Configuración del rol TACACS personalizado para Nexus 9K mediante ISE 3.2

Contenido

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

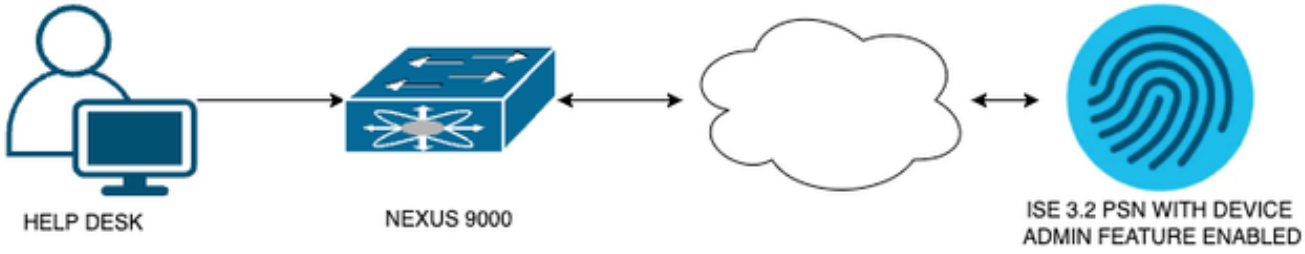
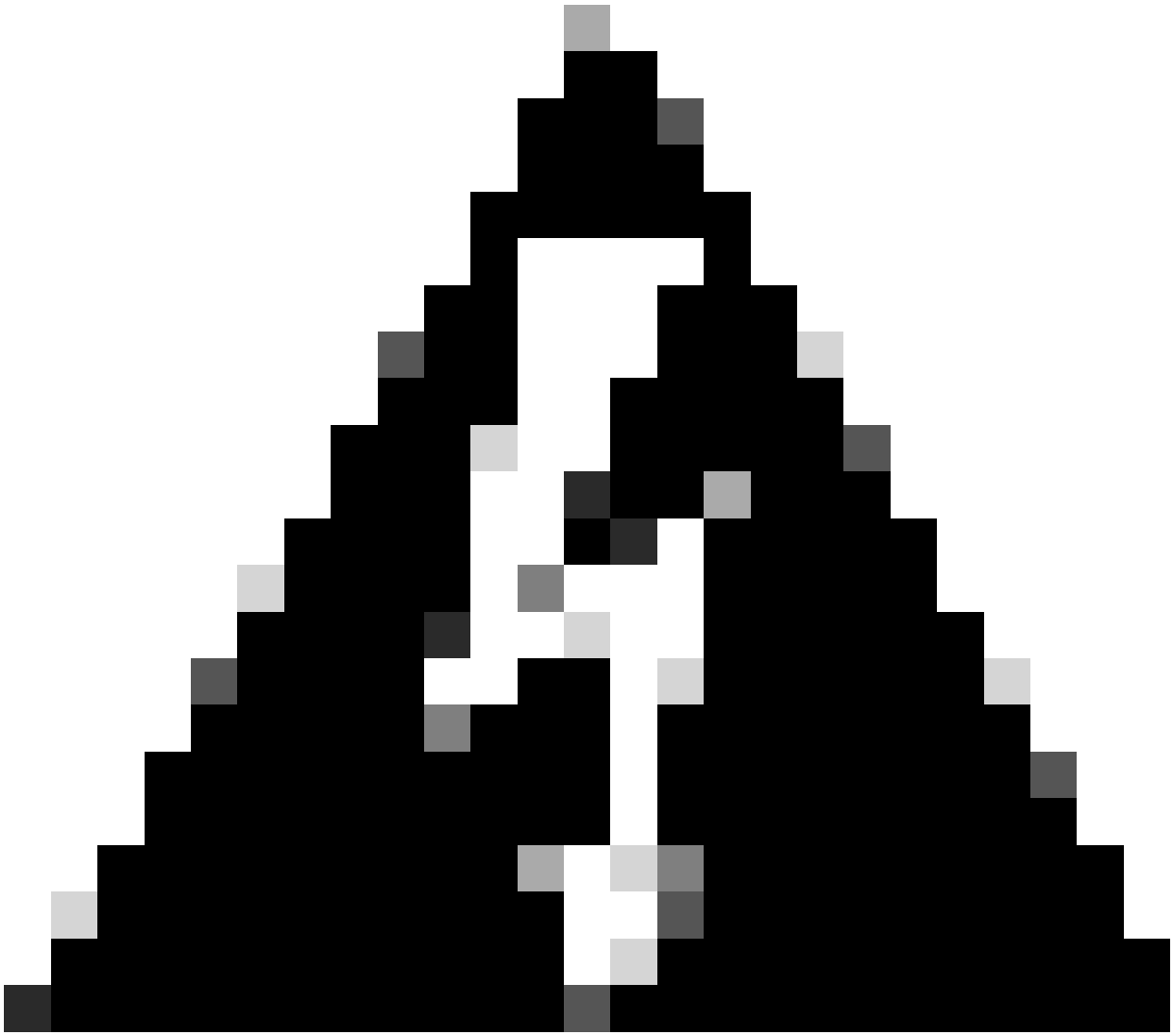


Diagrama de componentes de flujo

Paso 1: Configuración de Nexus 9000

1. Configuración 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.

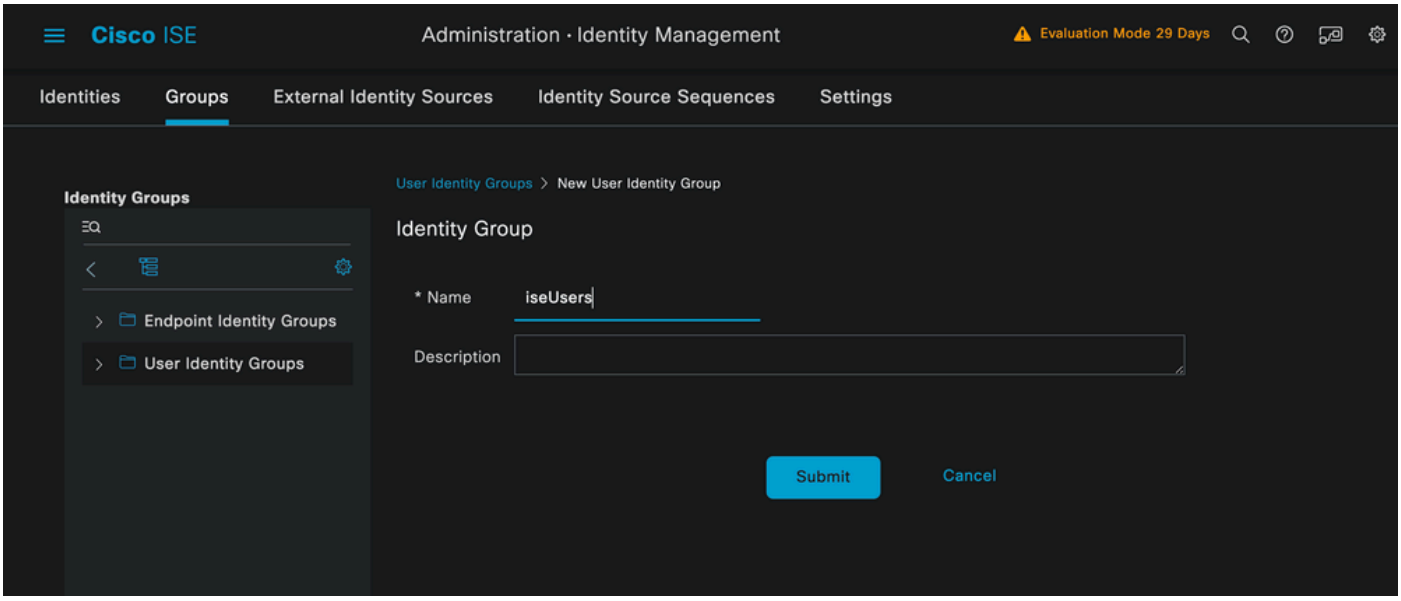
```
Nexus9000(config)# role name helpdesk
Nexus9000(config-role)#   description Can perform basic Toubleshooting and bounce certain  ports
Nexus9000(config-role)# rule 1 permit read
Nexus9000(config-role)# rule 2 permit command enable *
Nexus9000(config-role)# rule 3 permit command ssh *
Nexus9000(config-role)# 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.

