Testdocument

Inleiding

In dit document wordt beschreven hoe u een aangepaste Nexus-rol voor TACACS kunt configureren via CLI op NK9.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- TACACS +
- ISE 3.2

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco Nexus9000, NXOS-beeldbestand is: bootflash:///nxos.9.3.5.bin
- Identity Service Engine versie 3.2

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Vergunningseisen

Cisco NX-OS - TACACS+ vereist geen licentie.

Cisco Identity Service Engine

Voor nieuwe ISE-installaties hebt u een evaluatieperiode van 90 dagen met licentie die toegang heeft tot alle ISE-functies. Als u geen evaluatielicentie hebt, hebt u voor het gebruik van de ISE TACACS-functie een apparaatbeheerlicentie nodig voor de Policy Server-node die de verificatie uitvoert.

Nadat de Admin/Helpdesk-gebruikers zich hebben geverifieerd op het Nexus-apparaat, retourneert ISE de gewenste Nexus-shell-rol.

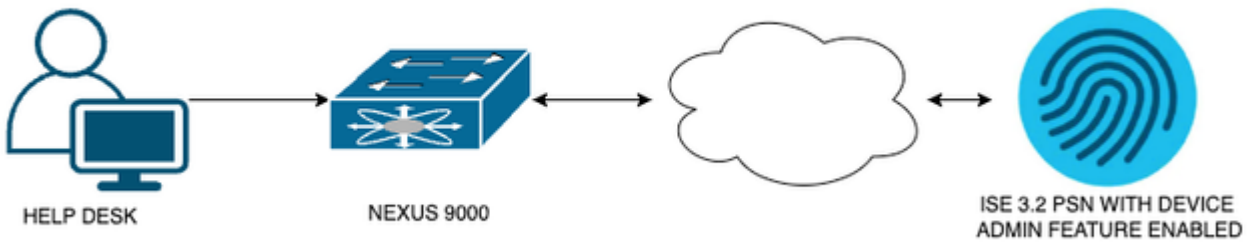
De gebruiker die met deze rol is toegewezen, kan eenvoudige probleemoplossing uitvoeren en bepaalde poorten stuiteren.

De TACACS-sessie die de Nexus-rol krijgt, moet alleen de volgende opdrachten en acties kunnen gebruiken en uitvoeren:

- Toegang tot configureer terminal om ALLEEN shut-down en geen shut-on interfaces uit te voeren van 1/1-1/21 en 1/25-1/30
- ssh
- SSH6
- telnet
- Telnet6
- traceroute
- Traceroute6
- pingelen
- Ping6
- Inschakelen

Configureren

Netwerkdiagram



Stap 1: Nexus 9000 configureren

1. AAA configureren.

Waarschuwing: Nadat u TACACS-verificatie hebt ingeschakeld, stopt het Nexus-apparaat met het gebruik van lokale verificatie en begint het AAA-servergebaseerde verificatie te gebruiken.

```
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. Configureer de aangepaste rol met de opgegeven vereisten.

