

# Documento de prueba

## Introducción

Este documento describe cómo configurar un rol personalizado de Nexus para TACACS a través de CLI en NK9.

## Prerequisites

### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- TACACS+
- ISE 3.2

### Componentes Utilizados

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

- El archivo de imagen de Cisco Nexus 9000, NXOS es: bootflash:///nxos.9.3.5.bin
- Identity Service Engine versión 3.2

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 tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

## Antecedentes

### Requisitos de licencia

Cisco NX-OS: TACACS+ no requiere licencia.

## Cisco Identity Service Engine

Para las instalaciones de ISE nuevas, dispone de una licencia de período de evaluación de 90 días que tiene acceso a todas las funciones de ISE. Si no dispone de una licencia de evaluación, para utilizar la función ISE TACACS necesita una licencia Device Admin para el nodo de Policy Server que realiza la autenticación.

Una vez que los usuarios de administración/soporte técnico se hayan autenticado en el dispositivo Nexus, ISE devuelve el rol de shell de Nexus deseado.

El usuario asignado a esta función puede llevar a cabo la resolución de problemas básica y rebotar determinados puertos.

La sesión TACACS que obtiene el rol Nexus solo debe poder utilizar y ejecutar los siguientes comandos y acciones:

- Acceso para configurar el terminal para que SÓLO ejecute las interfaces de apagado y no cierre de 1/1-1/21 y 1/25-1/30
- ssh
- ssh6
- telnet
- Telnet6
- Traceroute
- Traceroute6
- Ping
- Ping6
- Habilitar

## Configurar

Diagrama de la red

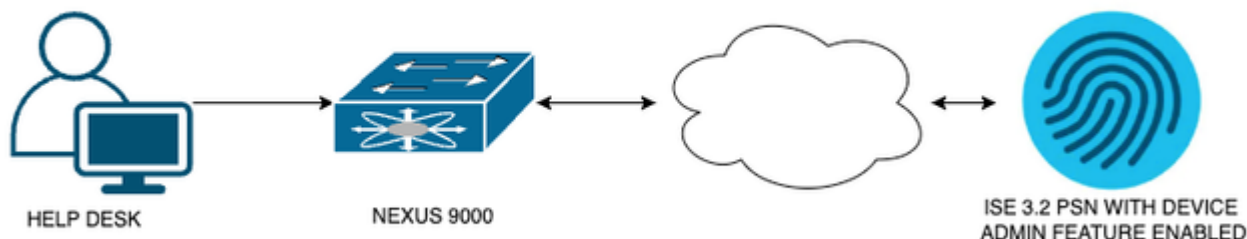


Diagrama de componentes de flujo

## Paso 1: Configuración de Nexus 9000

### 1. Configure AAA.



Advertencia: Después de activar la autenticación TACACS, el dispositivo Nexus deja de utilizar la autenticación local y comienza a utilizar la autenticación basada en servidor AAA.

```
Nexus9000(config)# feature tacacs+
Nexus9000(config)# tacacs-server host <Your ISE IP> key 0 Nexus3xample
Nexus9000(config)# tacacs-server key 0 "Nexus3xample"
Nexus9000(config)# aaa group server tacacs+ IsePsnServers
Nexus9000(config-tacacs+)# server <Your ISE IP>
Nexus9000(config)# aaa authentication login default group IsePsnServers local
```

### 2. Configure el rol personalizado con los requisitos especificados.

```
Nexus9000(config)# role name helpdesk
Nexus9000(config-role)# description Can perform basic Troubleshooting and bounce certain ports
Nexus9000(config-role)# rule 1 permit read
Nexus9000(config-role)# rule 2 permit command enable *
Nexus9000(config-role)# rule 3 permit command ssh *
Nexus9000(config-role)# rule 4 permit command ssh6 *
Nexus9000(config-role)# rule 5 permit command ping *
Nexus9000(config-role)# rule 6 permit command ping6 *
Nexus9000(config-role)# rule 7 permit command telnet *
Nexus9000(config-role)# rule 8 permit command traceroute *
Nexus9000(config-role)# rule 9 permit command traceroute6 *
Nexus9000(config-role)# rule 10 permit command telnet6 *
Nexus9000(config-role)# rule 11 permit command config t ; interface * ; shutdown
Nexus9000(config-role)# rule 12 permit command config t ; interface * ; no shutdown

vlan policy deny
```

interface policy deny

```
Nexus9000(config-role-interface)# permit interface Ethernet1/1
Nexus9000(config-role-interface)# permit interface Ethernet1/2
Nexus9000(config-role-interface)# permit interface Ethernet1/3
Nexus9000(config-role-interface)# permit interface Ethernet1/4
Nexus9000(config-role-interface)# permit interface Ethernet1/5
Nexus9000(config-role-interface)# permit interface Ethernet1/6
Nexus9000(config-role-interface)# permit interface Ethernet1/7
Nexus9000(config-role-interface)# permit interface Ethernet1/8
Nexus9000(config-role-interface)# permit interface Ethernet1/8
Nexus9000(config-role-interface)# permit interface Ethernet1/9
Nexus9000(config-role-interface)# permit interface Ethernet1/10
Nexus9000(config-role-interface)# permit interface Ethernet1/11
Nexus9000(config-role-interface)# permit interface Ethernet1/12
Nexus9000(config-role-interface)# permit interface Ethernet1/13
Nexus9000(config-role-interface)# permit interface Ethernet1/14
Nexus9000(config-role-interface)# permit interface Ethernet1/15
Nexus9000(config-role-interface)# permit interface Ethernet1/16
Nexus9000(config-role-interface)# permit interface Ethernet1/17
Nexus9000(config-role-interface)# permit interface Ethernet1/18
Nexus9000(config-role-interface)# permit interface Ethernet1/19
Nexus9000(config-role-interface)# permit interface Ethernet1/20
Nexus9000(config-role-interface)# permit interface Ethernet1/21
Nexus9000(config-role-interface)# permit interface Ethernet1/22
Nexus9000(config-role-interface)# permit interface Ethernet1/25
Nexus9000(config-role-interface)# permit interface Ethernet1/26
Nexus9000(config-role-interface)# permit interface Ethernet1/27
Nexus9000(config-role-interface)# permit interface Ethernet1/28
Nexus9000(config-role-interface)# permit interface Ethernet1/29
Nexus9000(config-role-interface)# permit interface Ethernet1/30
```

```
Nexus9000# copy running-config startup-config
[#####] 100%
Copy complete, now saving to disk (please wait)...
```