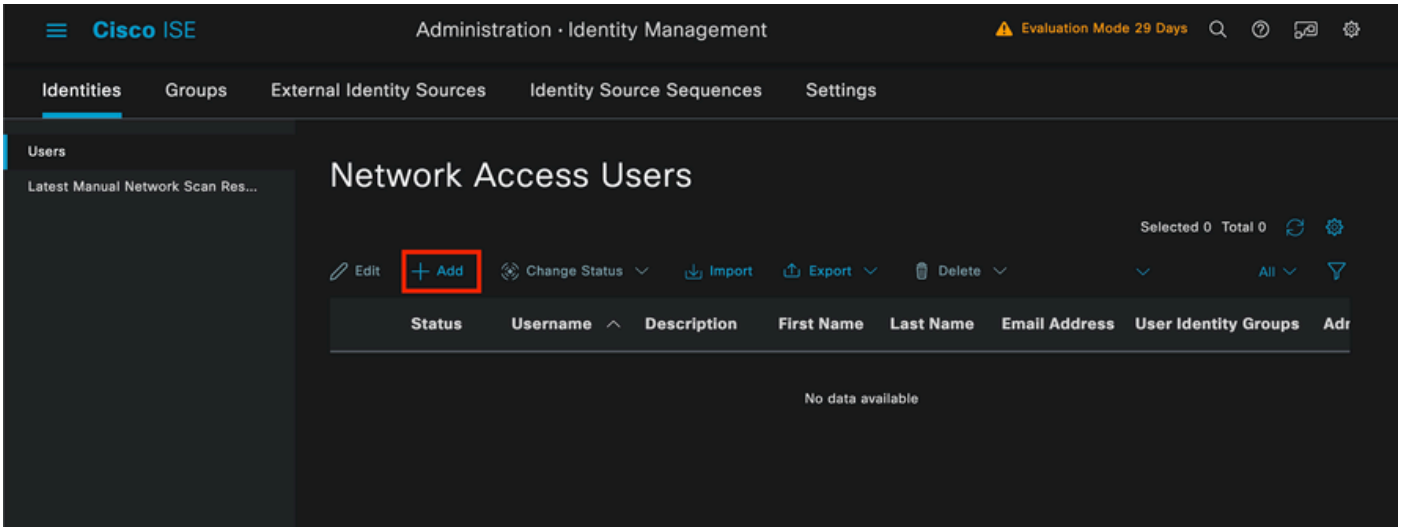


Creación de un grupo de usuarios

Haga clic en el botón Submit.

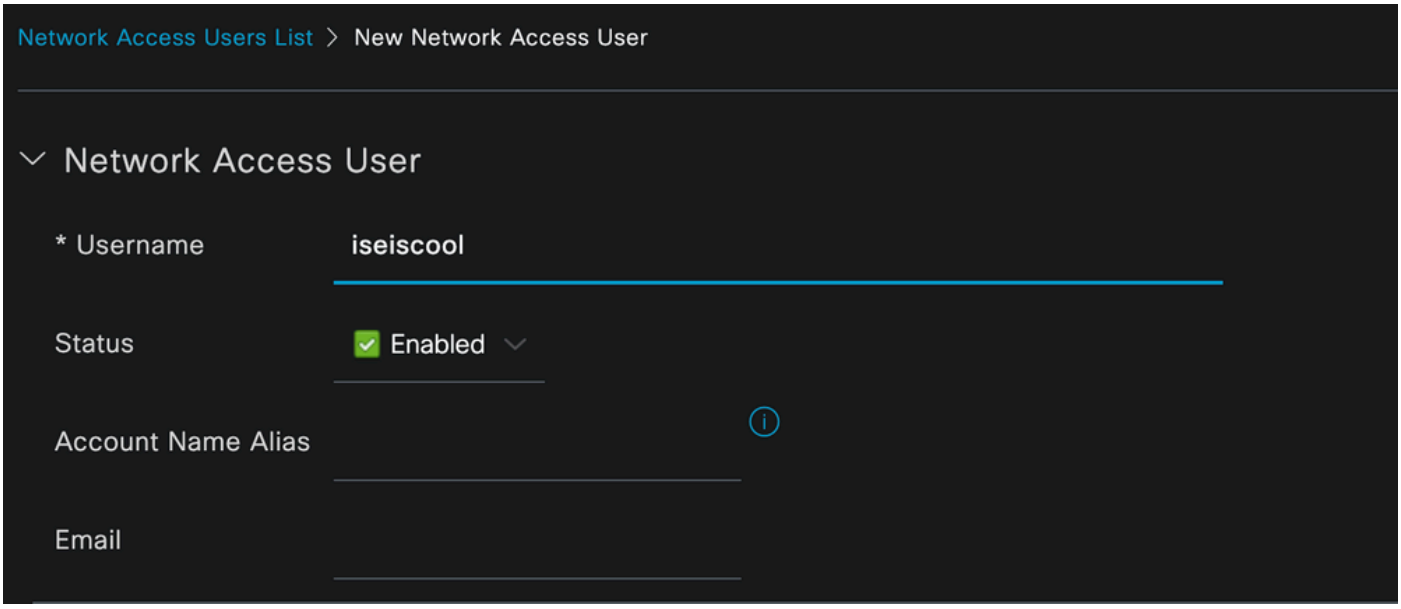
A continuación, vaya a la ficha Administration > Identity Management > Identity.

Presione el botón Add.



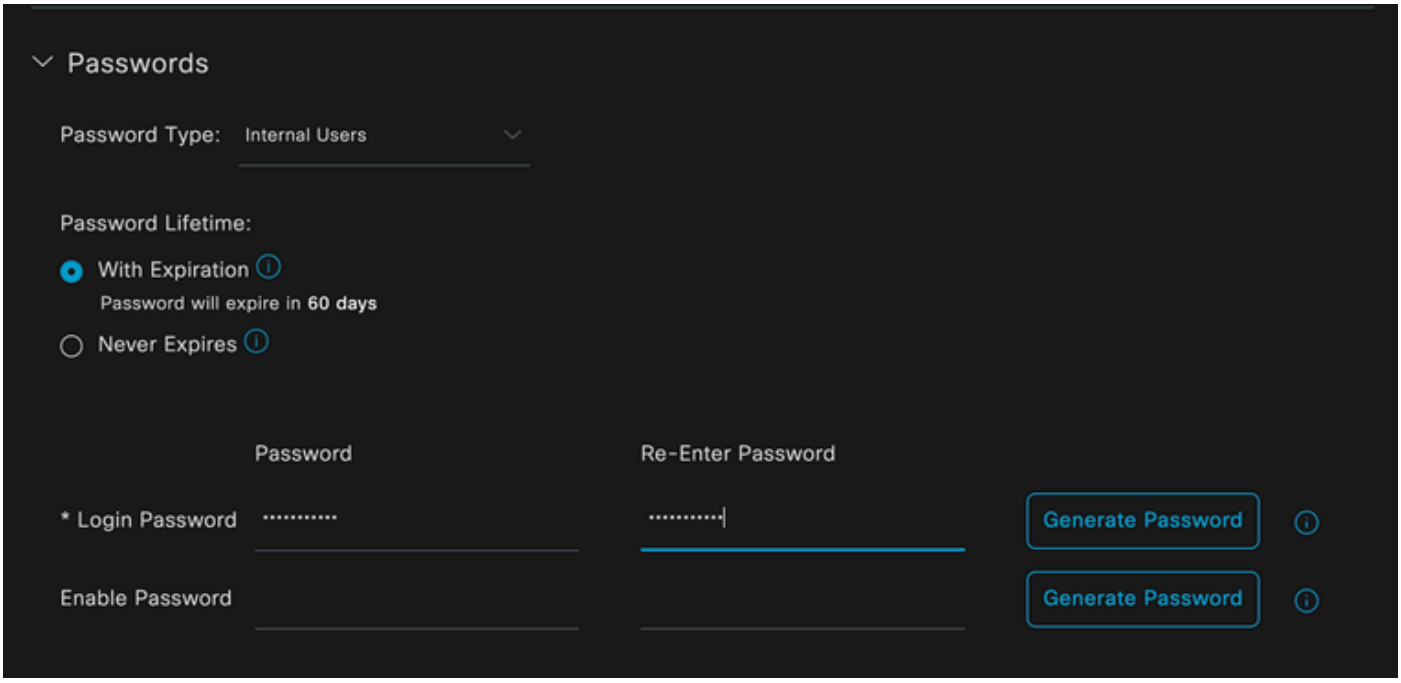
Creación de usuario

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



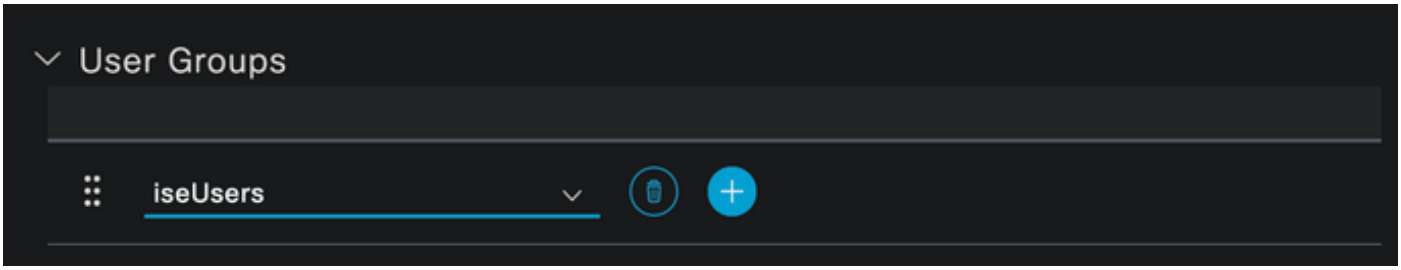
Nombrar al usuario y crearlo

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



Asignación de contraseña

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

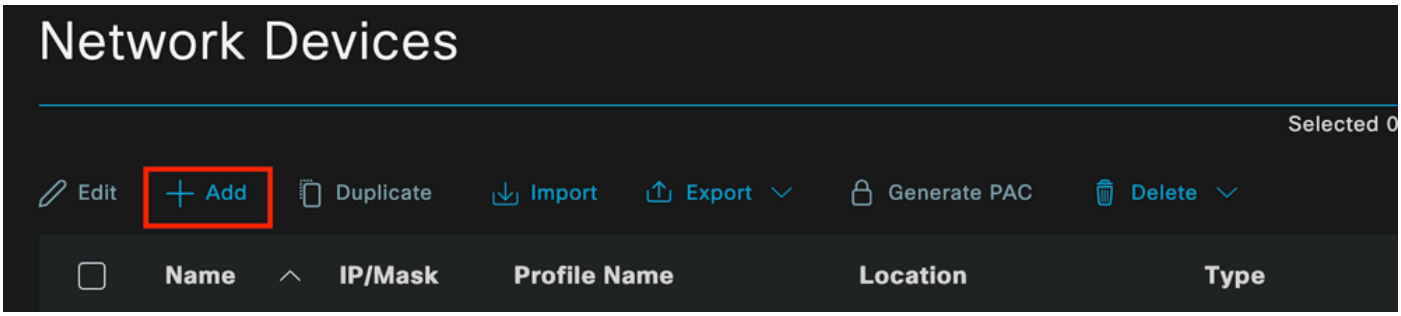


Asignación de grupo

