Acesso de usuário limitado ACS com RAIO no exemplo de configuração do nexo

Índice

[Introdução](#)
[Pré-requisitos](#)
[Requisitos](#)
[Componentes Utilizados](#)
[Configurar](#)
[Configuração dos papéis personalizados no nexo](#)
[Configurar o nexo para a authentication e autorização](#)
[Configuração do ACS](#)
[Verificar](#)
[Verificação do papel do nexo](#)
[Papel de usuário da verificação da atribuição do nexo](#)
[Troubleshooting](#)

Introdução

Este documento descreve como fornecer o acesso restrito aos usuários do nexo de modo que possam somente incorporar comandos limitados com Serviço de controle de acesso Cisco Secure (ACS) como um servidor Radius. Por exemplo, você pôde querer um usuário poder entrar a um privilegiado ou a um modo de configuração e somente ser reservado inscrever comandos interface. A fim conseguir isto, você deve criar um papel personalizado para o usuário no servidor Radius que é usado.

Pré-requisitos

Requisitos

O servidor Radius (ACS neste exemplo) e o nexo devem poder contactar-se e executar autenticações.

[Componentes Utilizados](#)

As informações neste documento são baseadas nestas versões de software e hardware:

- Versão de ACS 5.x

- 7000 Switch do nexo

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Configurar

Configuração dos papéis personalizados no nexo

A fim criar um papel que forneça somente o acesso de leitura/gravação para o comando interface, entre:

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

As regras adicionais do acesso da licença são definidas com esta sintaxe:

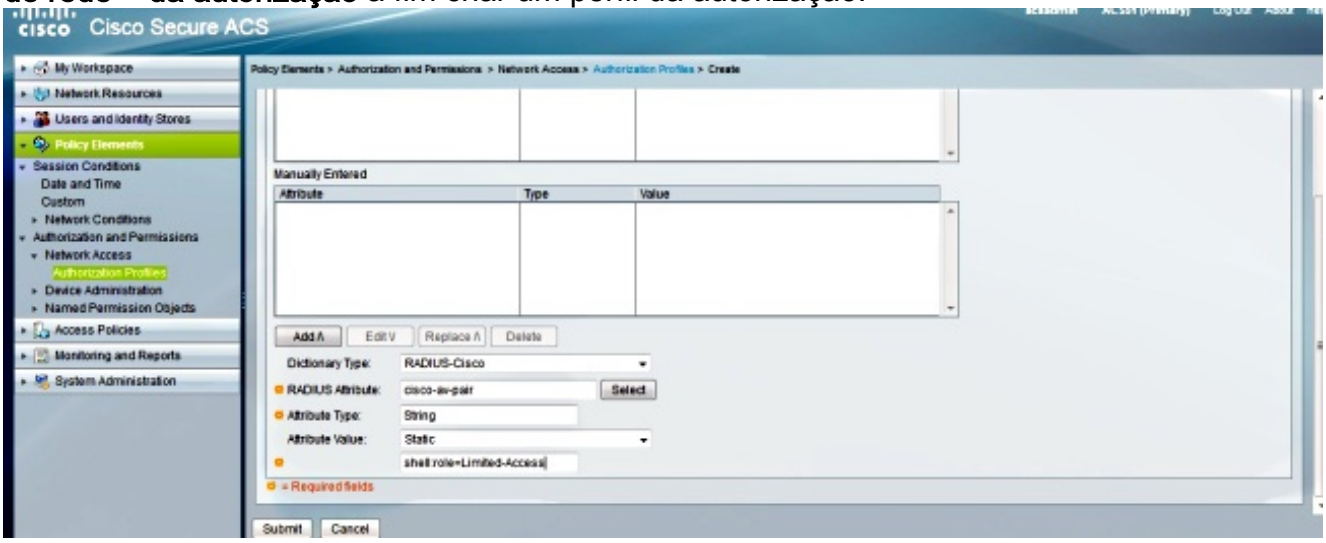
```
switch(config-role)# rule 1 permit read-write feature snmp
switch(config-role)# rule 2 permit read-write feature snmp
TargetParamsEntry
switch(config-role)# rule 3 permit read-write feature snmp
TargetAddrEntry
```