```
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
```

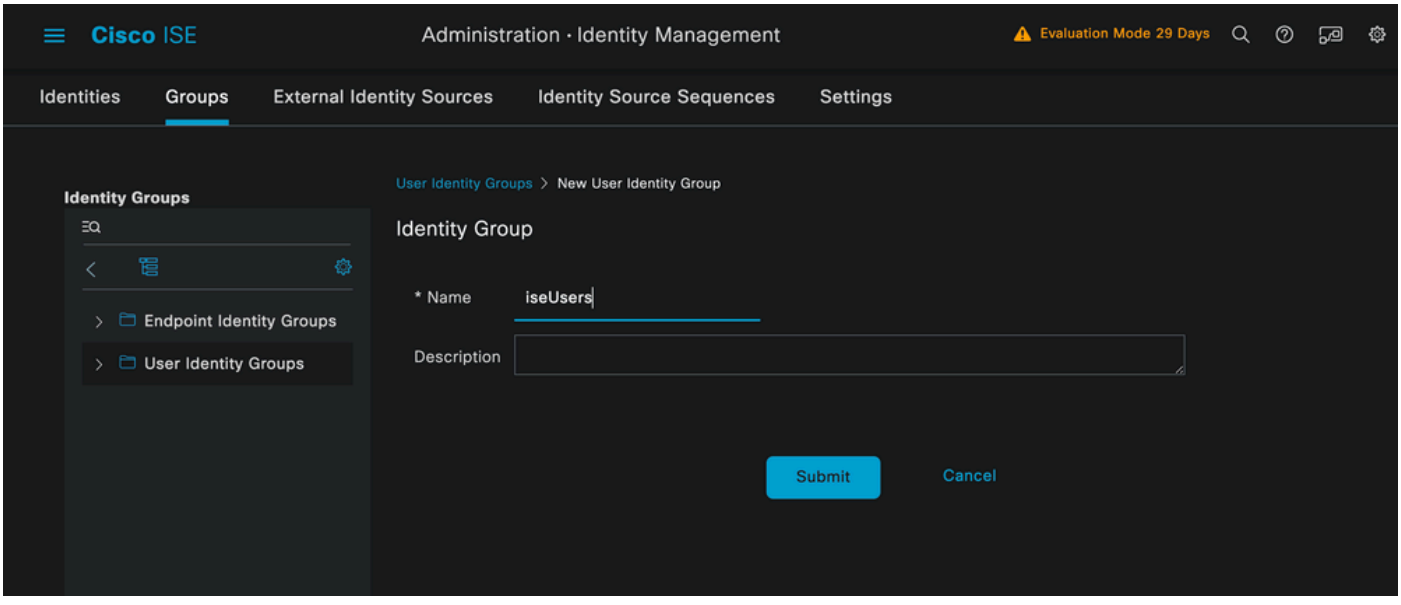
```
Nexus9000(config-role-interface)#     permit interface Ethernet1/11
Nexus9000(config-role-interface)#     permit interface Ethernet1/12
Nexus9000(config-role-interface)#     permit interface Ethernet1/13
Nexus9000(config-role-interface)#     permit interface Ethernet1/14
Nexus9000(config-role-interface)#     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.
```

Stap 2. Identiteitsservicemotor 3.2 configureren