2. Configure y agregue el dispositivo de red.

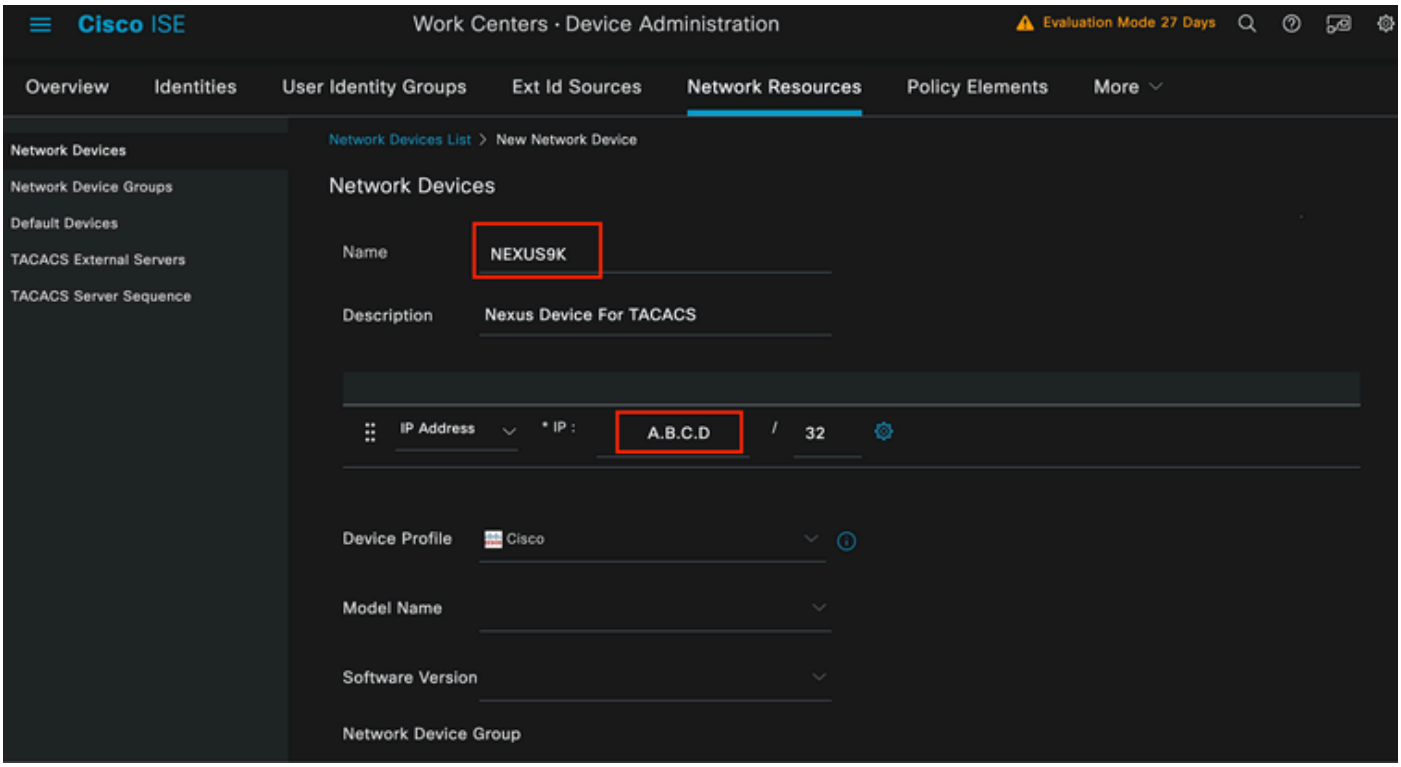
Agregue el dispositivo NEXUS 9000 a ISE Administration > Network Resources > Network Devices

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.



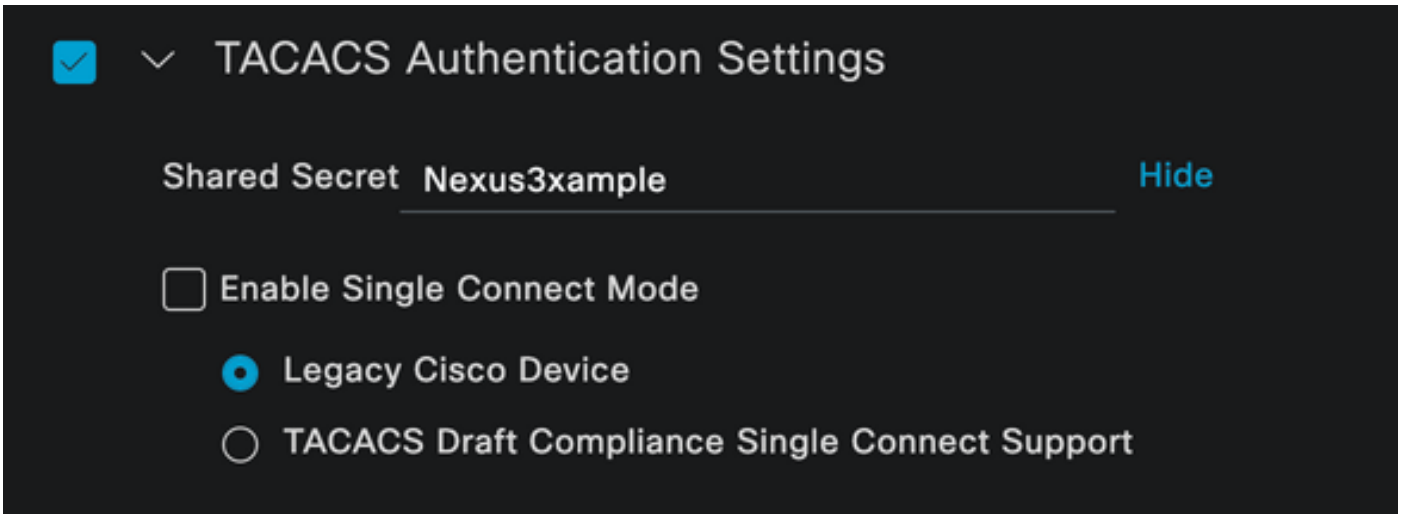
Configurar dispositivo de red

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 el secreto compartido que utilizó en la configuración de NAD para esta demostración; en

esta demostración se utiliza Nexus3xample.