Configurar o nexo para a authentication e autorização

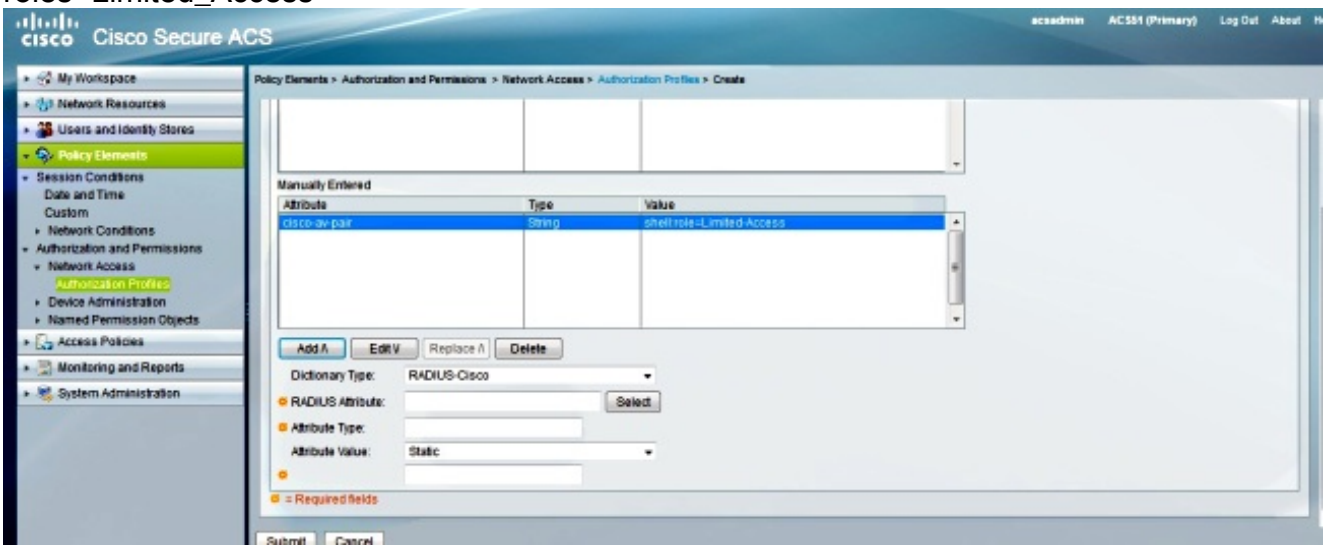
1. A fim criar um usuário local no interruptor com os privilégios completos para a reserva, inscreva o comando username:
   ```
   Switch(config)#username admin privilege 15 password 0 cisco123!
   ```
2. A fim fornecer o endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor Radius (ACS), entre:
   ```
   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
   ```
   Nota: A chave deve combinar o segredo compartilhado configurado no servidor Radius para este dispositivo do nexo.
3. A fim testar a Disponibilidade do servidor Radius, inscreva o comando aaa do teste:
   ```
   switch# test aaa server Radius 10.10.1.1 user1 Ur2Gd2BH
   ```
   A autenticação de teste deve falhar com uma rejeição do server desde que não é configurada ainda. Contudo, confirma que o server é alcançável.
4. A fim configurar autenticações de login, entre:
   ```
   Switch(config)#aaa authentication login
   default group Radserver
   Switch(config)#aaa accounting default group Radserver
   Switch(config)#aaa authentication login error-enable
   ```
   Você não tem que preocupar-se sobre o método local da reserva aqui, porque reservas do nexo ao local no seus próprios se o servidor Radius é não disponível.

