Acceso del usuario de ACS Limited con el RADIUS en el ejemplo de configuración del nexo

Contenido

Introducción

Este documento describe cómo proporcionar el acceso restringido a los usuarios del nexo de modo que puedan ingresar solamente los comandos limitados con el Cisco Secure Access Control Server (ACS) como servidor de RADIUS. Por ejemplo, usted puede ser que quiera que un usuario pudiera iniciar sesión a un privilegiado o a un modo de configuración y sea permitido solamente ingresar los comandos interface. Para alcanzar esto, usted debe crear un rol personalizado para el usuario en el servidor de RADIUS se utiliza que.

Prerrequisitos

Requisitos

El servidor de RADIUS (ACS en este ejemplo) y el nexo deben poder entrarse en contacto y realizar las autenticaciones.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- ACS versión 5.x
- 7000 Switch del nexo

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Configurar

Configuración de los rol personalizado en el nexo

Para crear un papel que proporcione solamente el acceso de lectura/grabación para el comando interface, ingrese:

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

Las reglas de acceso adicionales del permiso se definen con este sintaxis:

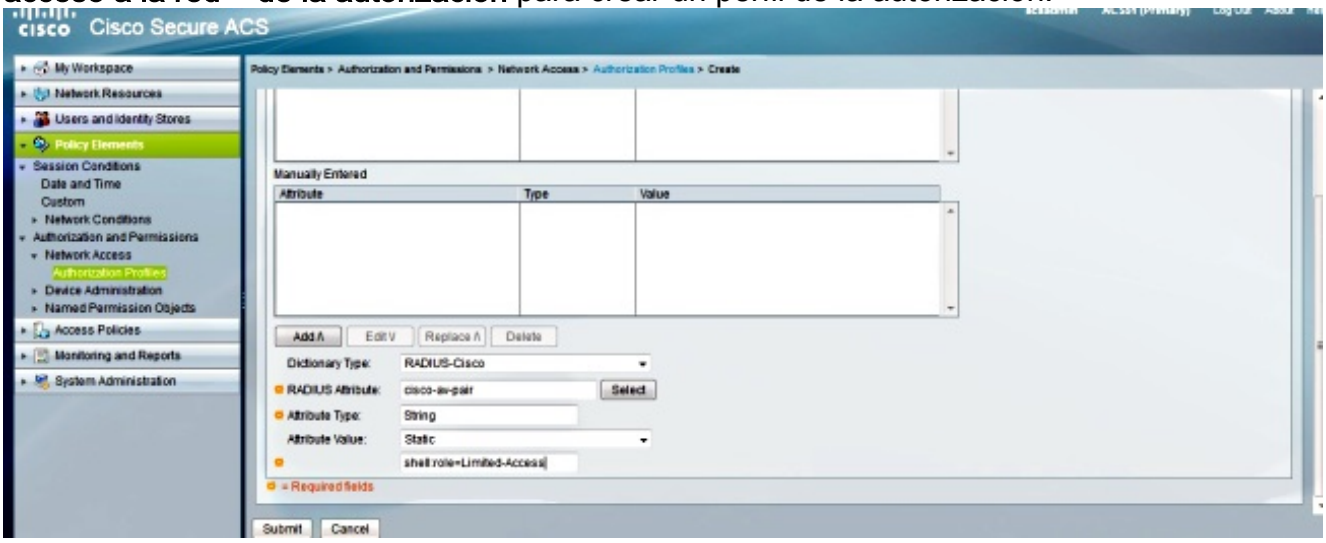
```
switch(config-role)# rule 1 permit read-write feature snmp
switch(config-role)# rule 2 permit read-write feature snmp
TargetParamsEntry
switch(config-role)# rule 3 permit read-write feature snmp
TargetAddrEntry
```