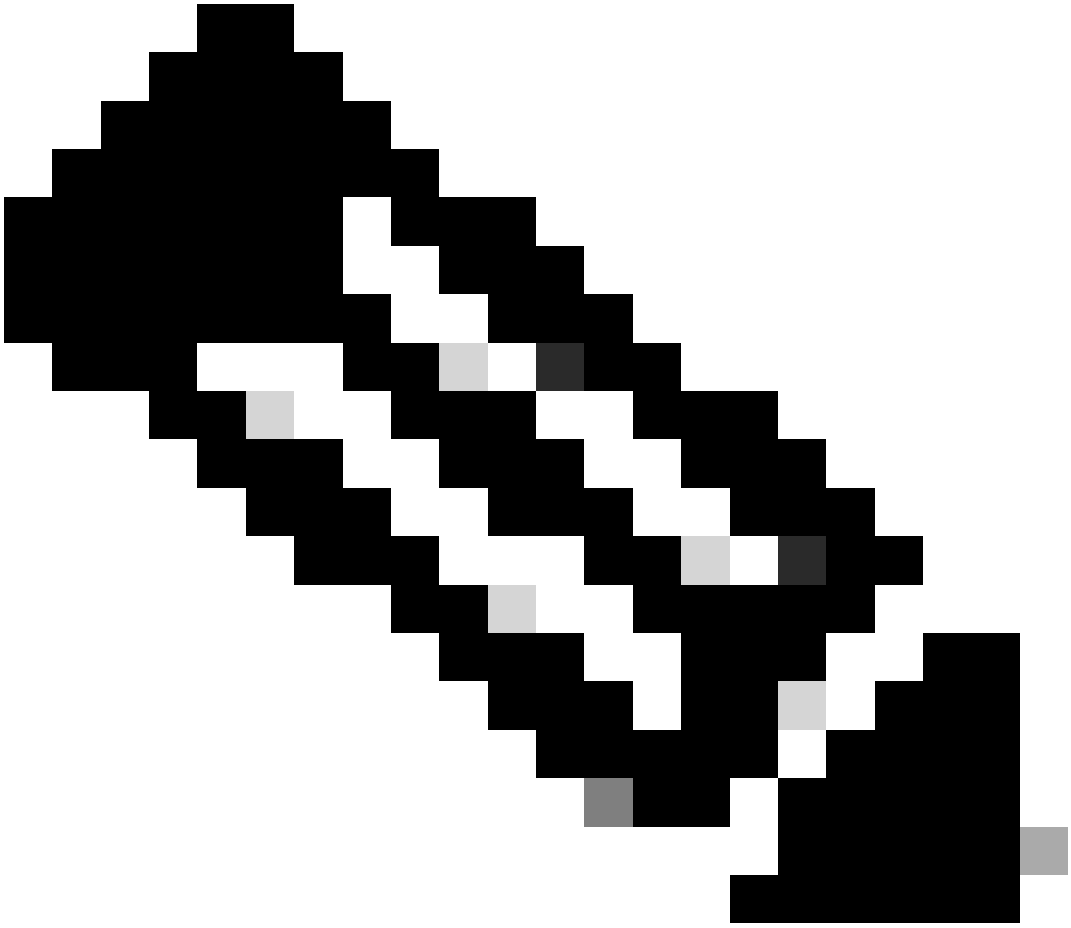


sección de configuración de TACACS

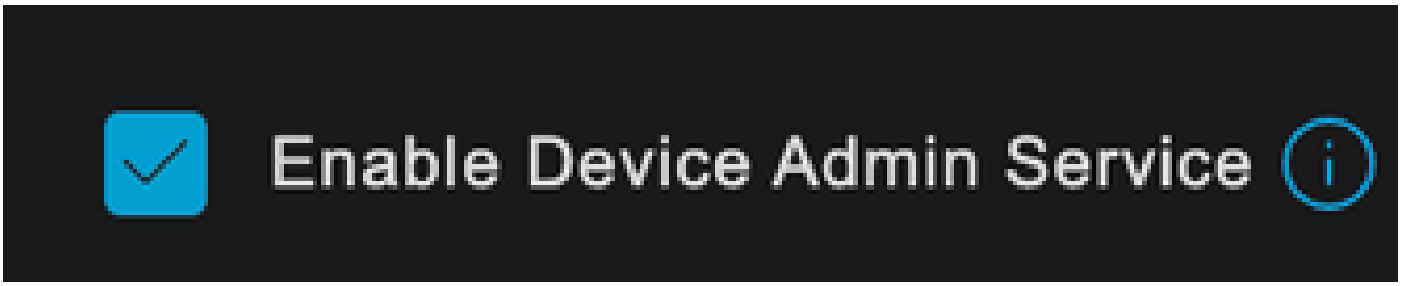
Guarde los cambios haciendo clic en el botón Submit.

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.



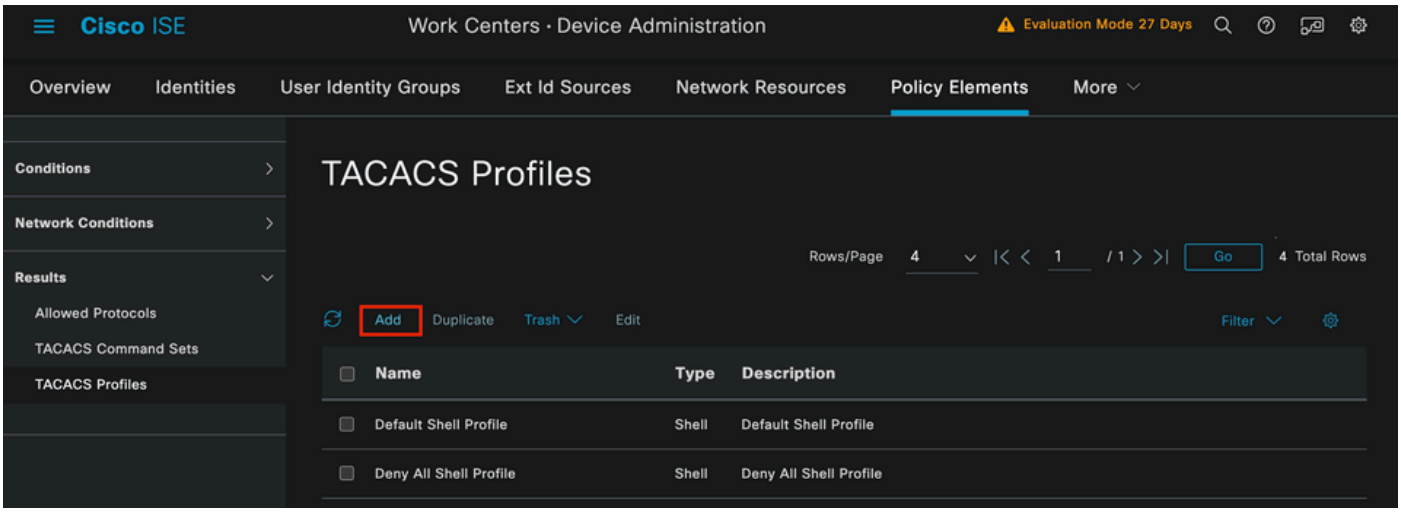
Comprobación de la función PSN Device Admin

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.

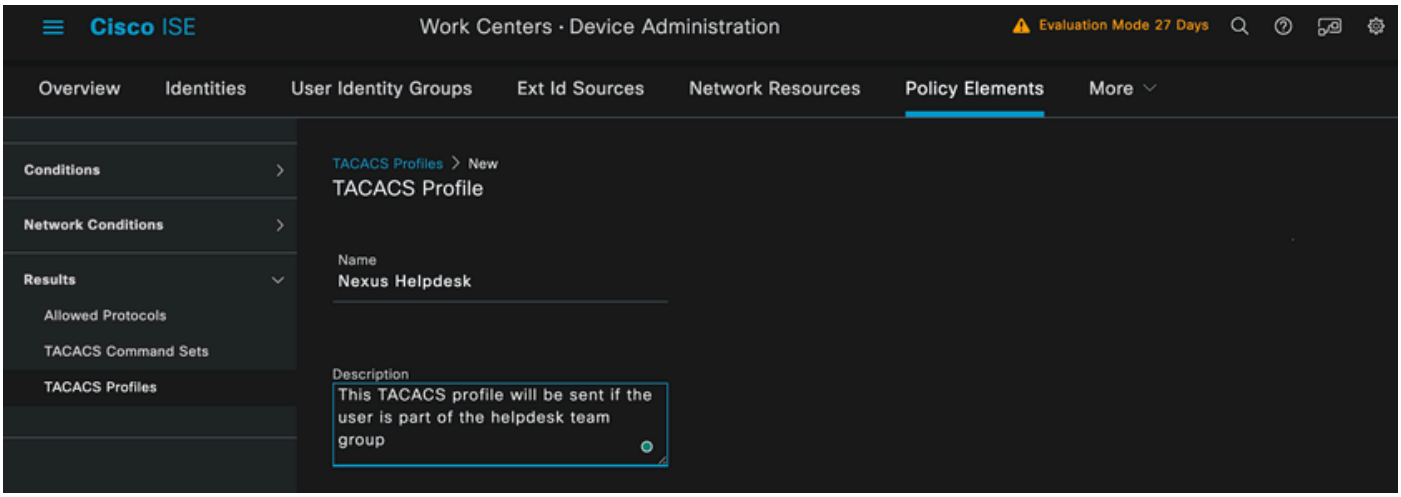
En el menú de ISE, vaya a Workcenters > Device Administration > Policy Elements > Results >

TACACS Profiles y haga clic en el botón Add.



