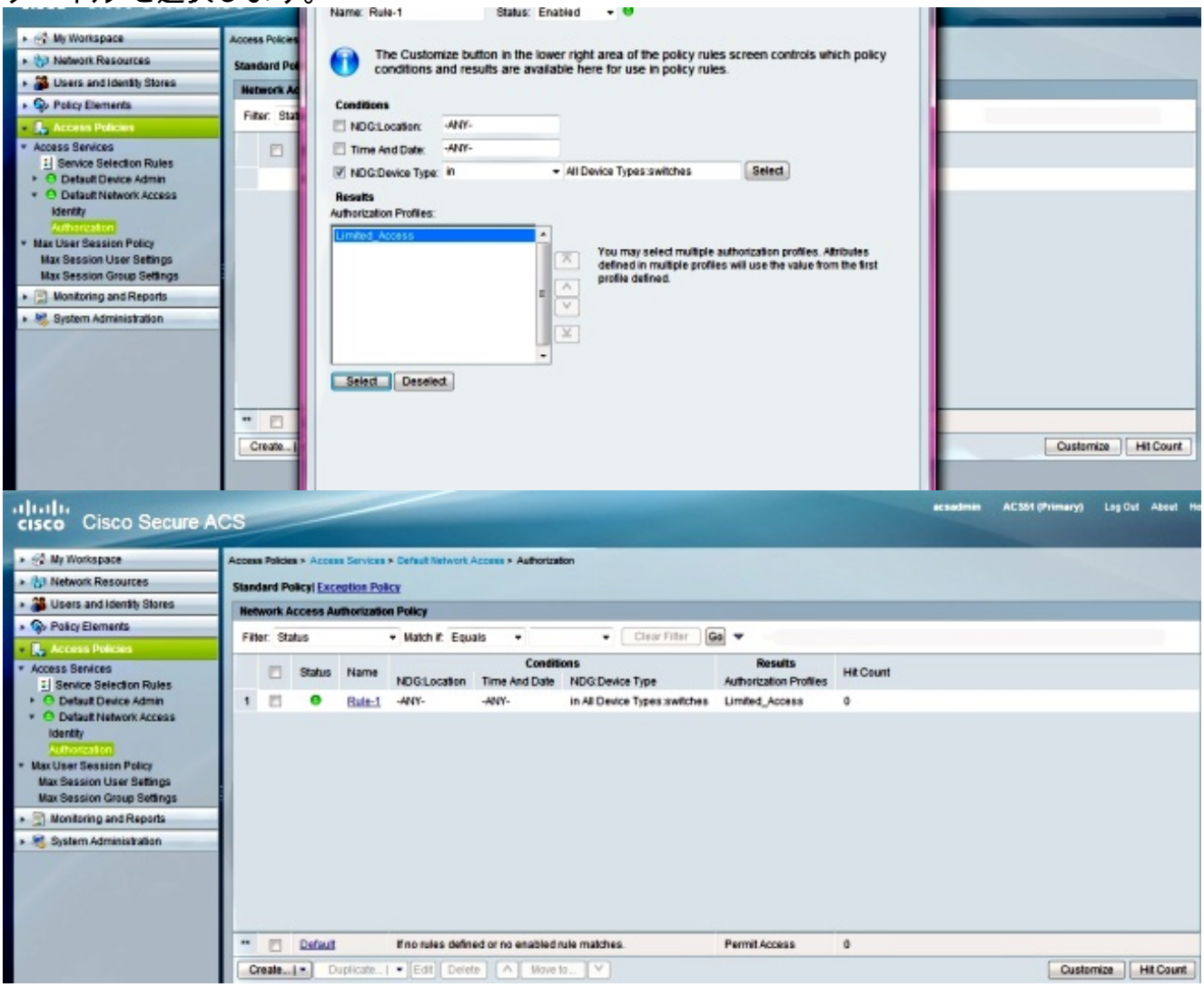
4. Nexus スイッチの属性ベースのロールを作成するため、変更内容を送信します。



5. 新しい認証ルールを作成するか、または正しいアクセス ポリシーで現在のルールを編集します。 デフォルトでは、RADIUS 要求はネットワーク 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。 [Results] 領域で、[Limited_Access] プロファイル を選択します。



7. [OK] をクリックします。

確認

このセクションでは、設定が正常に機能していることを確認します。

Nexus ロールの検証

定義されているロールと設定されているアクセス ルールを表示するため、Nexus で **show role** コマンドを入力します。

```
switch# show role (Displays all the roles and includes
custom roles that you have created and their permissions.)

Role: network-admin

Description: Predefined network admin role has access to all
commands on the switch.
------------------------------------------------------------------
Rule Perm Type Scope Entity
------------------------------------------------------------------
```

```
1 permit read-write

Role:Limited_Access
Description: Predefined Limited_Access role has access to these commands.
-------------------------------------------------------------------
Rule Perm Type Scope Entity
-------------------------------------------------------------------
1 permit read-write feature Interface
```

Nexus ユーザ ロール割り当ての検証

ACS で設定されたユーザ名とパスワードを使用して Nexus にログインします。 ログイン後、**show user-account** コマンドを入力して、テスト ユーザに Limited_Access ロールが割り当てられていることを確認します。

```
switch# show user-account
user:admin
this user account has no expiry date
roles:network-admin

user:Test
this user account has no expiry date
roles:Limited_Access
```

ユーザ アクセス ロールを確認したら、コンフィギュレーション モードに切り替え、インターフェイス コマンド以外のコマンドを入力してください。 ユーザに対しアクセスが拒否されるはずです。

特定の show コマンドがアウトプット インタープリタ ツール（登録ユーザ専用）でサポートされています。 show コマンド出力の分析を表示するには、アウトプット インタープリタ ツールを使用します。

- **show role**：ロールの定義と設定されているアクセス ルールを表示します。
- **show user-account**：ユーザ アカウントの詳細（ロール割り当てを含む）を表示します。

トラブルシューティング

ここでは、スイッチの設定のトラブルシューティングに役立つ情報を提供します。

ロールを割り当てるため、スイッチで次の手順を実行します。

1. **show running-config aaa** コマンドと **show aaa authentication** コマンドを使用して、認証に使用される AAA グループを確認します。
2. RADIUS では、**show aaa authentication** コマンドと **show running-config radius コマンド**を使用して、AAA グループとの Virtual Routing and Forwarding（VRF）関連付けを確認します。
3. これらのコマンドで関連付けが正しいことが確認できたら、**debug radius all** コマンドを入力して、トレース ロギングを有効化します。
4. 正しい属性が ACS からプッシュされることを確認します。

特定の show コマンドがアウトプット インタープリタ ツール（登録ユーザ専用）でサポートされています。 show コマンド出力の分析を表示するには、アウトプット インタープリタ ツールを使用します。

注: debug コマンドを使用する前に、『**debug コマンドの重要な情報**』を参照してください。

- show running-config aaa-
- show aaa authentication-
- show running-config radius
- debug radius all