Configure el nexo para la autenticación y autorización

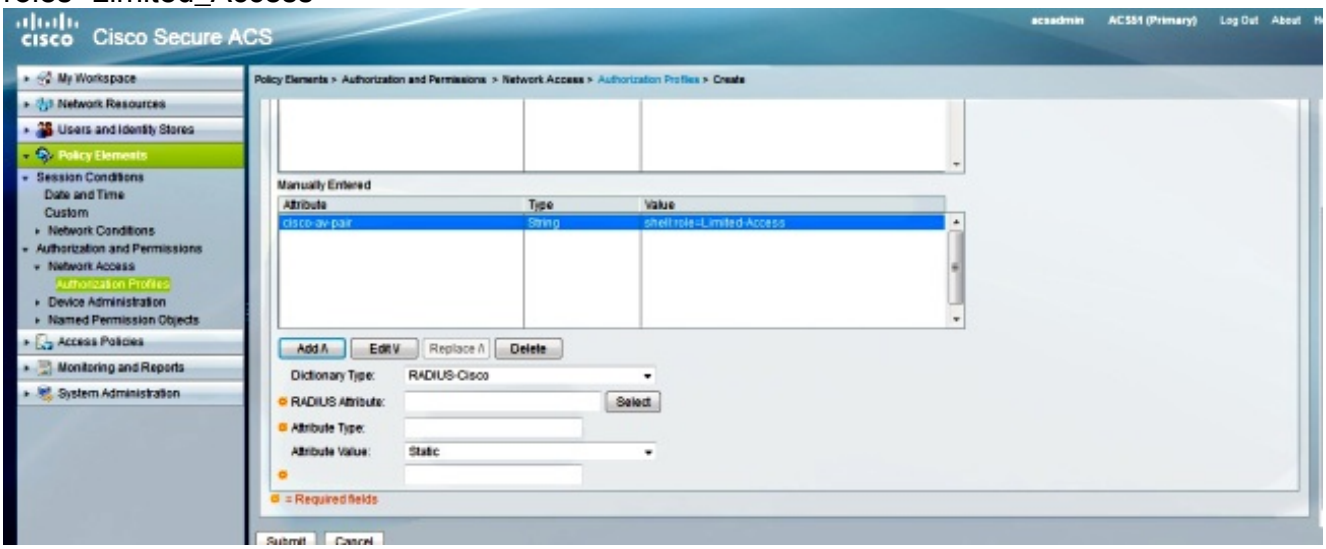
1. Para crear a un usuario local en el Switch con los privilegios completos para el retraso, ingrese el **comando username**:
   `Switch(config)#username admin privilege 15 password 0 cisco123!`
2. Para proporcionar el IP Address del servidor de RADIUS (ACS), ingrese:
   ```
   switch# conf terminal
   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: La clave debe hacer juego el secreto compartido configurado en el servidor de RADIUS para este dispositivo del nexo.
3. Para probar la Disponibilidad del servidor de RADIUS, ingrese el **comando aaa de la prueba**:
   `switch# test aaa server Radius 10.10.1.1 user1 Ur2Gd2BH`
   La prueba de la autentificación debe fallar con un rechazo del servidor puesto que todavía no se configura. Sin embargo, confirma que el servidor es accesible.
4. Para configurar las autenticaciones de inicio de sesión, ingrese: `Switch(config)#aaa authentication login default group Radserver`
   `Switch(config)#aaa accounting default group Radserver`
   `Switch(config)#aaa authentication login error-enable`
   Usted no tiene que preocuparse del método local del retraso aquí, porque los retrasos del nexo al local en sus los propio si el servidor de RADIUS es inasequible.