Perfil TACACS

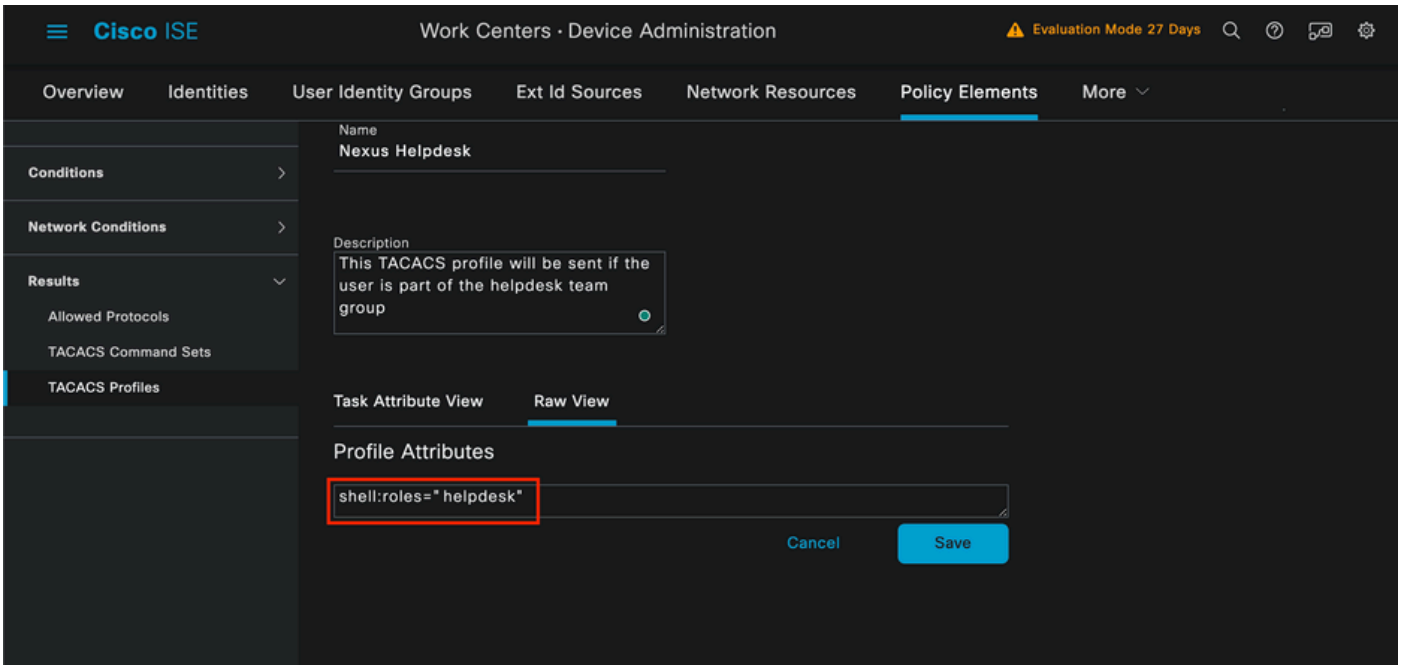
Asigne un nombre y, opcionalmente, una descripción.



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".



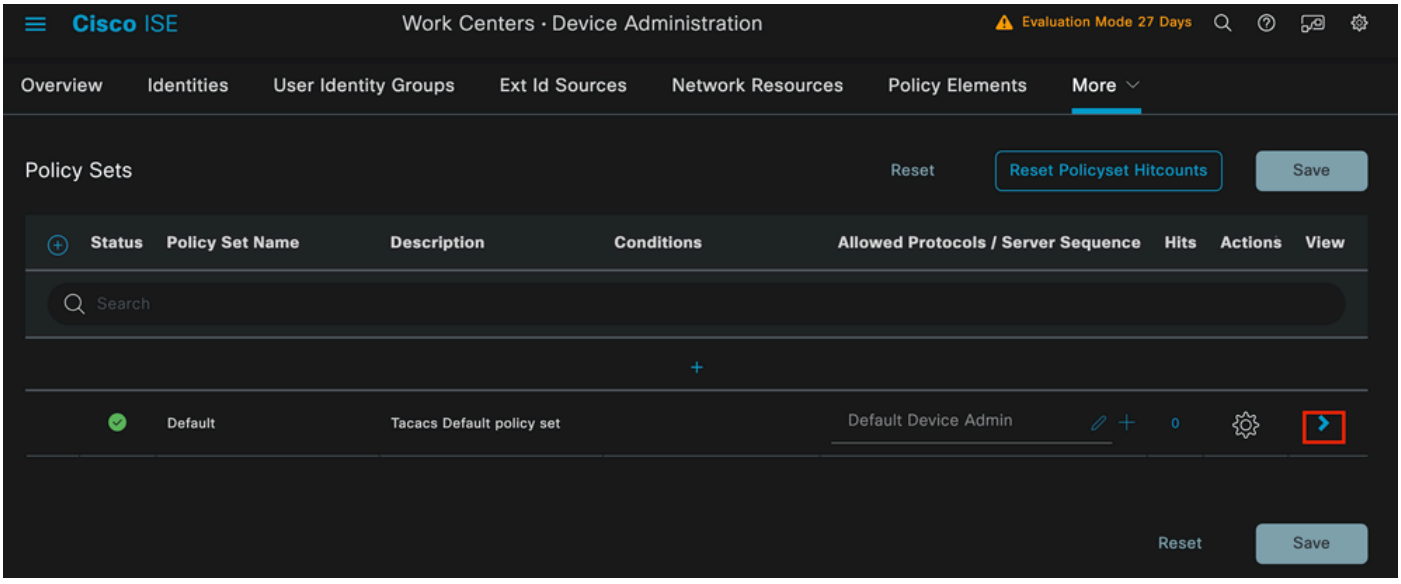
Adición de atributos de perfil

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 para que coincida con escenarios específicos.

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

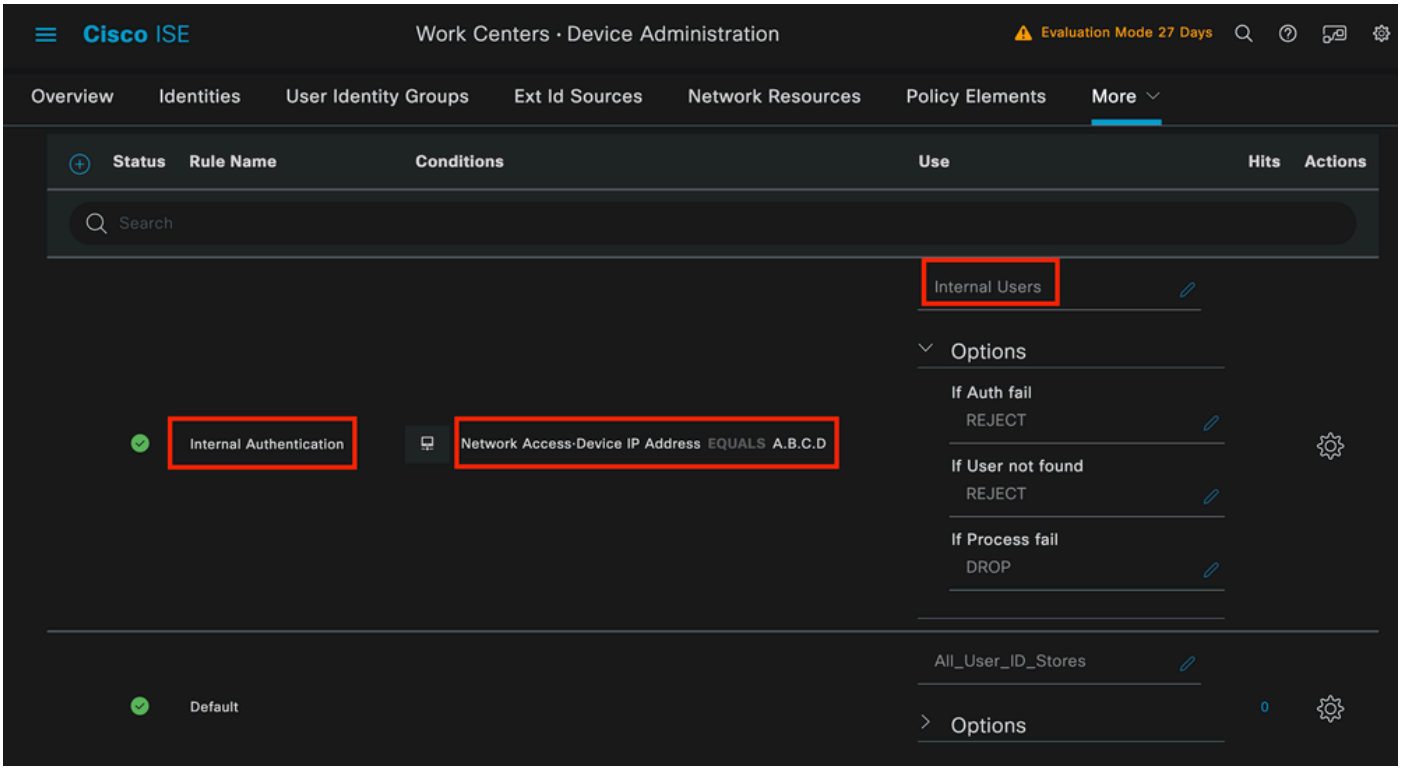


Página Conjuntos de directivas de administración de dispositivos

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.