1. Configureer de identiteit die wordt gebruikt tijdens de Nexus TACACS-sessie.

ISE lokale authenticatie wordt gebruikt.

Navigeer naar het tabblad Beheer > Identiteitsbeheer > Groepen en maak de groep aan waarvan de gebruiker deel moet uitmaken. De identiteitsgroep die voor deze demonstratie is gemaakt, is iseUsers.

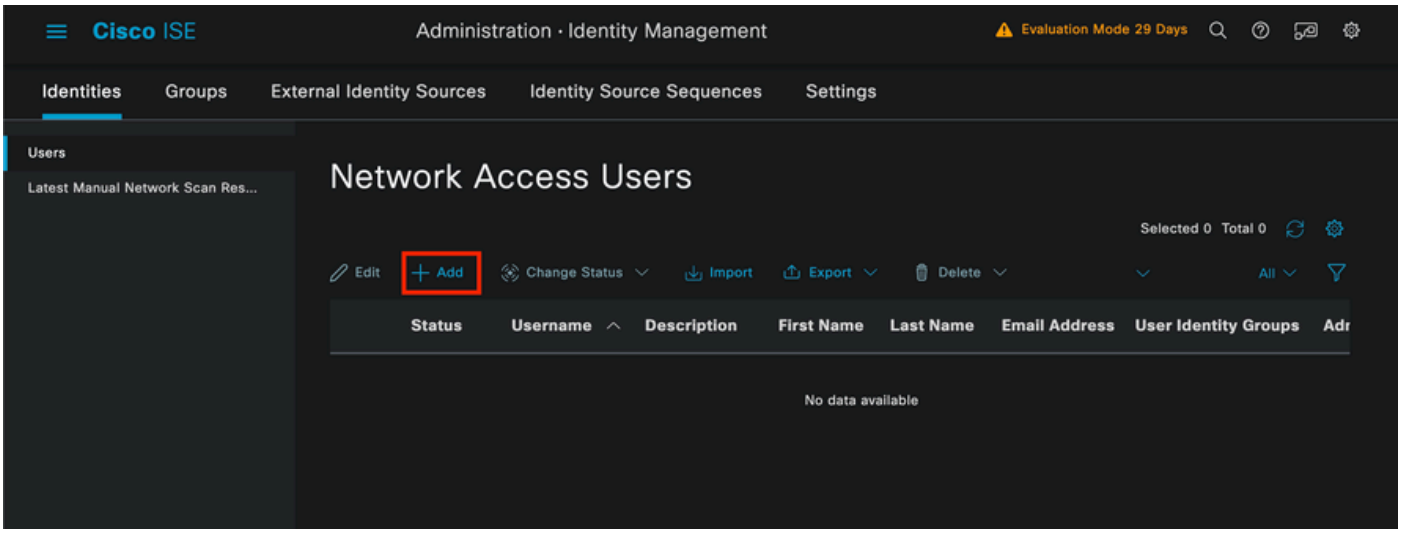


Een gebruikersgroep maken

Klik op de knop Verzenden.

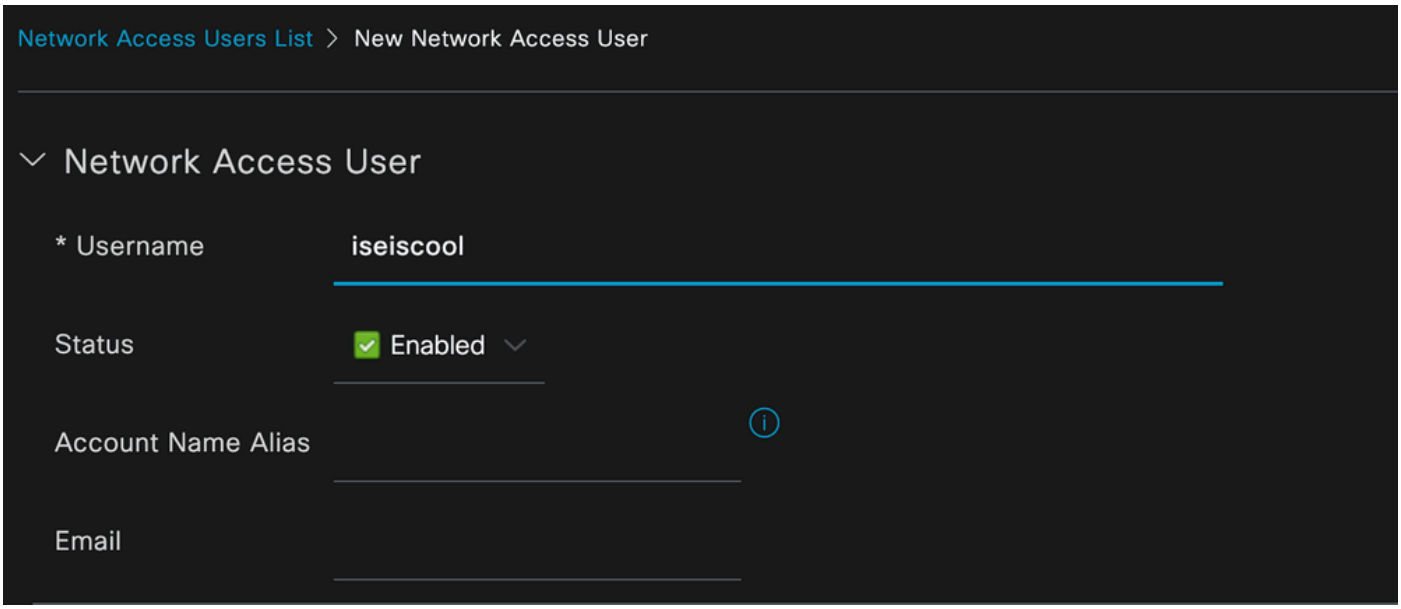