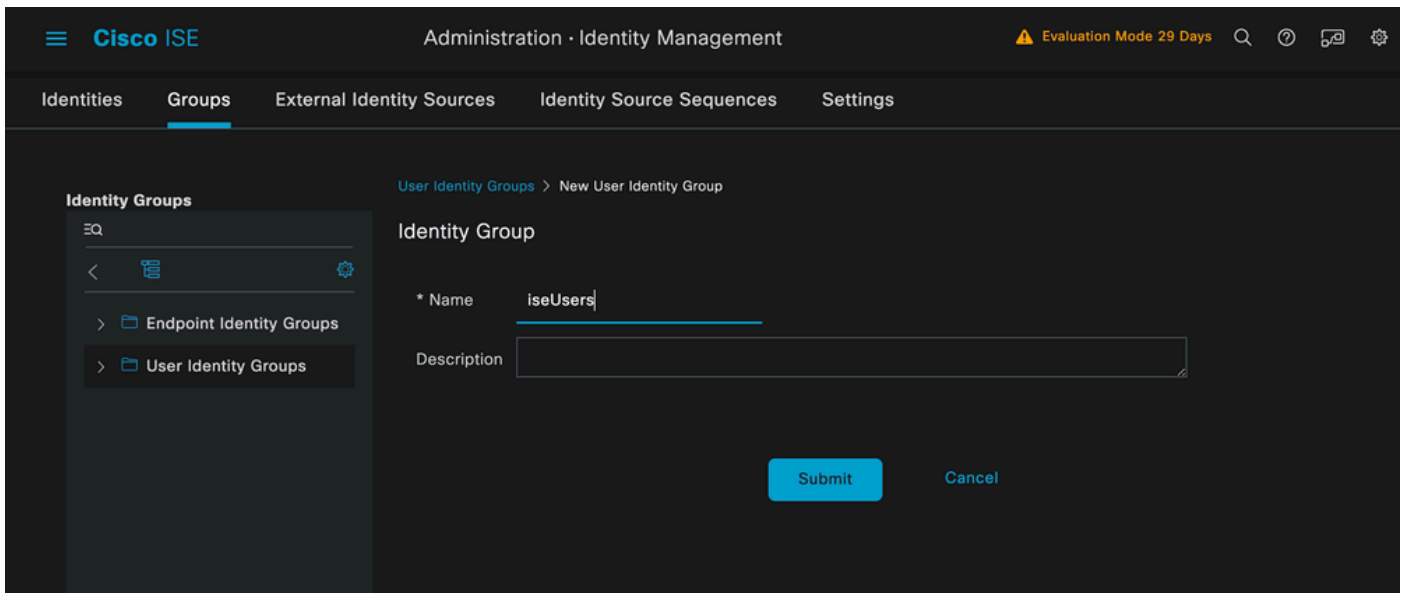
Copy complete.

## Paso 2. Configuración de Identity Service Engine 3.2

1. Configure la identidad que se utiliza durante la sesión TACACS de Nexus.

Se utiliza la autenticación local de ISE.

Vaya a la pestaña Administration > Identity Management > Groups y cree el grupo del que el usuario debe ser parte; el grupo de identidad creado para esta demostración es iseUsers.

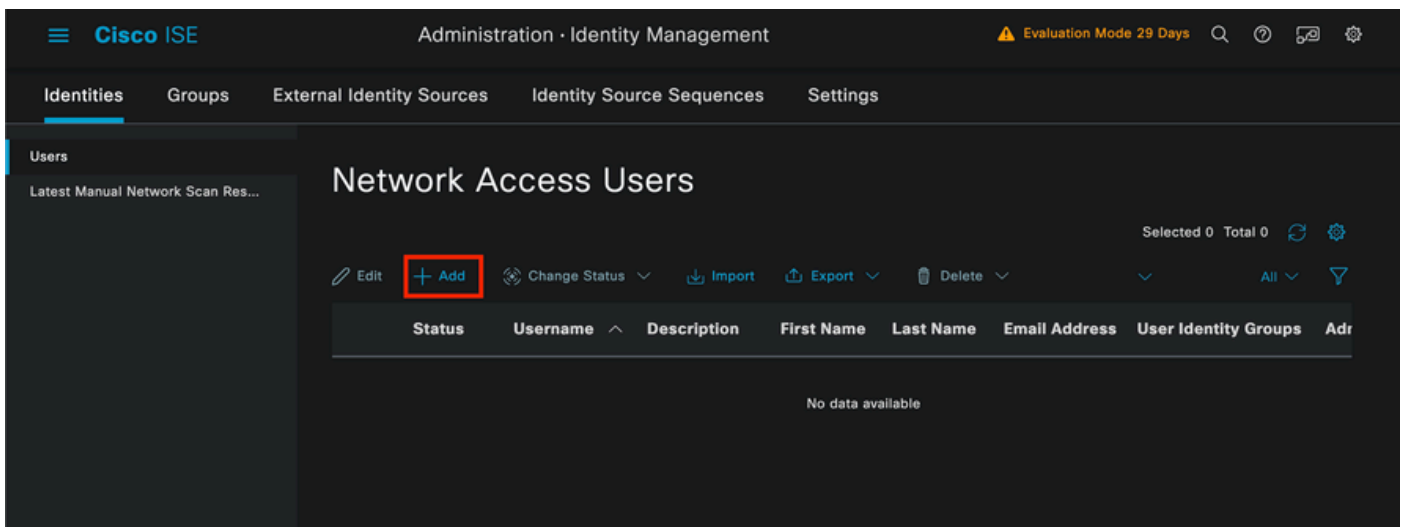


Creación de un grupo de usuarios

Haga clic en el botón Submit.

A continuación, vaya a la ficha Administration > Identity Management > Identity.

‘Haga clic en el botón Add (Agregar).’



Creación de usuario

Como parte de los campos obligatorios, comience con el nombre del usuario, en este ejemplo se utiliza el nombre de usuario iseiscool.

## Network Access User

\* Username

Status  Enabled ▼

Account Name Alias  ⓘ

Email

*Nombrar al usuario y crearlo*

El siguiente paso es asignar una contraseña al nombre de usuario creado. VainillaISE97 es la contraseña utilizada en esta demostración.

## Passwords

Password Type:  ▼

Password Lifetime:

With Expiration ⓘ  
Password will expire in 60 days

Never Expires ⓘ

Password

Re-Enter Password

\* Login Password

Generate Password ⓘ

Enable Password

Generate Password ⓘ

*Asignación de contraseña*

Por último, asigne el usuario al grupo creado anteriormente, que en este caso es iseUsers.