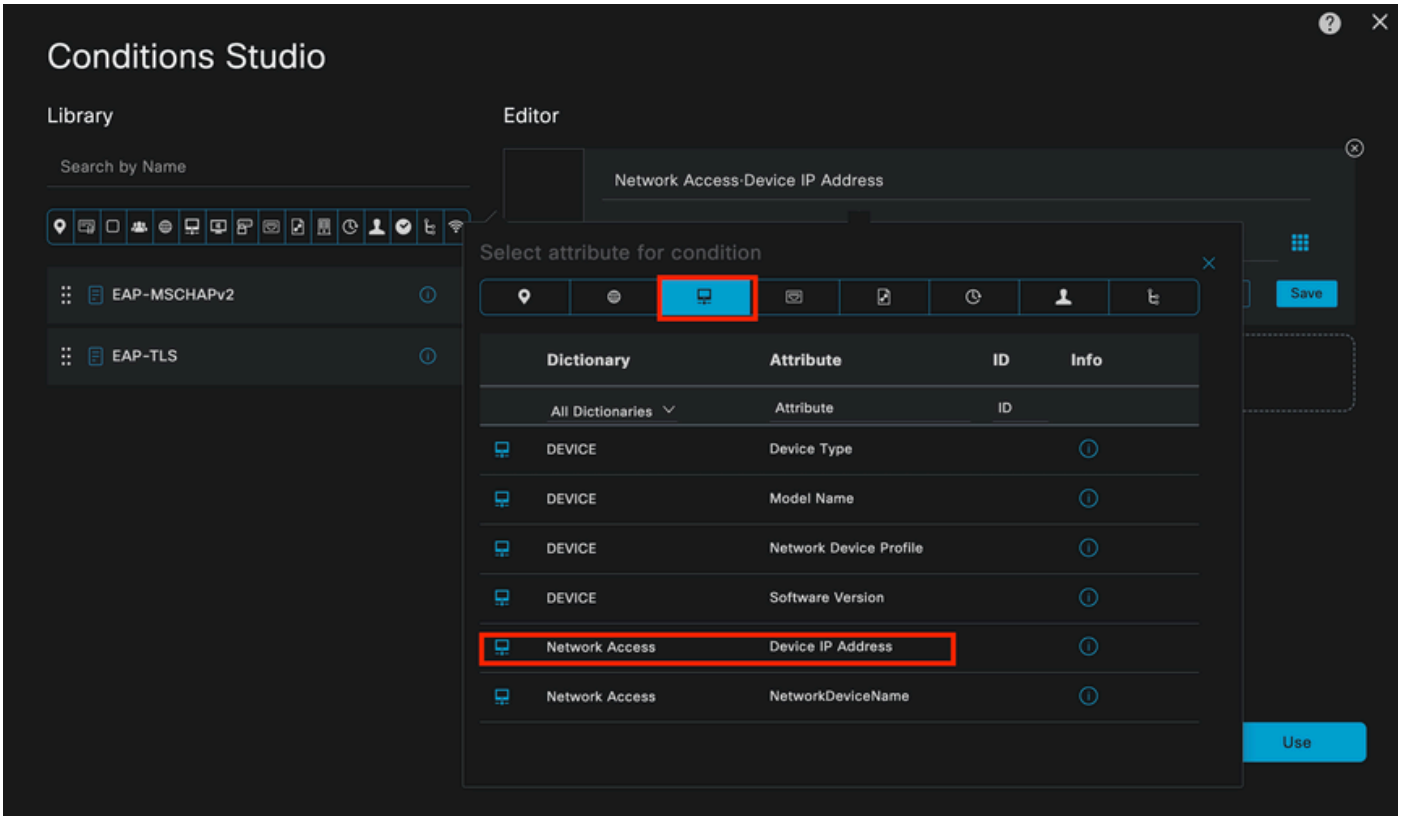
Para este ejemplo de configuración, el valor Name es Internal Authentication y la condición elegida es Network Device (Nexus) IP (sustituya el A.B.C.D.). Esta directiva de autenticación utiliza el almacén de identidad de usuarios internos.



Política de autenticación

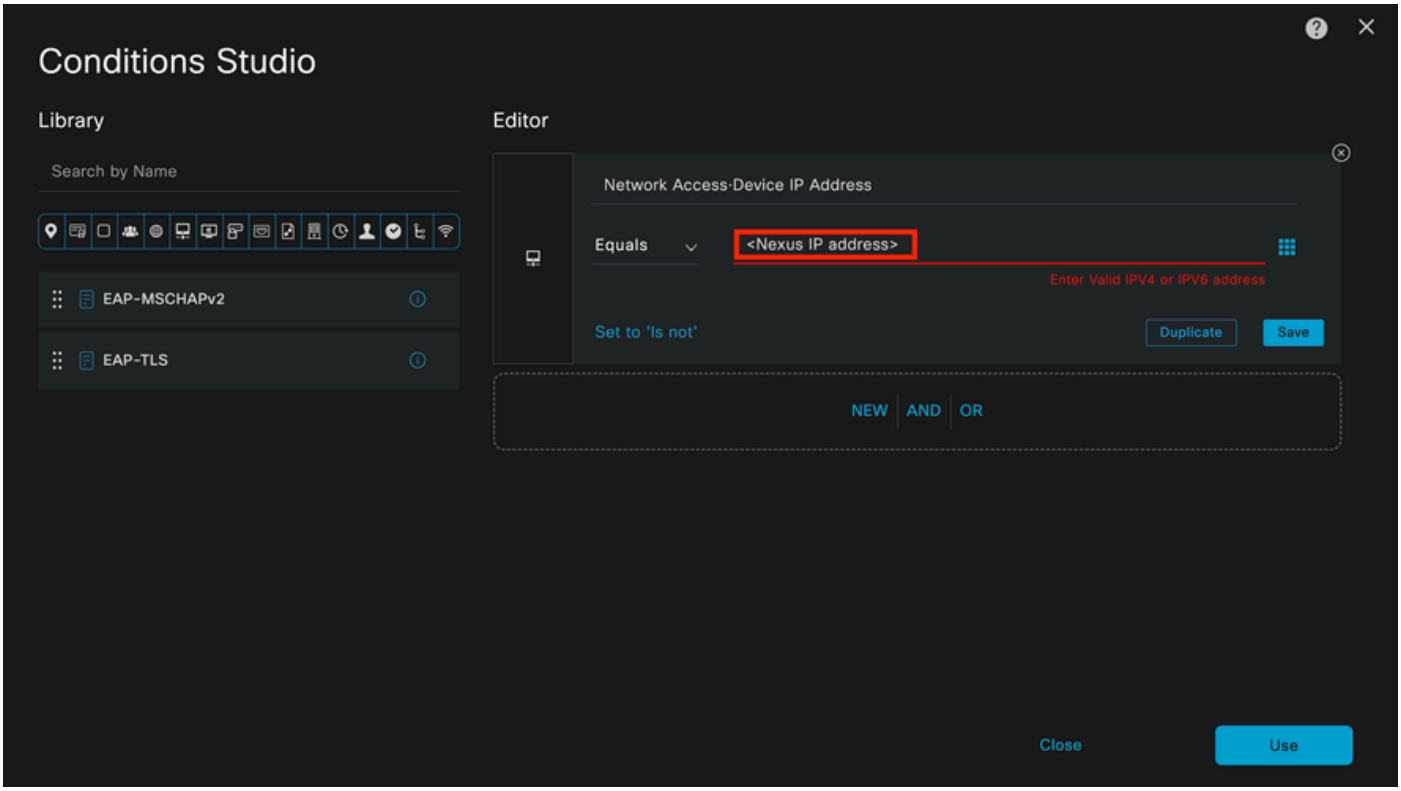
Así es como se configuró la condición.

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

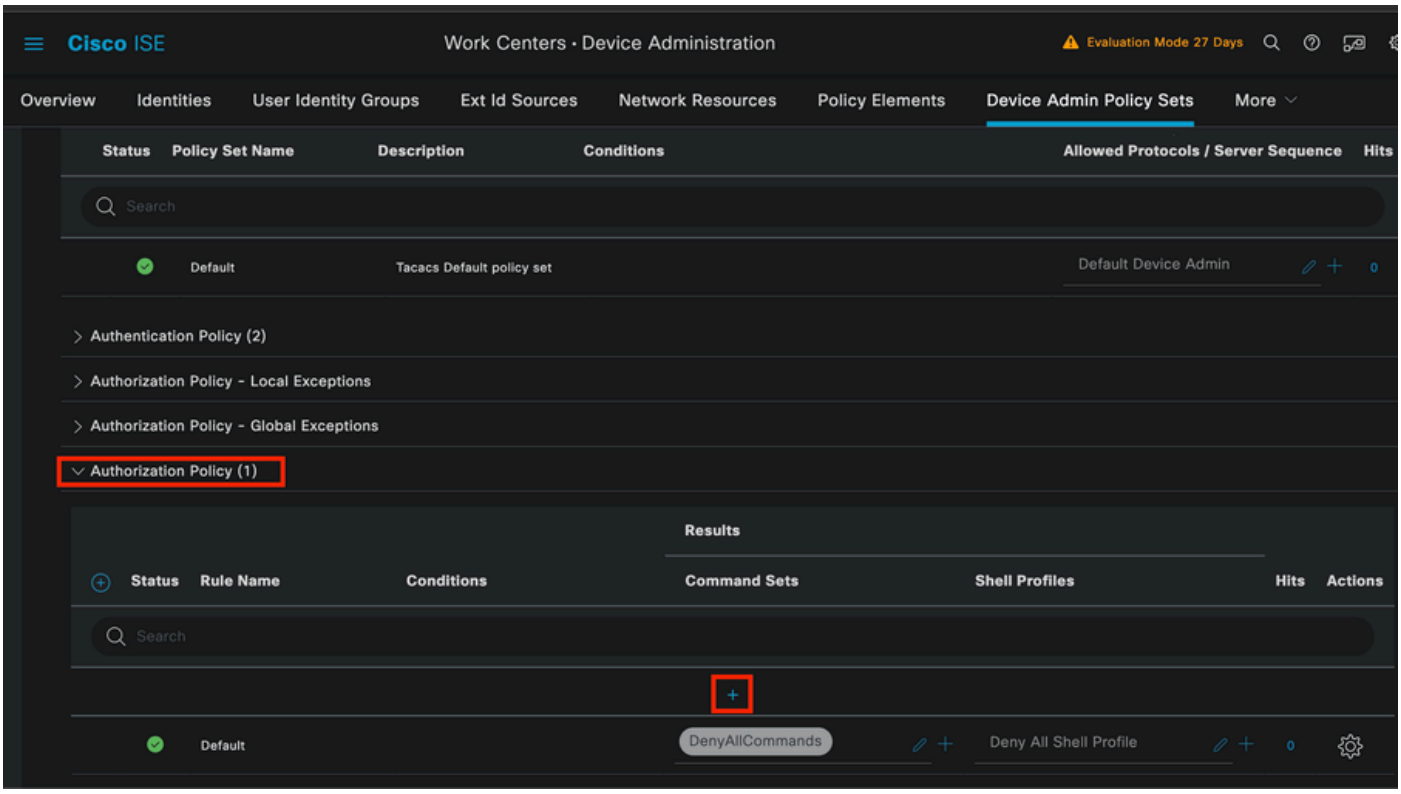
Haga clic en el botón Use.