Configuração do ACS

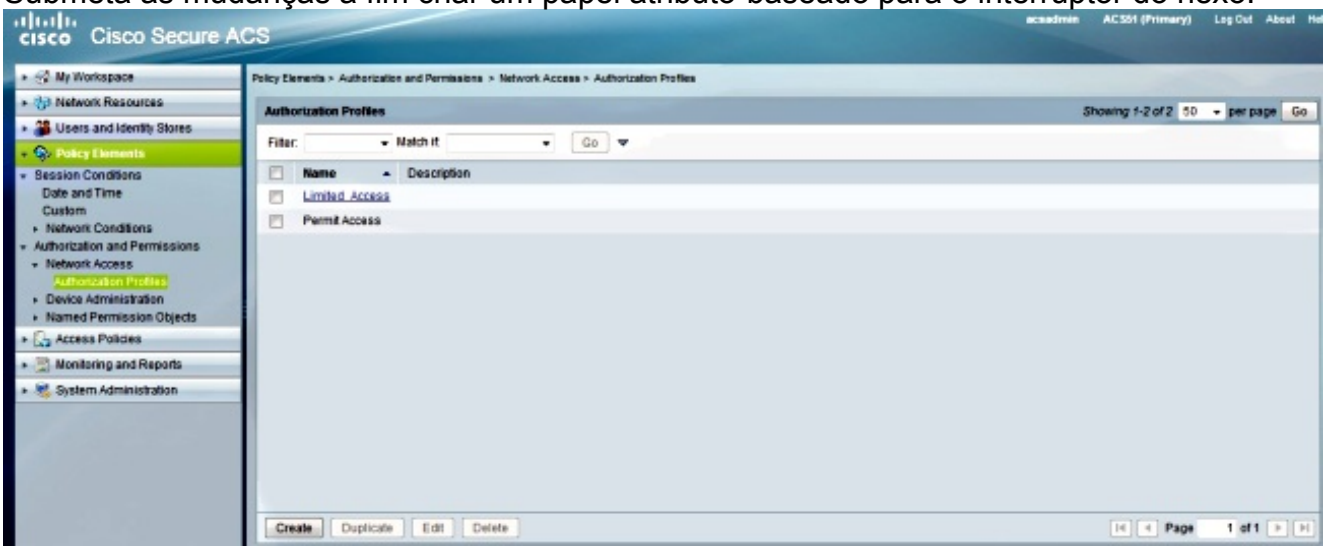
1. Navegue aos **elementos da política > à autenticação e às permissões > ao perfil do acesso de rede > da autorização** a fim criar um perfil da autorização.



2. Dê entrada com um nome para o perfil.
3. Sob os **atributos feitos sob encomenda** catalogue, incorpore estes valores:
   Tipo de dicionário: Raio-CiscoAtributo: Cisco-av-pairExigência: ObrigatórioValor: shell: roles=Limited_Access