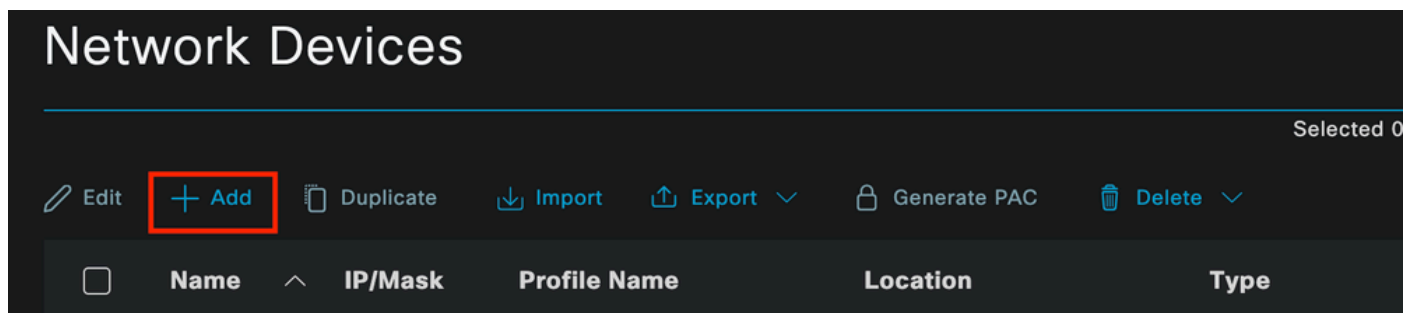
## User Groups

▼ ⓘ +

## 2. Configure y agregue el dispositivo de red.

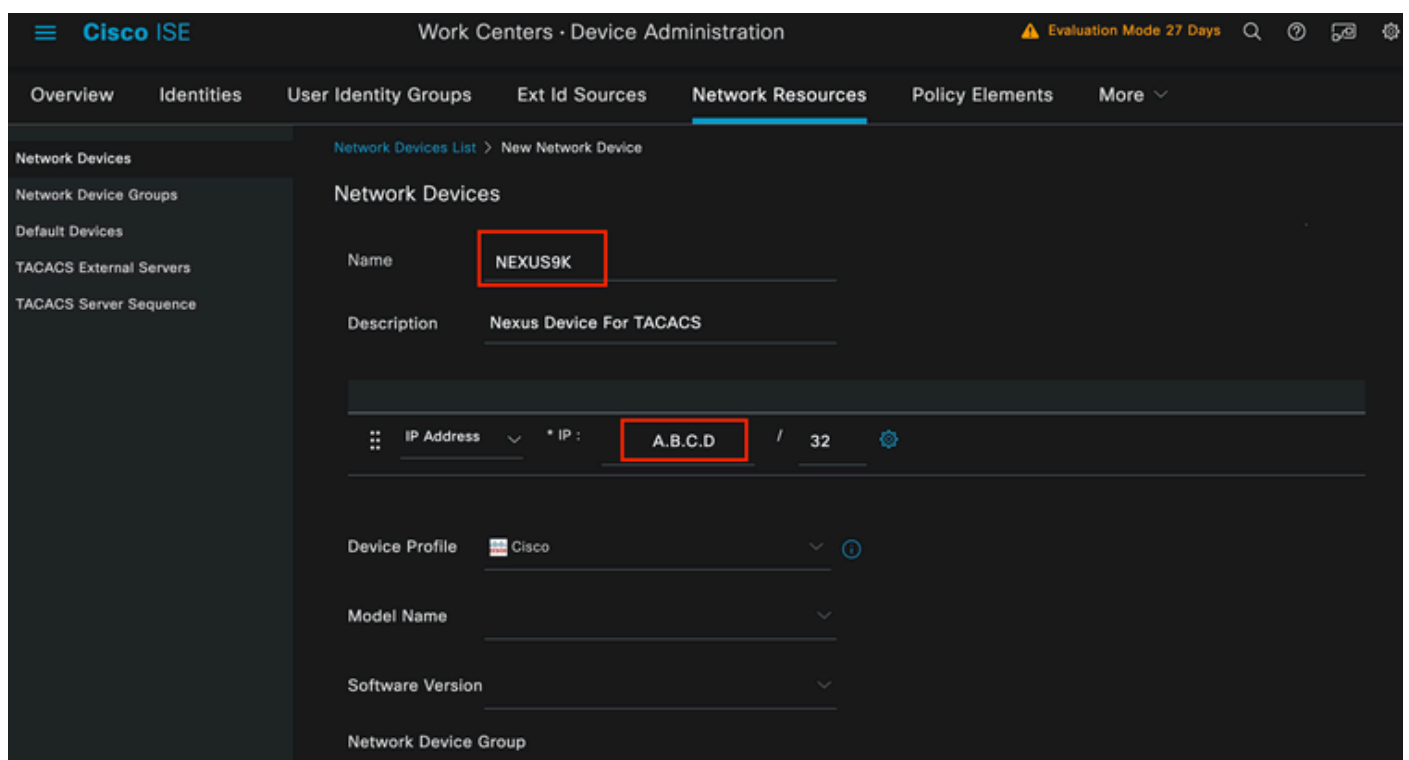
Agregue el dispositivo NEXUS 9000 a ISE Administration > Network Resources > Network Devices

Haga clic en el botón Add para comenzar.



Página Dispositivo de Acceso a Red

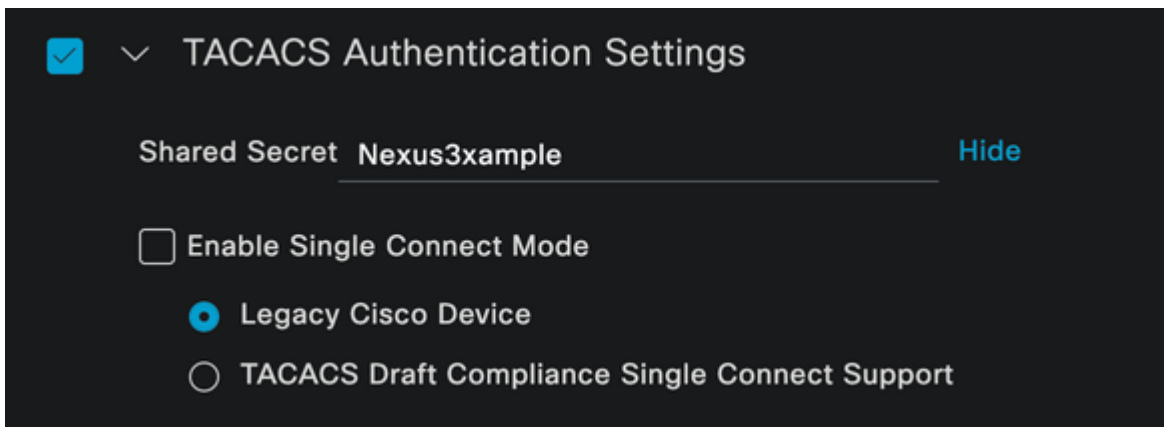
Introduzca los valores en el formulario, asigne un nombre al NAD que está creando y una IP desde la que el NAD se ponga en contacto con ISE para la conversación TACACS.



Configurar dispositivo de red

Las opciones desplegables se pueden dejar en blanco y se pueden omitir; estas opciones están diseñadas para categorizar sus NAD por ubicación, tipo de dispositivo, versión y, a continuación, cambiar el flujo de autenticación basado en estos filtros.

En Administration > Network Resources > Network Devices > Your NAD > TACACS Authentication Settings, agregue la clave secreta compartida que utilizó en su configuración de NAD. Nexus3example se utiliza en esta demostración.



sección de configuración de TACACS

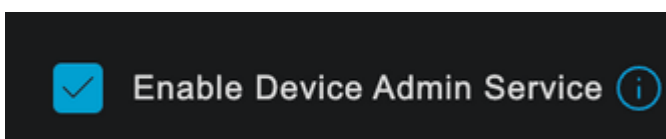
Guarde los cambios haciendo clic en el botón Submit.

### 3. Configuración de TACACS en ISE.

Compruebe dos veces que el PSN que ha configurado en el Nexus 9k tiene la opción Device Admin habilitada.



Nota: Habilitar el servicio Device Admin NO provoca un reinicio en ISE.



Comprobación de la función PSN Device Admin

Esto se puede verificar en el menú de ISE Administration > System > Deployment > Your PSN > Policy Server section > Enable Device Admin Services.

- Cree un perfil TACACS que devuelva el servicio de asistencia al dispositivo Nexus si la autenticación es correcta.

En el menú de ISE, navegue hasta Workcenters > Device Administration > Policy Elements > Results > TACACS Profiles y haga clic en el botón Add.

Work Centers · Device Administration

Overview Identities User Identity Groups Ext Id Sources Network Resources Policy Elements More

Conditions >

Network Conditions >

Results >

Allowed Protocols

TACACS Command Sets

TACACS Profiles

## TACACS Profiles

Rows/Page 4 |<< 1 / 1 >> | Go 4 Total Rows

[Add](#) Duplicate Trash Edit Filter

Name	Type	Description
Default Shell Profile	Shell	Default Shell Profile
Deny All Shell Profile	Shell	Deny All Shell Profile

Perfil TACACS

Asigne un nombre y, opcionalmente, una descripción.