Esta condición solo la cumple el dispositivo Nexus configurado; sin embargo, si el propósito es

habilitar esta condición para una gran cantidad de dispositivos, se debe considerar una condición diferente.

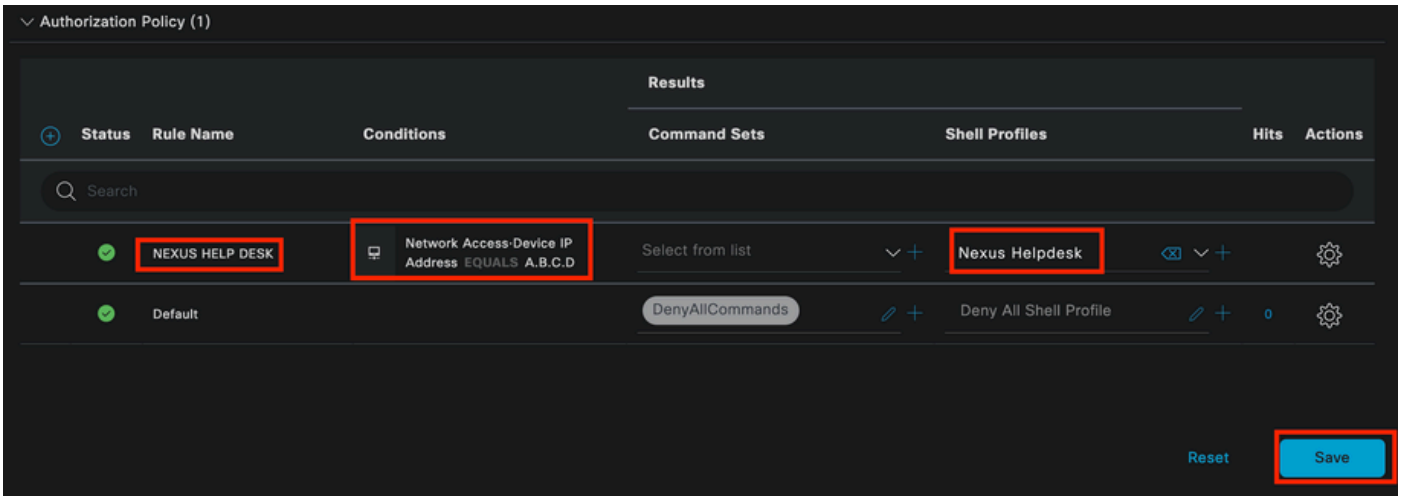
A continuación, desplácese a la sección Directiva de autorización y expándala.

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.

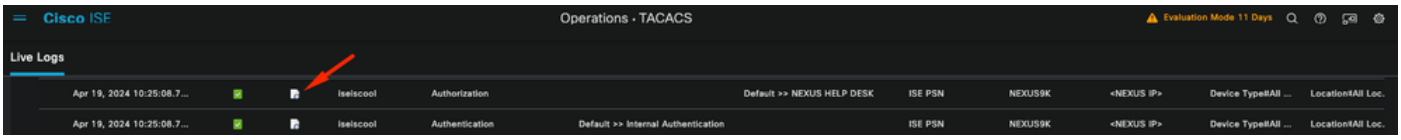
En la columna Perfiles de shell, se selecciona el perfil configurado antes de Nexus Helpdesk.

Por último, haga clic en el botón Save.

Verificación

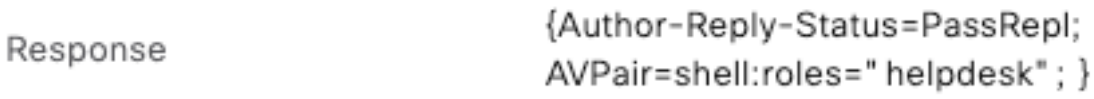
Utilize esta sección para confirmar que su configuración funcione correctamente.

Desde la GUI de ISE, navegue hasta Operations > 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.



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"



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

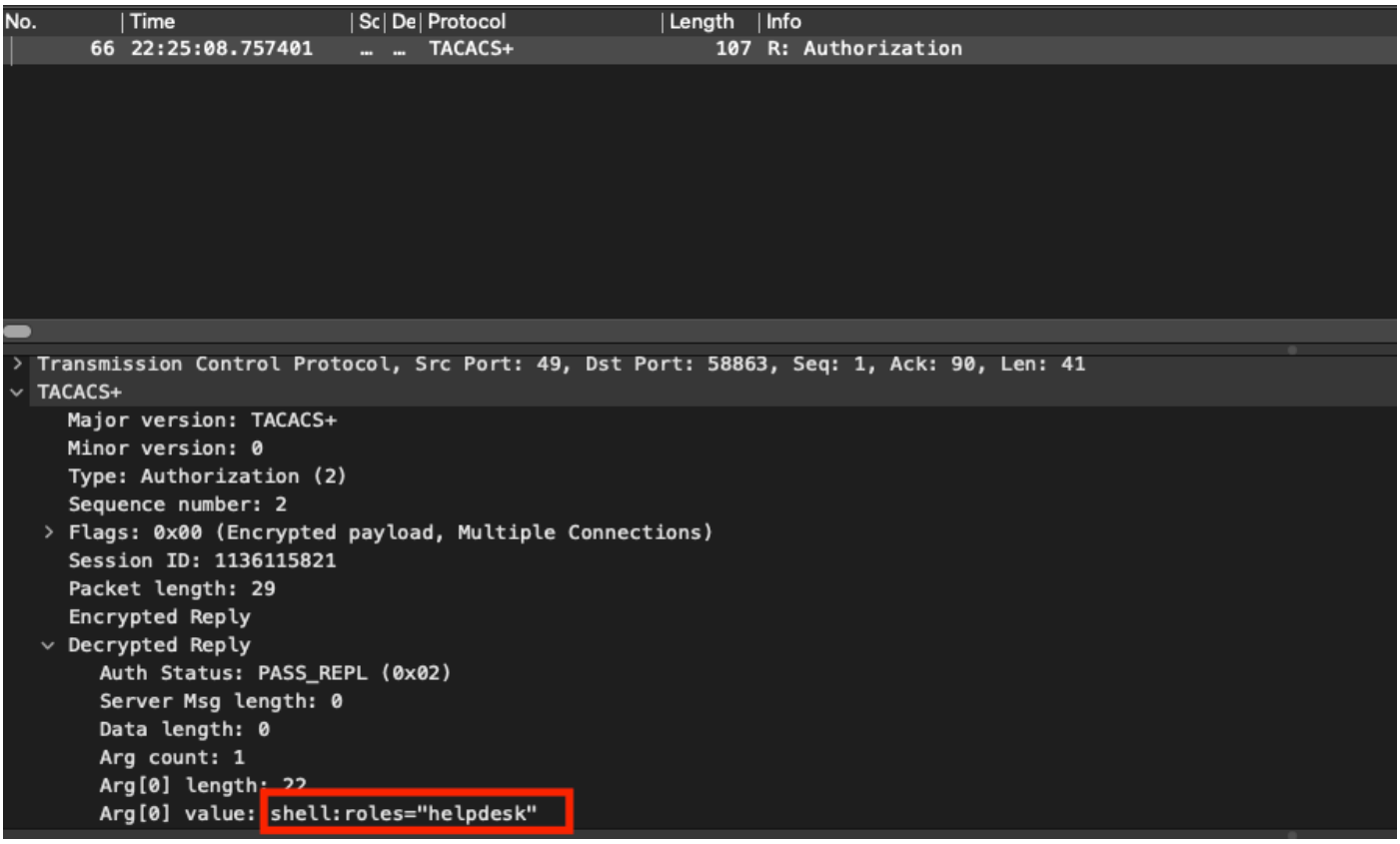
- Verifique que ISE sea accesible desde el dispositivo Nexus.Nexus9000# ping <Su IP de ISE>
  PING <Su IP de ISE> (<Su IP de ISE>> 56 bytes de datos
  64 bytes de <Su IP de ISE>: icmp_seq=0 ttl=59 tiempo=1,22 ms
  64 bytes de <Su IP de ISE>: icmp_seq=1 ttl=59 tiempo=0,739 ms
  64 bytes de <Su IP de ISE>: 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 Apr 19 22:50:44.199329 tacacs: event_loop(): calling 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 Apr 19 22:50:44.199392 tacacs: fsrv no consumió 8421 opcode