Configuración del ACS

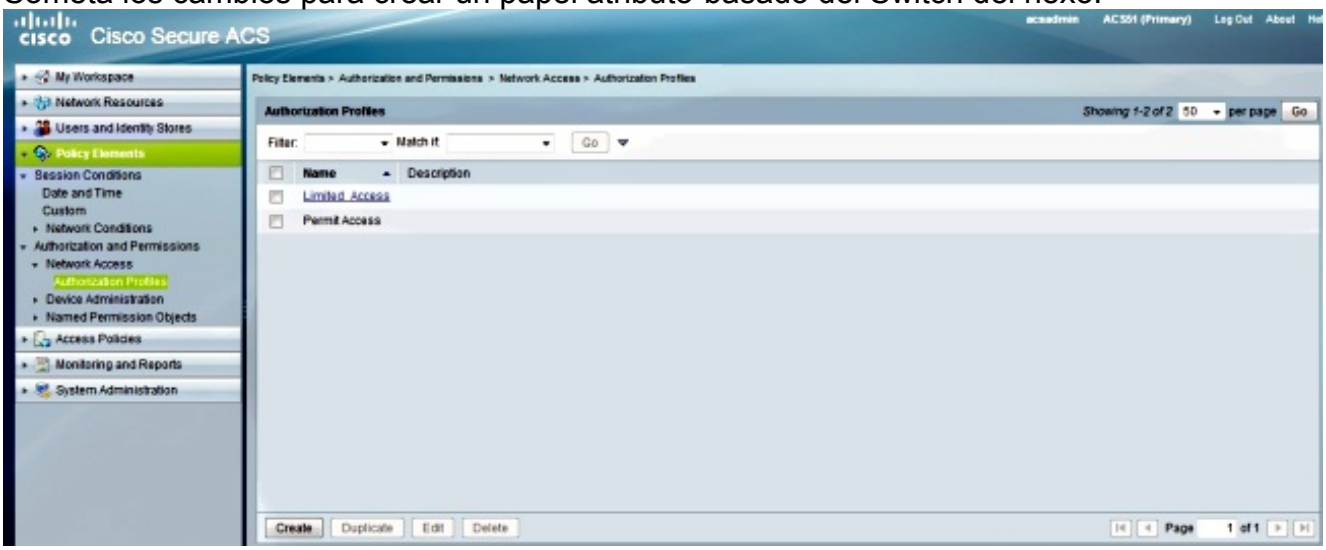
1. Navegue a los **elementos de la directiva > a la autenticación y a los permisos > al perfil del acceso a la red > de la autorización** para crear un perfil de la autorización.



2. Ingrese un nombre para el perfil.
3. Bajo **atributos personalizados** tabule, ingrese estos valores:
   Tipo de diccionario: Radio-CiscoAtributo: Cisco-av-pairRequisito: ObligatorioValor: shell: roles=Limited_Access

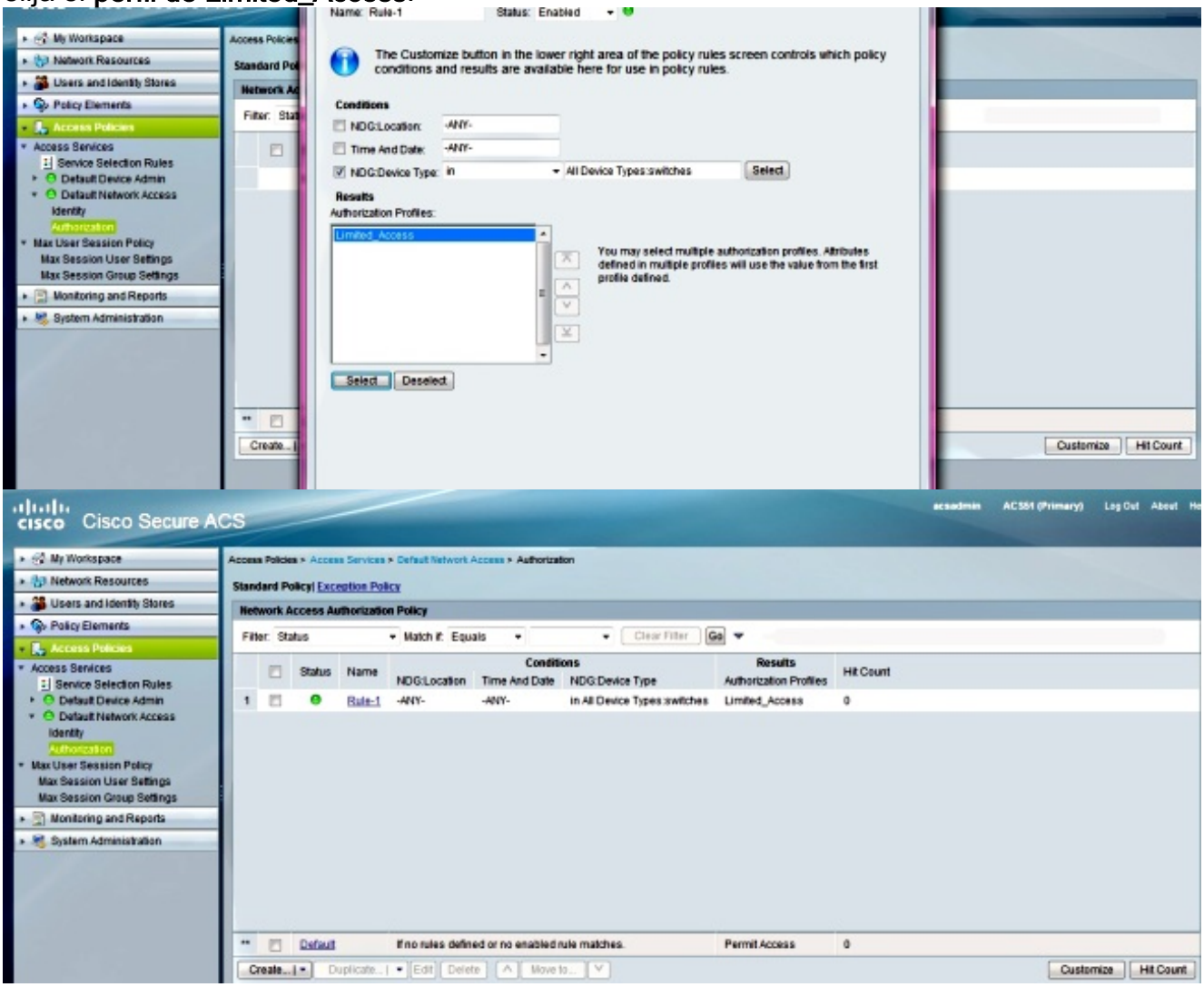


4. Someta los cambios para crear un papel atributo-basado del Switch del nexo.



5. Cree una nueva regla de la autorización o edite una regla actual en la política de acceso correcta. Los pedidos de RADIUS son procesados por la directiva de acceso a la red por abandono.

6. En el área de las **condiciones**, elija las condiciones apropiadas. En el área de **resultados**, elija el **perfil de Limited_Access**.



7. Haga clic en OK.

Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

Verificación del papel del nexo

Ingrese el comando del **papel de la demostración** en el nexo para visualizar los papeles y las reglas definidos del acceso 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
```