Work Centers · Device Administration

Overview Identities User Identity Groups Ext Id Sources Network Resources Policy Elements More

Conditions >

Network Conditions >

Results >

Allowed Protocols

TACACS Command Sets

TACACS Profiles

## TACACS Profiles > New TACACS Profile

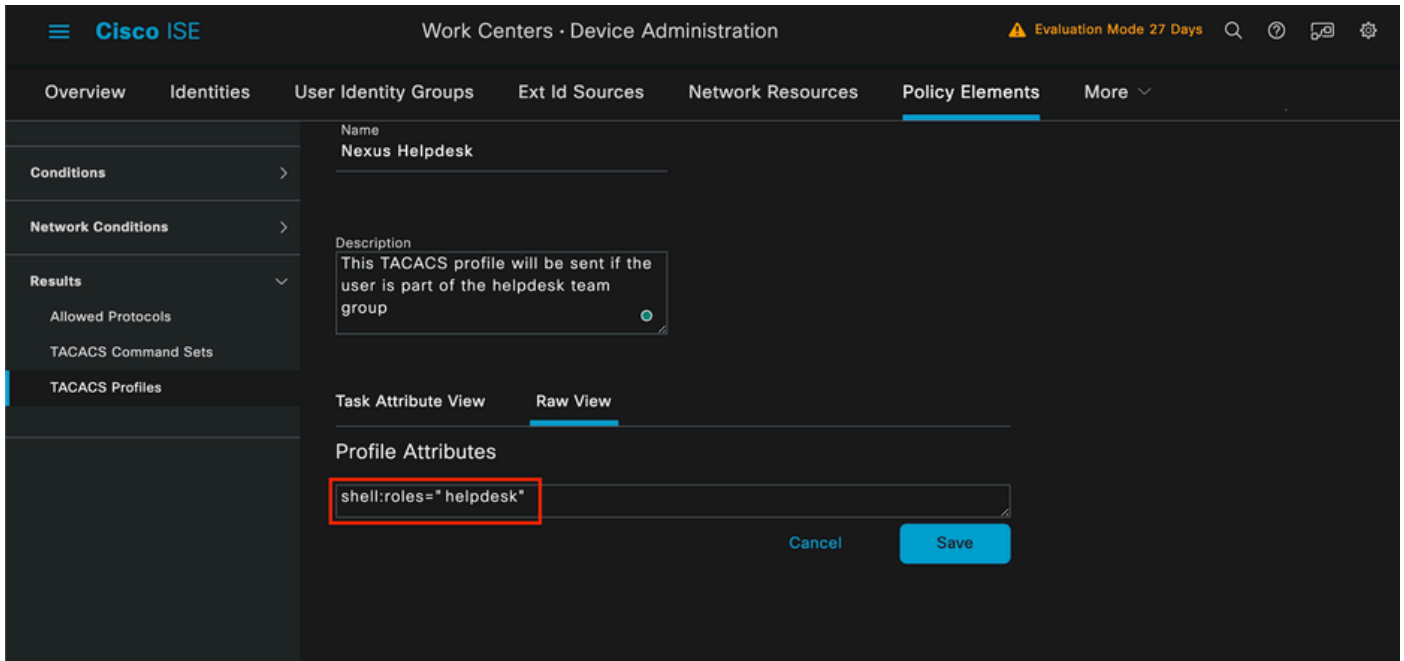
Name  
Nexus Helpdesk

Description  
This TACACS profile will be sent if the user is part of the helpdesk team group

Perfil de Tacacs de denominación

Omita la sección Vista de atributos de tarea y navegue hasta la sección Vista sin procesar.

E introduzca el valor shell:roles="helpdesk".



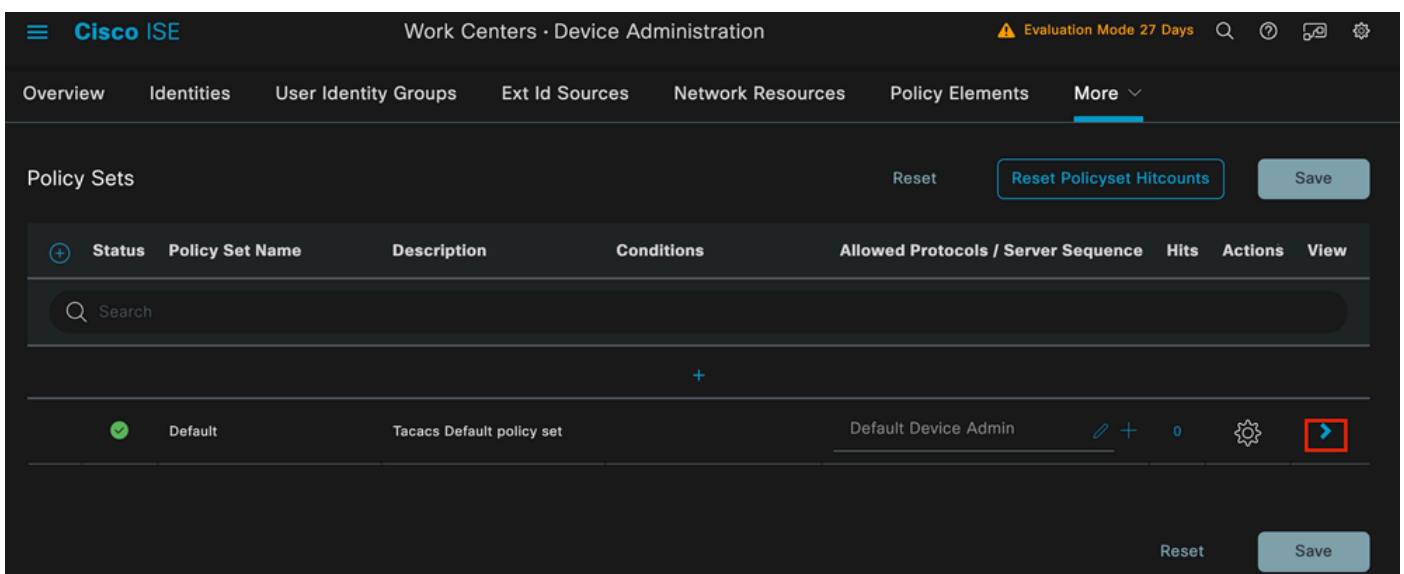
Adición de atributos de perfil

Configure el conjunto de directivas que incluye la directiva de autenticación y la directiva de autorización.

En el menú de ISE, acceda a Centros de trabajo > Administración de dispositivos > Conjuntos de políticas de administración de dispositivos.

A modo de demostración, se utiliza el conjunto de políticas predeterminadas. Sin embargo, se puede crear otro conjunto de directivas, con condiciones que coincidan con escenarios específicos.