Navigeer vervolgens naar Beheer > Identiteitsbeheer > tabblad Identiteit.

Klik op de knop Toevoegen.



Gebruikerscreatie

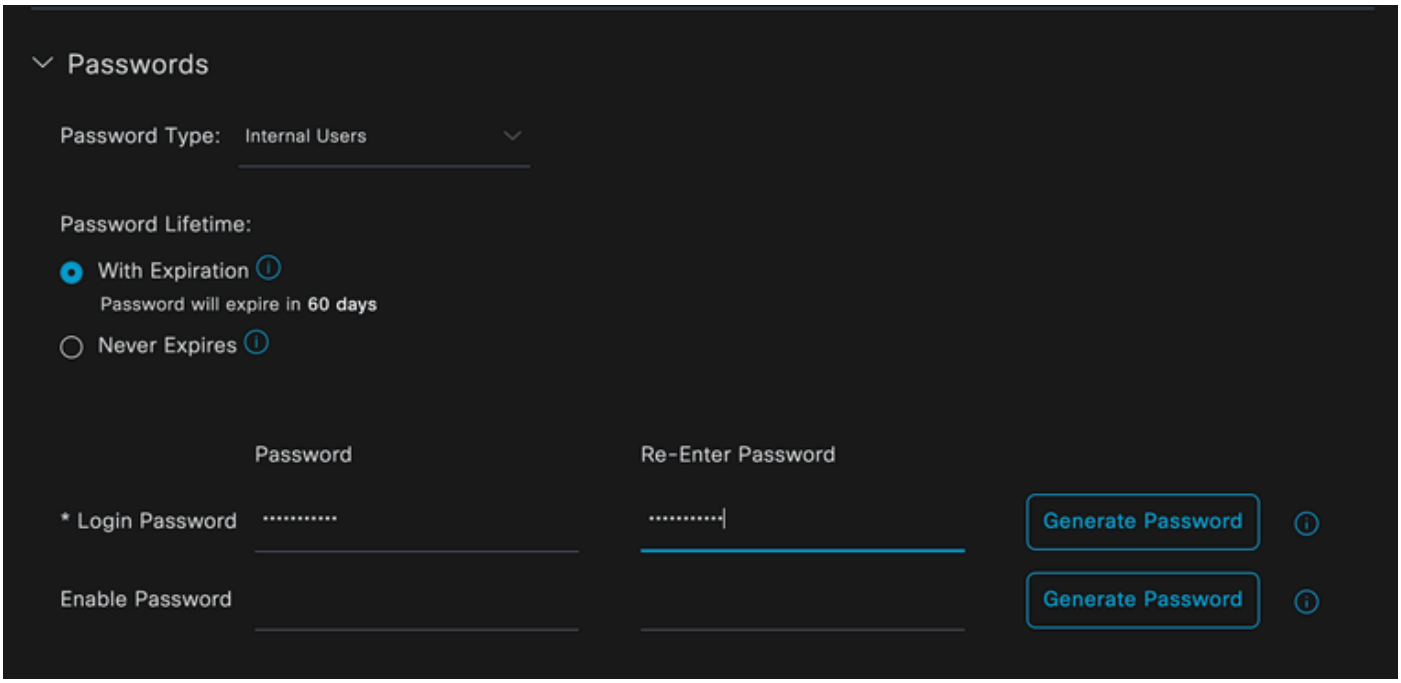
Als onderdeel van de verplichte velden, te beginnen met de naam van de gebruiker, de gebruikersnaam iseiscool wordt gebruikt in dit voorbeeld.



De gebruiker benoemen en aanmaken

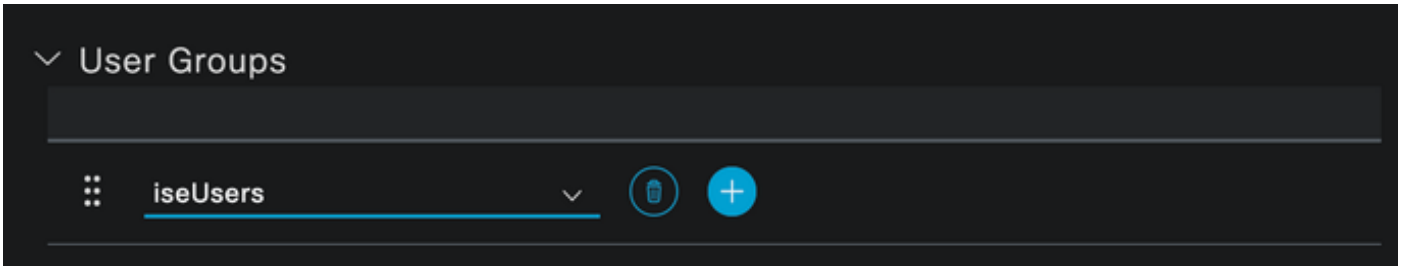
De volgende stap is om een wachtwoord toe te wijzen aan de gemaakte gebruikersnaam.

VanillaISE97 is het wachtwoord dat in deze demonstratie wordt gebruikt.