Rol del usuario de la verificación de la asignación del nexo

Inicie sesión al nexo con el nombre de usuario y contraseña configurado en el ACS. Después del login, ingrese el comando de la **cuenta de usuario de la demostración** para verificar que el usuario a prueba tiene el 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
```

Una vez que se confirma el papel del acceso del usuario, conmute en el modo de configuración e intente ingresar un comando con excepción de un comando interface. El usuario debe ser negado el acceso.

La herramienta del Output Interpreter (clientes registrados solamente) apoya los ciertos comandos show. Utilice la herramienta del Output Interpreter para ver una análisis de la salida del comando show.

- **papel de la demostración** - Visualiza las reglas de la definición y del acceso configurado del papel.
- **cuenta de usuario de la demostración** - Visualiza los detalles de la cuenta de usuario e incluye la asignación del papel.

Troubleshooting

Esta sección proporciona la información que usted puede utilizar para resolver problemas su configuración del switch.

Complete estos pasos en el Switch para la asignación del papel:

1. Verifique que utilizan el grupo AAA para la autenticación con los ejecutar-**config aaa de la demostración** y **muestre los comandos aaa authentication**.
2. Para el RADIUS, verifique la asociación del ruteo virtual y de la expedición (VRF) con el grupo AAA con la **autenticación aaa de la demostración** y **muestre los comandos radius de los ejecutar-config**.
3. Si estos comandos verify que la asociación está correcta, ingresan el **comando all del radio del debug** para habilitar el registro de la traza.
4. Verifique que los atributos correctos se estén avanzando del ACS.

La herramienta del Output Interpreter (clientes registrados solamente) apoya los ciertos

comandos show. Utilice la herramienta del Output Interpreter para ver una análisis de la salida del comando show.

> Nota: Consulte Información Importante sobre Comandos de Debug antes de usar un **comando debug**.

- **muestre los ejecutar-config AAA**
- **muestre la autenticación aaa**
- **muestre el radio de los ejecutar-config**
- **haga el debug del radio todo**