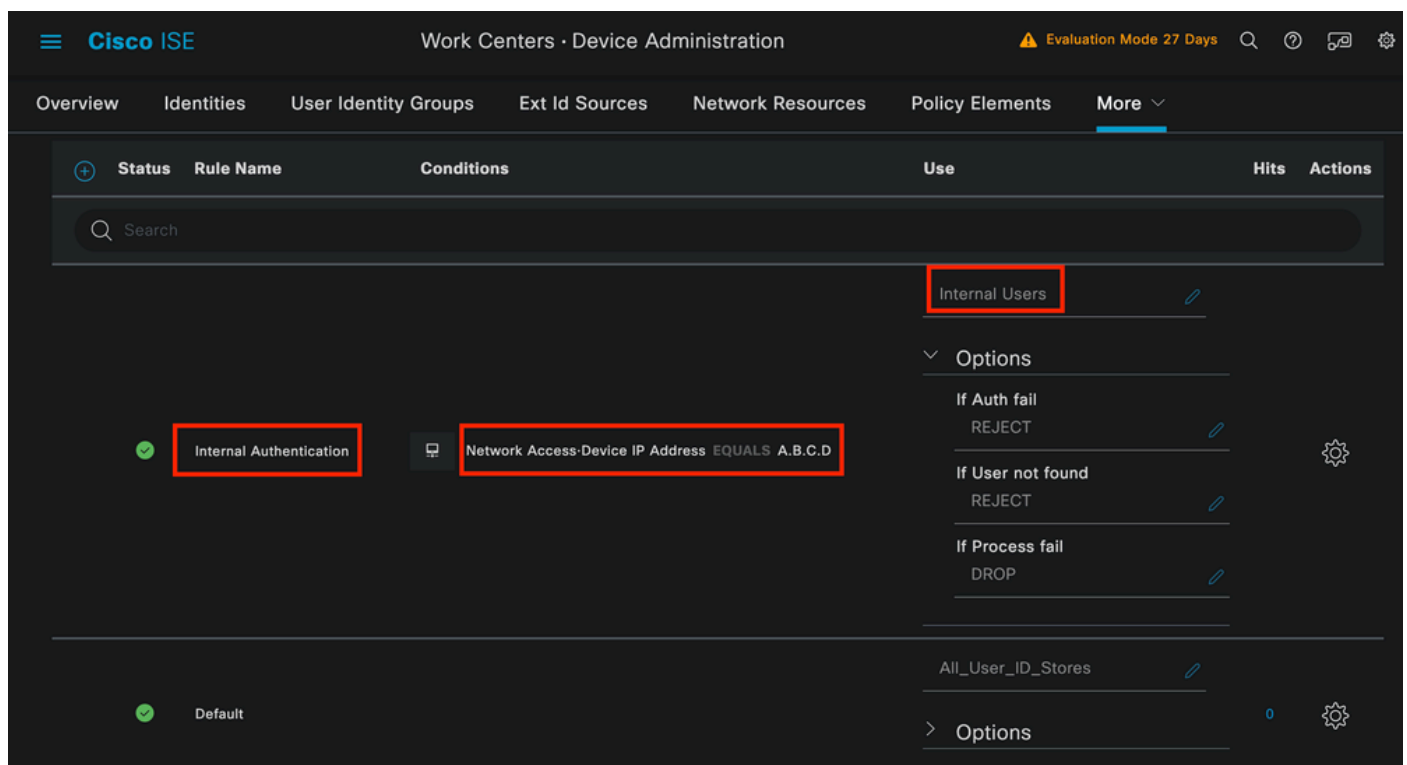
Haga clic en la flecha situada al final de la fila.



Una vez dentro de la configuración del conjunto de políticas, desplácese hacia abajo y expanda la sección Política de autenticación.

Haga clic en el icono Add.

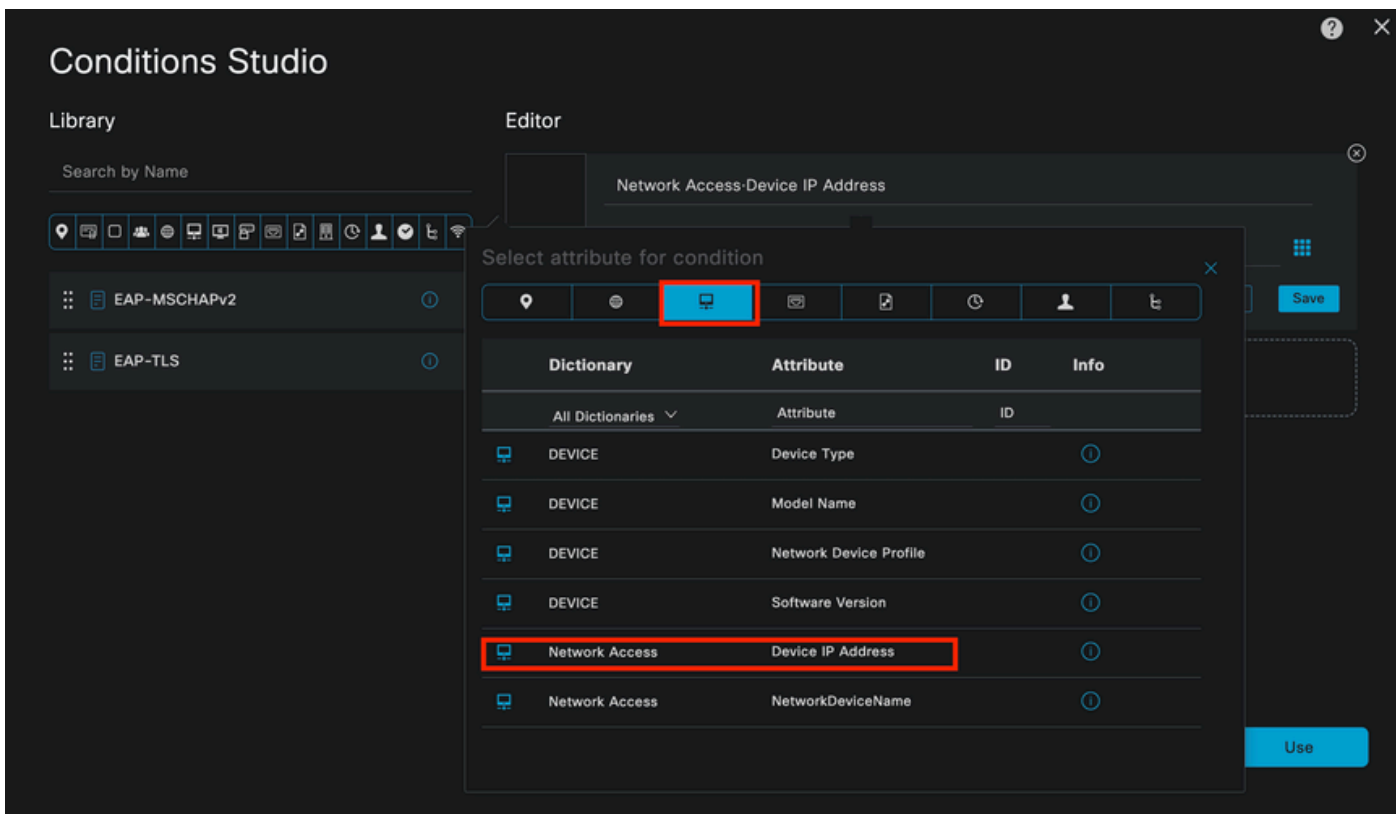
Para este ejemplo de configuración, el valor Name es Internal Authentication y la condición elegida es Network Device (Nexus) IP (sustituya el A.B.C.D.). Esta directiva de autenticación utiliza el almacén de identidad de usuarios internos.