Wachtwoordtoewijzing

Wijs de gebruiker ten slotte toe aan de eerder gemaakte groep, in dit geval iseUsers.

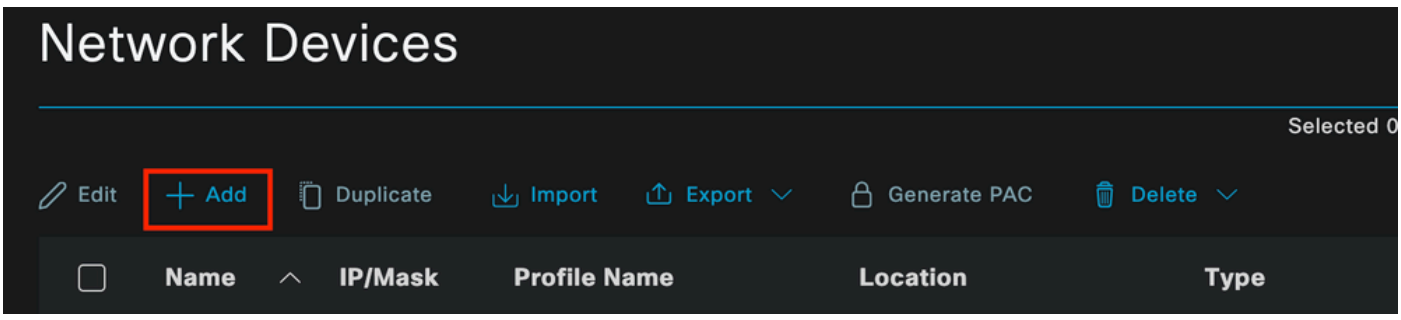


Groepstoewijzing

2. Configureer en voeg het netwerkapparaat toe.

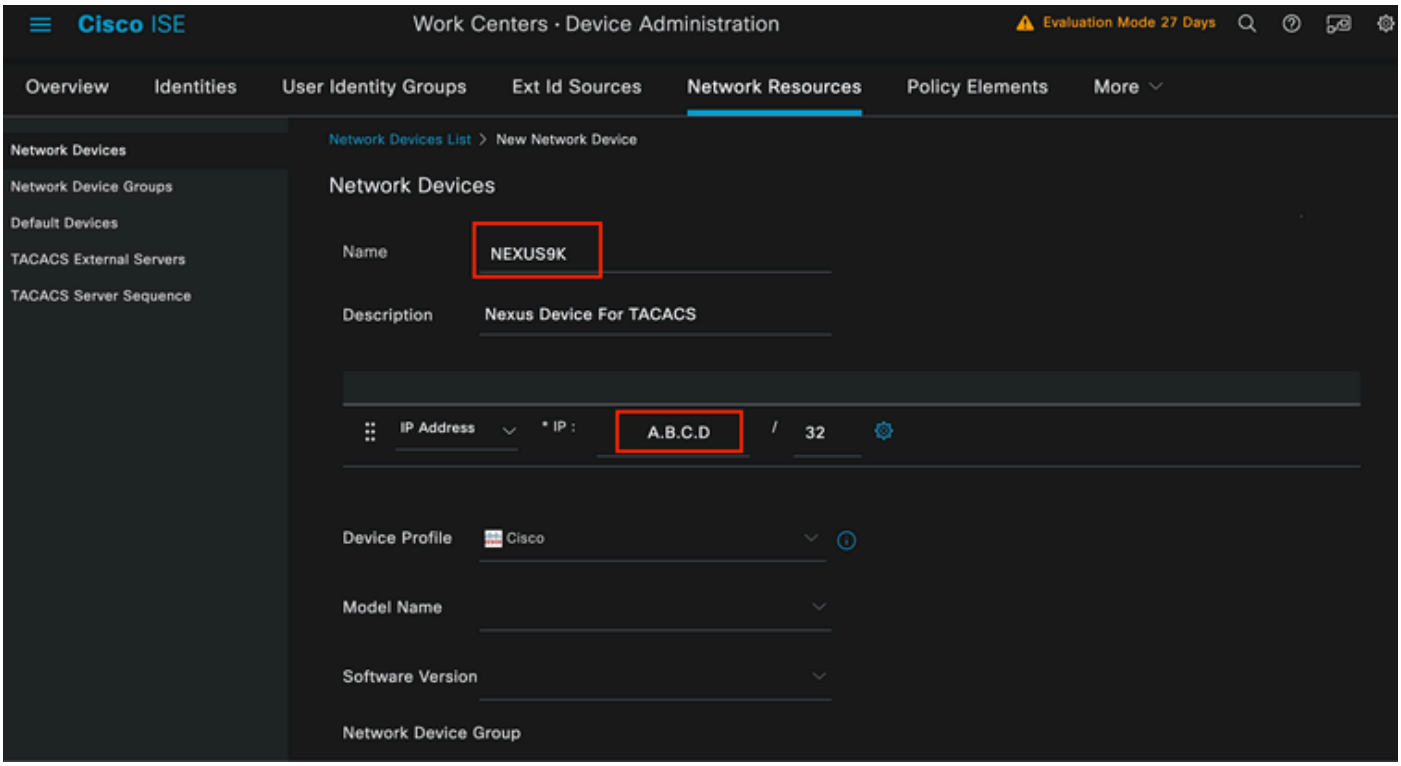
Voeg het NEXUS 9000-apparaat toe aan ISE-beheer > Netwerkbronnen > Netwerkapparaten

Klik op de knop Toevoegen om te starten.



Pagina Netwerktoegangsapparaat

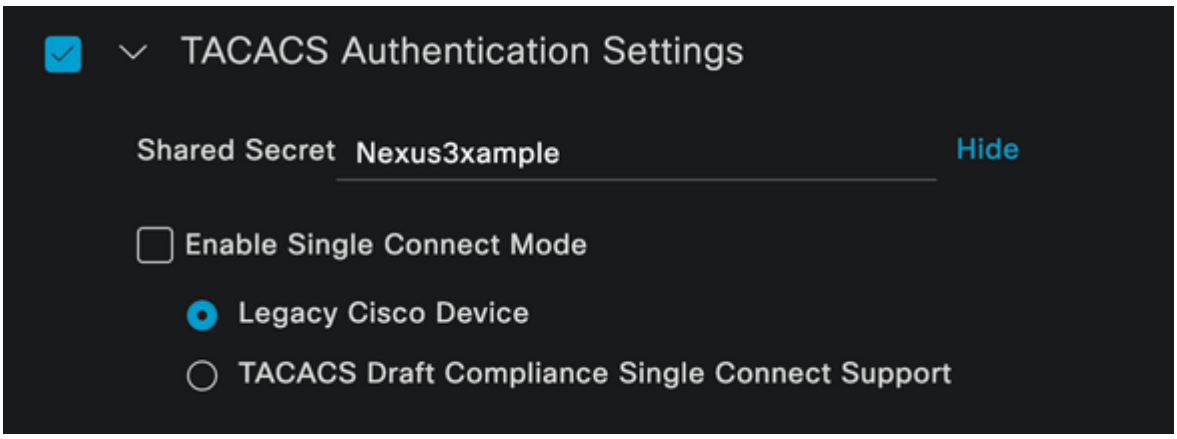