2024 Abr 19 22:50:44.199406 tacacs: process_implicit_cfs_session_start: introduciendo...
2024 Abril 19 22:50:44.199414 tacacs: process_implicit_cfs_session_start: salir; estamos en estado de distribución inhabilitada
2024 Apr 19 22:50:44.199424 tacacs: process_aaa_tplus_request: introducción de aaa session id 0
2024 Apr 19 22:50:44.199438 tacacs: process_aaa_tplus_request:Comprobando el estado del puerto mgmt0 con servergroup IsePsnServers
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 de 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 Apr 19 22:50:44.208062 tacacs: tacacs_global_config: REQ:num timeout 5
2024 Abr 19 22:50:44.208070 tacacs: tacacs_global_config: REQ:num deadtime 0
2024 Abr 19 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 Apr 19 22:50:44.208098 tacacs: process_aaa_tplus_request:group_info se completa en aaa_req, por lo que el uso de servergroup IsePsnServers
2024 Apr 19 22:50:44.208108 tacacs: tacacs_servergroup_config: introducción para el grupo de servidores, índice 0
2024 Abr 19 22:50:44.208117 tacacs: tacacs_servergroup_config: GETNEXT_REQ for Protocol server group index:0 name:
2024 Abr 19 22:50:44.208148 tacacs: tacacs_pss2_move2key: rcode = 40480003 syserr2str = no hay tal clave pss
2024 Abr 19 22:50:44.208160 tacacs: tacacs_pss2_move2key: llamando a pss2_getkey
2024 Abr 19 22:50:44.208171 tacacs: tacacs_servergroup_config: GETNEXT_REQ got Protocol server group index:2 name:IsePsnServers
2024 Apr 19 22:50:44.208184 tacacs: tacacs_servergroup_config: recuperó el valor devuelto de la operación de grupo de protocolos:SUCCESS
2024 Apr 19 22:50:44.208194 tacacs: tacacs_servergroup_config: devolviendo el valor de retorno 0 para el grupo de servidores Protocol:IsePsnServers
2024 Abr 19 22:50:44.208210 tacacs: process_aaa_tplus_request: Se encontraron IsePsnServers de grupo. el vrf correspondiente es el valor predeterminado, source-intf es 0
2024 19 de abril 22:50:44.208224 tacacs: process_aaa_tplus_request: verificación de mgmt0 vrf:management contra vrf:default del grupo solicitado
19 de abril de 2024 22:50:44.208256 tacacs: process_aaa_tplus_request:mgmt_if 83886080
2024 Abr 19 22:50:44.208272 tacacs: process_aaa_tplus_request:global_src_intf : 0, local src_intf es 0 y vrf_name es el valor predeterminado
2024 Apr 19 22:50:44.208286 tacacs: create_tplus_req_state_machine(902): introducción de aaa session id 0
2024 19 de abril 22:50:44.208295 tacacs: recuento de máquinas de estado 0
2024 Apr 19 22:50:44.208307 tacacs: init_tplus_req_state_machine: introducción de aaa session id 0
2024 Abr 19 22:50:44.208317 tacacs: init_tplus_req_state_machine(1298):tplus_ctx es NULL debería ser si autor y prueba
2024 Apr 19 22:50:44.208327 tacacs: tacacs_servergroup_config: introducir para el grupo de servidores IsePsnServers, índice 0
2024 Abr 19 22:50:44.208339 tacacs: tacacs_servergroup_config: GET_REQ para el índice de grupo de servidores de protocolo:0 name:IsePsnServers
2024 Apr 19 22:50:44.208357 tacacs: find_tacacs_servergroup: introducción para el grupo de servidores IsePsnServers
2024 Abr 19 22:50:44.208372 tacacs: tacacs_pss2_move2key: rcode = 0 syserr2str = SUCCESS
2024 Abr 19 22:50:44.208382 tacacs: find_tacacs_servergroup: salir del grupo de servidores IsePsnServers index es 2

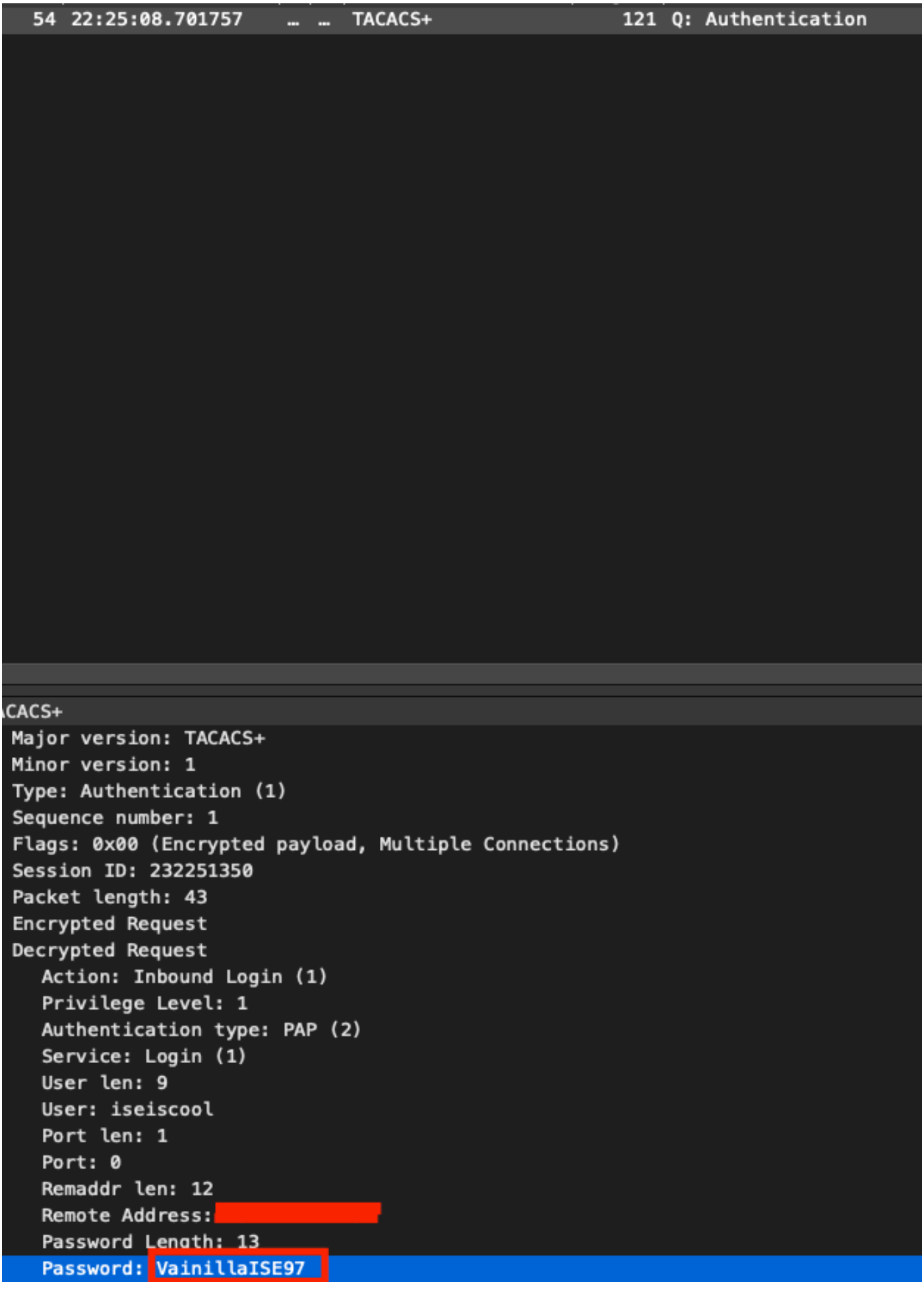
2024 Abr 19 22:50:44.208401 tacacs: tacacs_servergroup_config: GET_REQ: find_tacacs_servergroup error 0 para el grupo de servidores de protocolo IsePsnServers
2024 Abr 19 22:50:44.208420 tacacs: tacacs_pss2_move2key: rcode = 0 syserr2str = SUCCESS
2024 Abr 19 22:50:44.208433 tacacs: tacacs_servergroup_config: GET_REQ got Protocol server group index: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 utilizada por Nexus e ISE)



Paquete de autorización TACACS

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



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).