Política de autenticación

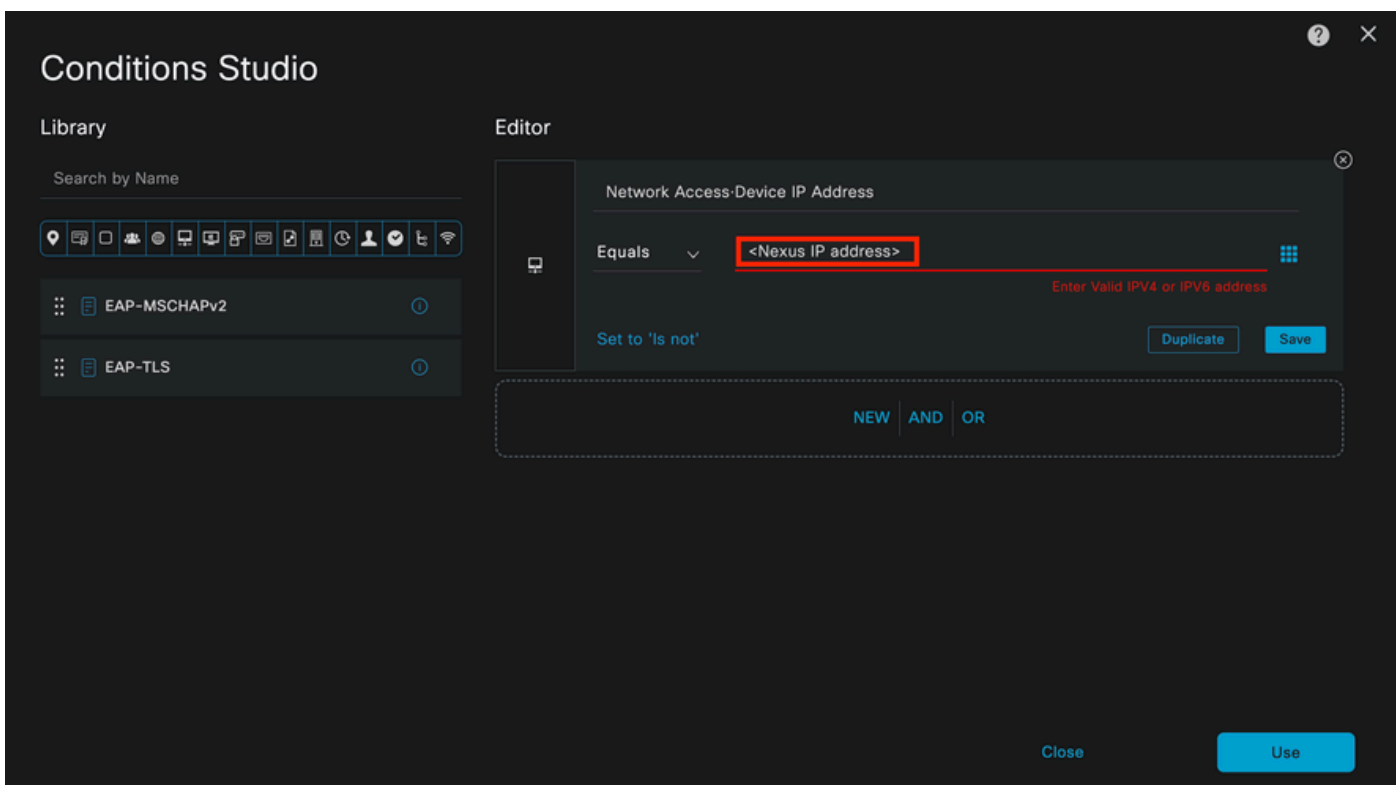
Así es como se configuró la condición.

Seleccione Network Access > Device IP address Dictionary Attribute.



Estudio de condición para la política de autenticación

Sustituya el comentario <dirección IP de Nexus> por la dirección IP correcta.



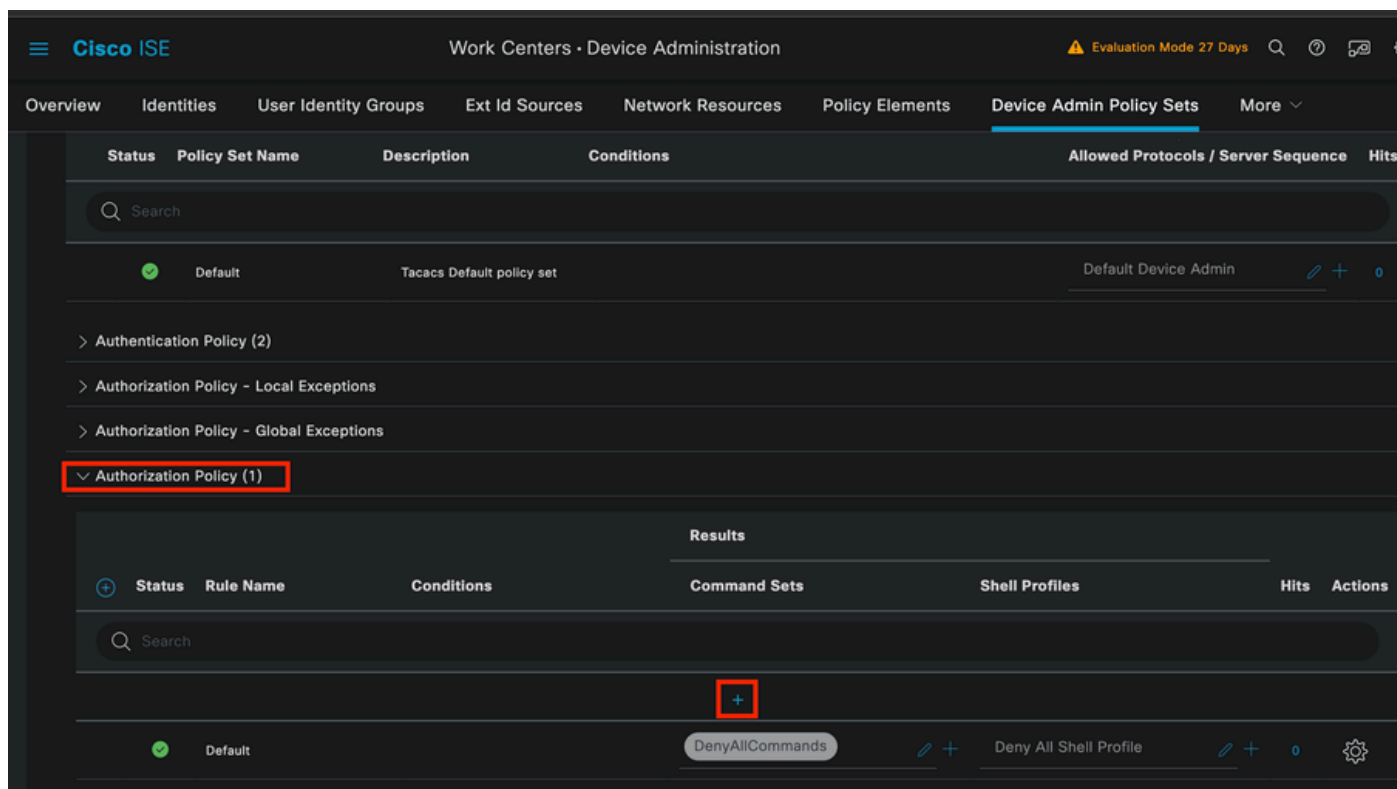
Adición del filtro IP

Haga clic en el botón Use.