Voer de waarden in het formulier in, wijs een naam toe aan de NAD die u maakt en een IP waaruit de NAD contact opneemt met ISE voor het TACACS-gesprek.



Netwerkapparaat configureren

De vervolgkeuzemogelijkheden kunnen leeg worden gelaten en kunnen worden weggelaten, deze opties zijn bedoeld om uw NAD's te categoriseren op locatie, apparaattype, versie en vervolgens de verificatiestroom op basis van deze filters te wijzigen.

Voeg op Beheer > Netwerkbronnen > Netwerkapparaten > Uw NAD > TACACS-verificatie-instellingen het gedeelde geheim toe dat u hebt gebruikt in uw NAD-configuratie. In deze demonstratie wordt Nexus3xample gebruikt.



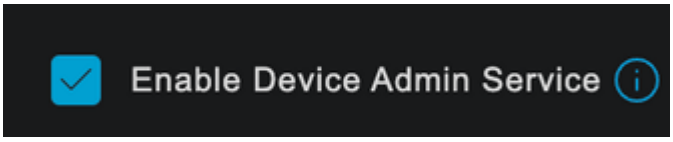
sectie over de TACACS-configuratie

Sla de wijzigingen op door op Verzenden te klikken.

3. TACACS configureren op ISE.

Controleer of de PSN die u in de Nexus 9k hebt geconfigureerd, de optie Apparaatbeheer ingeschakeld heeft.

Opmerking: Apparaatbeheerservice inschakelen veroorzaakt GEEN herstart op ISE.

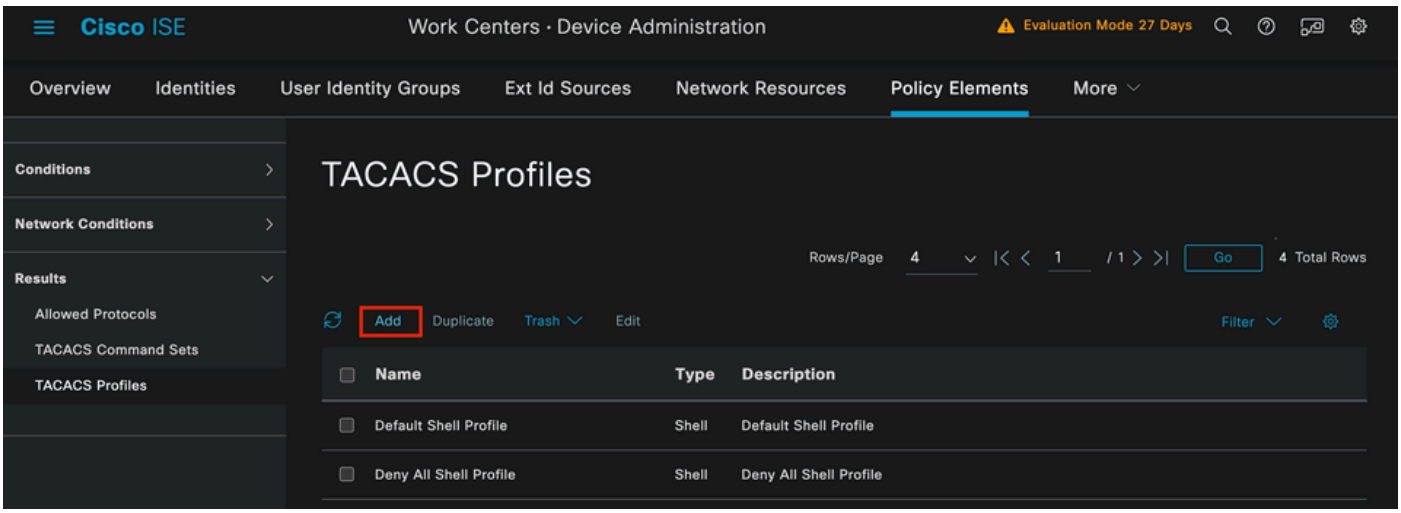