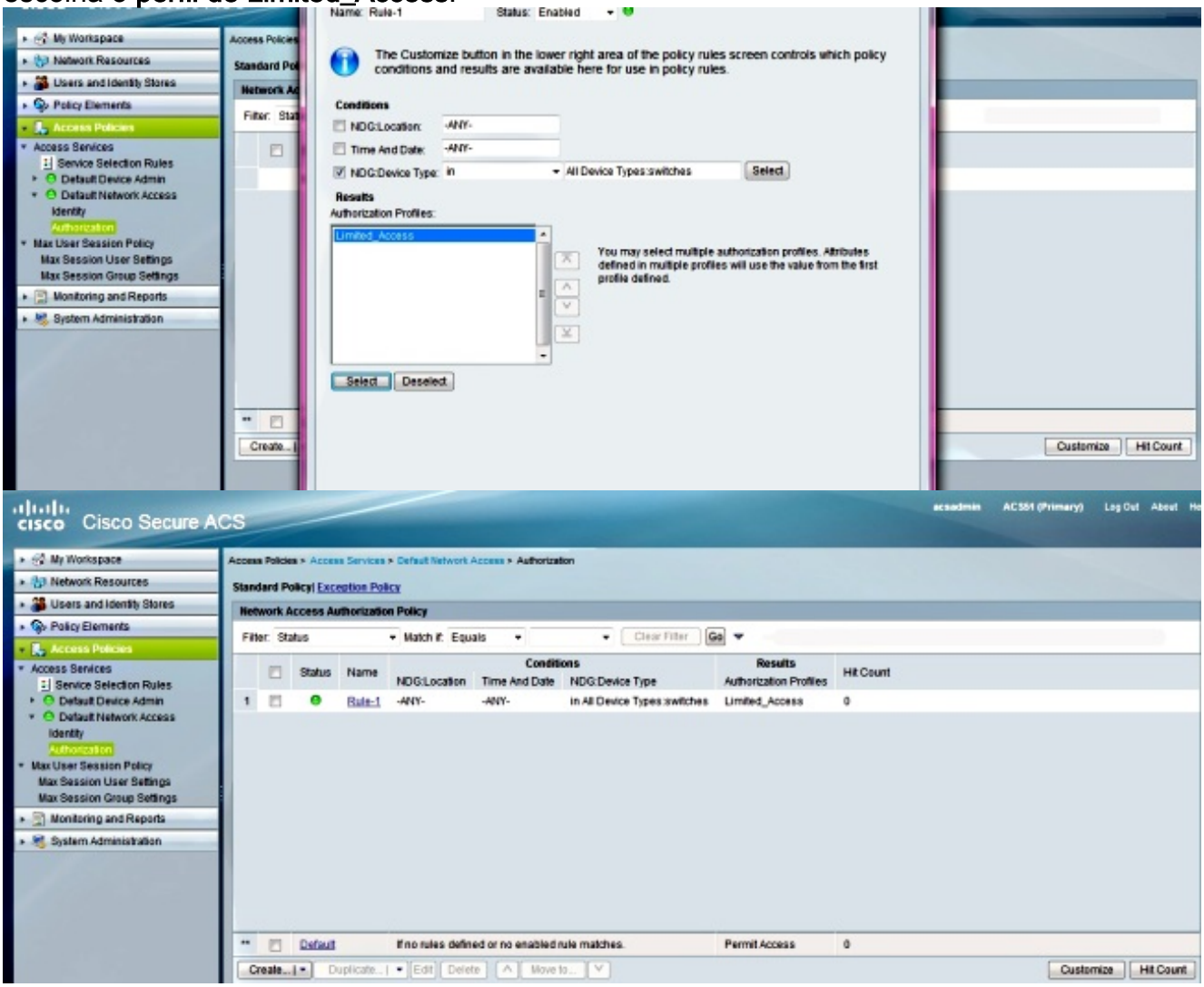


4. Submeta as mudanças a fim criar um papel atributo-baseado para o interruptor do nexo.



5. Crie uma regra nova da autorização ou edite uma regra atual na política de acesso correta. As requisições RADIUS são processadas pela política do acesso de rede à revelia.
6. Na área das **circunstâncias**, escolha as circunstâncias apropriadas. Na área de **resultados**,

escolha o **perfil de Limited_Access**.



7. Clique em **OK**.

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Verificação do papel do nexo

Incorpore o comando do **papel da mostra no** nexo a fim indicar os papéis e as regras definidos do acesso configurado.

```
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
```

Papel de usuário da verificação da atribuição do nexo

Entre ao nexo com o nome de usuário e senha configurado no ACS. Após o início de uma sessão, incorpore o comando da **conta de usuário da mostra** a fim verificar que o usuário de teste tem o papel de Limited_Access:

```
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
```

Uma vez que o papel do acesso de usuário é confirmado, comute no modo de configuração e tente incorporar um comando a não ser um comando interface. O usuário deve ser negado o acesso.

A ferramenta Output Interpreter (clientes registrados somente) apoia determinados comandos de exibição. Use a ferramenta Output Interpreter a fim ver uma análise do emissor de comando de execução.

- **papel da mostra** - Indica as regras da definição e do acesso configurado do papel.
- **conta de usuário da mostra** - Indica os detalhes da conta de usuário e inclui a atribuição do papel.

Troubleshooting

Esta seção fornece a informação que você pode se usar a fim pesquisar defeitos sua configuração de switch.

Termine estas etapas no interruptor para a atribuição do papel:

1. Verifique que grupo AAA é usado para a autenticação com a executar-**configuração aaa da mostra** e **mostre comandos aaa authentication**.
2. Para o RAIO, verifique a associação do roteamento virtual e da transmissão (VRF) com o grupo AAA com a **autenticação aaa da mostra** e **mostre comandos radius da executar-configuração**.
3. Se estes comandos verify que a associação está correta, inscrevem o **comando all do raio debugar** a fim permitir o log de rastreamento.
4. Verifique que os atributos corretos estão sendo empurrados do ACS.

A ferramenta Output Interpreter (clientes registrados somente) apoia determinados comandos de exibição. Use a ferramenta Output Interpreter a fim ver uma análise do emissor de comando de execução.

Nota: Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos **debug**.

- **mostre a executar-configuração AAA**
- **mostre a autenticação aaa**
- **mostre o raio da executar-configuração**
- **debugar o raio todo**