Esta condición solo la cumple el dispositivo Nexus configurado. Sin embargo, si el propósito es habilitar esta condición para una gran cantidad de dispositivos, considere una condición diferente.

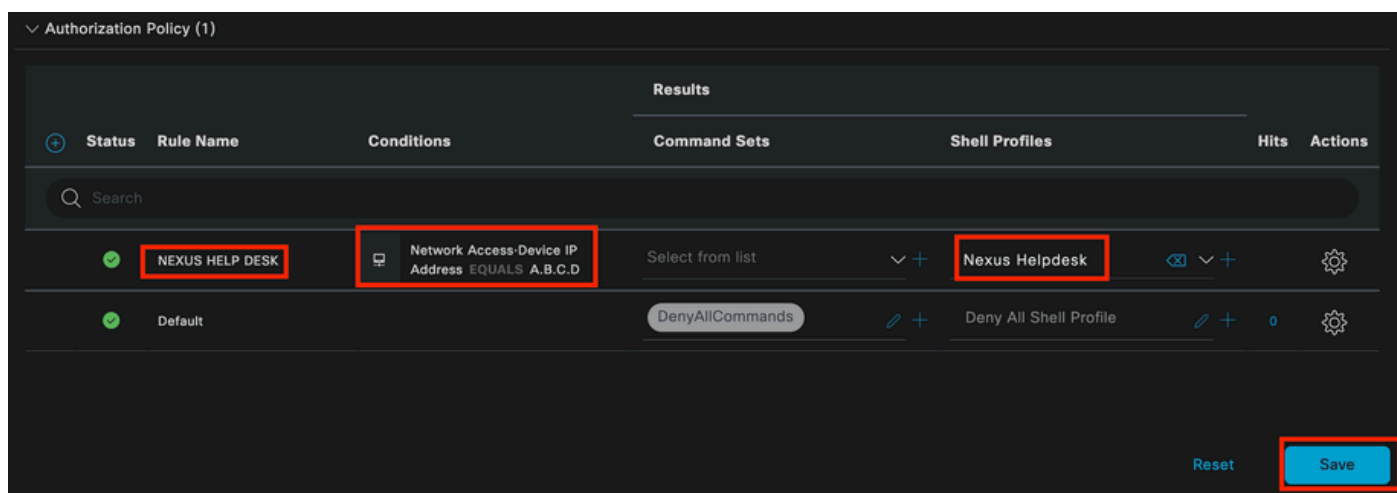
A continuación, desplácese a la sección Directiva de autorización y expándala.

Haga clic en el icono + (más).



Sección de directiva de autorización

En este ejemplo, se utilizó NEXUS HELP DESK como nombre de la política de autorización.



Estudio de condiciones para la directiva de autorización

La misma condición que se configuró en la directiva de autenticación se utiliza para la directiva de

autorización.

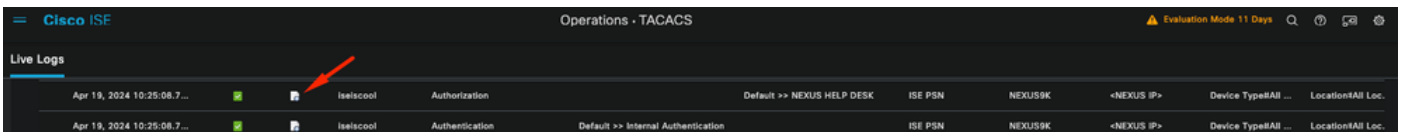
En la columna Perfiles de shell, se selecciona el perfil configurado antes de Nexus Helpdesk.

Por último, haga clic en el botón Save.

## Verificación

Utilice esta sección para confirmar que su configuración funcione correctamente.

Desde la GUI de ISE, navegue hasta Operaciones > TACACS > Live Logs. Identifique el registro que coincida con el nombre de usuario utilizado y haga clic en Live Log Detail del evento de autorización.



Cisco ISE		Operations - TACACS		Evaluation Mode 11 Days	
Live Logs					
Apr 19, 2024 10:25:08.7...	ISESCOOL	Authorization	Default >> NEXUS HELP DESK	ISE PSN	NEXUS9K
Apr 19, 2024 10:25:08.7...	ISESCOOL	Authentication	Default >> Internal Authentication	ISE PSN	NEXUS9K

Live Log de TACACS

Como parte de los detalles que incluye este informe, se puede encontrar la sección Respuesta, donde puede ver cómo ISE devolvió el valor shell:roles="helpdesk"

```
Response          {Author-Reply-Status=PassRepl;  
                  AVPair=shell:roles=" helpdesk" ; }
```

Respuesta detallada de Live Log

En el dispositivo Nexus:

```
Nexus9000 login: iseiscool  
Password: VainillaISE97
```

```
Nexus9000# conf t  
Enter configuration commands, one per line. End with CNTL/Z.  
Nexus9000(config)# interface ethernet 1/23  
% Interface permission denied
```

```
Nexus9000(config)# ?  
  interface  Configure interfaces  
  show       Show running system information  
  end        Go to exec mode
```

exit           Exit from command interpreter

```
Nexus9000(config)# role name test
% Permission denied for the role
```

```
Nexus9000(config)#
```

```
Nexus9000(config)# interface loopback 0
% Interface permission denied
```

```
Nexus9000(config)#
Nexus9000# conf t
```

```
Nexus9000(config)# interface ethernet 1/5
Notice that only the commands allowed are listed.
Nexus9000(config-if)# ?
```

no	Negate a command or set its defaults
show	Show running system information
shutdown	Enable/disable an interface
end	Go to exec mode
exit	Exit from command interpreter

```
Nexus9000(config-if)# cdp
Nexus9000(config-if)# cdp enable
% Permission denied for the role
Nexus9000(config-if)#
```

## Troubleshoot

- Verifique que ISE sea accesible desde el dispositivo Nexus:

```
Nexus9000# ping <Su IP de ISE>
PING <Your ISE IP> (<Your ISE IP> 56 bytes de datos
64 bytes de <Su IP de ISE>: icmp_seq=0 ttl=59 tiempo=1,22 ms
64 bytes de <Su IP de ISE>: icmp_seq=1 ttl=59 tiempo=0,739 ms
64 bytes de <Su IP de ISE>: icmp_seq=2 ttl=59 tiempo=0,686 ms
64 bytes de <Su IP de ISE>: icmp_seq=3 ttl=59 tiempo=0,71 ms
64 bytes de <Su IP de ISE>: icmp_seq=4 ttl=59 tiempo=0,72 ms
```

- Verifique que el puerto 49 esté abierto entre ISE y el dispositivo Nexus:

```
Nexus9000# telnet <Su IP de ISE> 49
Intentando <Su IP de ISE>...
Conectado a <Su IP de ISE> .
El carácter de escape es '^'].
```

- Utilice estas depuraciones:

```
debug tacacs+ all
Nexus9000#
```

Nexus9000# 2024 19 de abril 22:50:44.199329 tacacs: event\_loop(): llamar a process\_rd\_fd\_set  
2024 19 de abril 22:50:44.199355 tacacs: process\_rd\_fd\_set: devolución de llamada de llamada para fd 6  
2024 19 de abril 22:50:44.199392 tacacs: fsrv no consumió el código operativo 8421  
2024 19 de abril 22:50:44.199406 tacacs: process\_implicit\_cfs\_session\_start: introduciendo...  
2024 19 de abril 22:50:44.199414 tacacs: process\_implicit\_cfs\_session\_start: exiting; estamos en estado de distribución inhabilitada  
2024 19 de abril 22:50:44.199424 tacacs: process\_aaa\_tplus\_request: introducción para aaa session id 0  
2024 19 de abril 22:50:44.199438 tacacs: process\_aaa\_tplus\_request:Comprobando el estado del puerto mgmt0 con servergroup lsePsnServers  
2024 19 de abril 22:50:44.199451 tacacs: tacacs\_global\_config(4220): introduciendo ...  
2024 19 de abril 22:50:44.199466 tacacs: tacacs\_global\_config(4577): GET\_REQ...  
2024 19 de abril 22:50:44.208027 tacacs: tacacs\_global\_config(4701): recuperó el valor devuelto por la operación de configuración de protocolo global:SUCCESS  
2024 19 de abril 22:50:44.208045 tacacs: tacacs\_global\_config(4716): REQ:num server 0  
2024 19 de abril 22:50:44.208054 tacacs: tacacs\_global\_config: REQ:num group 1  
2024 19 de abril 22:50:44.208062 tacacs: tacacs\_global\_config: REQ:num timeout 5  
2024 19 de abril 22:50:44.208070 tacacs: tacacs\_global\_config: REQ:num deadtime 0  
2024 19 de abril 22:50:44.208078 tacacs: tacacs\_global\_config: REQ:num encryption\_type 7  
2024 19 de abril 22:50:44.208086 tacacs: tacacs\_global\_config: devolviendo reval 0  
2024 19 de abril 22:50:44.208098 tacacs: process\_aaa\_tplus\_request:group\_info se rellena en aaa\_req, por lo que se utiliza servergroup lsePsnServers  
2024 19 de abril 22:50:44.208108 tacacs: tacacs\_servergroup\_config: introducir para grupo de servidores, índice 0  
2024 19 de abril 22:50:44.208117 tacacs: tacacs\_servergroup\_config: GETNEXT\_REQ para índice de grupo de servidores de protocolo:0 nombre:  
2024 19 de abril 22:50:44.208148 tacacs: tacacs\_pss2\_move2key: rcode = 40480003 syserr2str = no existe tal clave pss  
2024 19 de abril 22:50:44.208160 tacacs: tacacs\_pss2\_move2key: llamando a pss2\_getkey  
2024 19 de abril 22:50:44.208171 tacacs: tacacs\_servergroup\_config: GETNEXT\_REQ obtuvo el índice de grupo de servidores de protocolo:2 name:lsePsnServers  
2024 19 de abril 22:50:44.208184 tacacs: tacacs\_servergroup\_config: recuperó el valor devuelto por la operación de grupo de protocolos:CORRECTO  
2024 19 de abril 22:50:44.208194 tacacs: tacacs\_servergroup\_config: devolviendo el valor de retorno 0 para el grupo de servidores Protocol:lsePsnServers  
2024 19 de abril 22:50:44.208210 tacacs: process\_aaa\_tplus\_request: Grupo lsePsnServers encontrado. el vrf correspondiente es el predeterminado, source-intf es 0  
2024 19 de abril 22:50:44.208224 tacacs: process\_aaa\_tplus\_request: comprobación de mgmt0 vrf:management contra vrf:default del grupo solicitado  
2024 19 de abril 22:50:44.208256 tacacs: process\_aaa\_tplus\_request:mgmt\_if 83886080  
2024 19 de abril 22:50:44.208272 tacacs: process\_aaa\_tplus\_request:global\_src\_intf: 0, src\_intf local es 0 y vrf\_name es el predeterminado  
2024 19 de abril 22:50:44.208286 tacacs: create\_tplus\_req\_state\_machine(902): introducción para aaa session id 0  
2024 19 de abril 22:50:44.208295 tacacs: state machine count 0

2024 19 de abril 22:50:44.208307 tacacs: init\_tplus\_req\_state\_machine: introducción para aaa session id 0

2024 19 de abril 22:50:44.208317 tacacs: init\_tplus\_req\_state\_machine(1298):tplus\_ctx es NULL, debería serlo si el autor y la prueba

2024 19 de abril 22:50:44.208327 tacacs: tacacs\_servergroup\_config: escribir para el grupo de servidoresIsePsnServers, índice 0

2024 19 de abril 22:50:44.208339 tacacs: tacacs\_servergroup\_config: GET\_REQ for Protocol server group index:0 name:IsePsnServers

2024 19 de abril 22:50:44.208357 tacacs: find\_tacacs\_servergroup: introducir para el grupo de servidores IsePsnServers

2024 19 de abril 22:50:44.208372 tacacs: tacacs\_pss2\_move2key: rcode = 0 syserr2str = ÉXITO

2024 19 de abril 22:50:44.208382 tacacs: find\_tacacs\_servergroup: El índice de salida del grupo de servidores IsePsnServers es 2

2024 19 de abril 22:50:44.208401 tacacs: tacacs\_servergroup\_config: GET\_REQ: find\_tacacs\_servergroup error 0 para Protocol server group IsePsnServers

2024 19 de abril 22:50:44.208420 tacacs: tacacs\_pss2\_move2key: rcode = 0 syserr2str = ÉXITO

2024 19 de abril 22:50:44.208433 tacacs: tacacs\_servergroup\_config: GET\_REQ obtuvo el índice de grupo de servidores Protocol:2 name:IsePsnServers

2024 A2024 19 de abril 22:52024 19 de abril 22:52024 19 de abril 22:5  
Nexus9000#

- Realizar una captura de paquetes. (Para ver los detalles del paquete, debe cambiar las preferencias de Wireshark TACACS+ y actualizar la clave compartida que utilizan Nexus e ISE.)

```

No. | Time | Sc | De | Protocol | Length | Info
---|---|---|---|---|---|---
66 | 22:25:08.757401 | ... | ... | TACACS+ | 107 | R: Authorization

> Transmission Control Protocol, Src Port: 49, Dst Port: 58863, Seq: 1, Ack: 90, Len: 41
  TACACS+
    Major version: TACACS+
    Minor version: 0
    Type: Authorization (2)
    Sequence number: 2
    > Flags: 0x00 (Encrypted payload, Multiple Connections)
    Session ID: 1136115821
    Packet length: 29
    Encrypted Reply
    < Decrypted Reply
      Auth Status: PASS_REPL (0x02)
      Server Msg length: 0
      Data length: 0
      Arg count: 1
      Arg[0] length: 22
      Arg[0] value: shell:roles="helpdesk"
  
```

- Compruebe que la clave compartida es la misma en ISE y Nexus. Esto también se puede comprobar en Wireshark.

## TACACS+

```
Major version: TACACS+
Minor version: 1
Type: Authentication (1)
Sequence number: 1
Flags: 0x00 (Encrypted payload, Multiple Connections)
Session ID: 232251350
Packet length: 43
Encrypted Request
Decrypted Request
  Action: Inbound Login (1)
  Privilege Level: 1
  Authentication type: PAP (2)
  Service: Login (1)
  User len: 9
  User: iseiscool
  Port len: 1
  Port: 0
  Remaddr len: 12
  Remote Address: ██████████
  Password Length: 13
  Password: VainillaISE97
```

Paquete de autenticación

## Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).