Functie PSN-apparaatbeheer controleren

Dit kan worden gecontroleerd onder ISE-menu Beheer > Systeem > Implementatie > Uw PSN > Sectie Beleidsserver > Apparaatbeheerservices inschakelen.

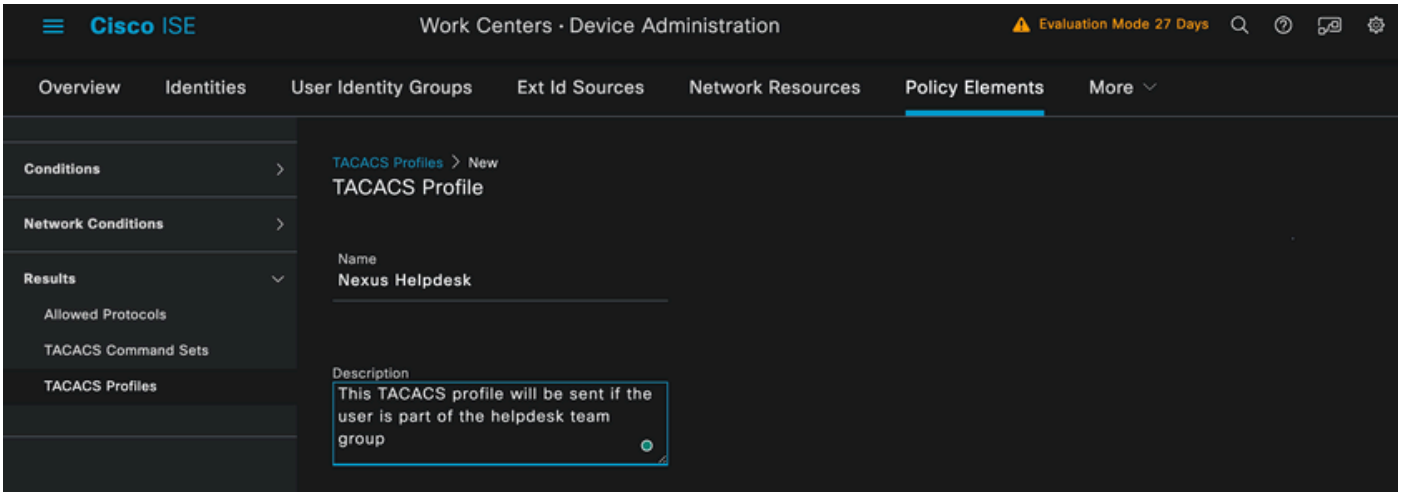
- Maak een TACACS-profiel aan, dat de helpdesk terugstuurt naar het Nexus-apparaat als de verificatie succesvol is.

Navigeer in het menu ISE naar Workcenters > Apparaatbeheer > Beleidselementen > Resultaten > TACACS-profielen en klik op de knop Toevoegen.



TACACS-profiel

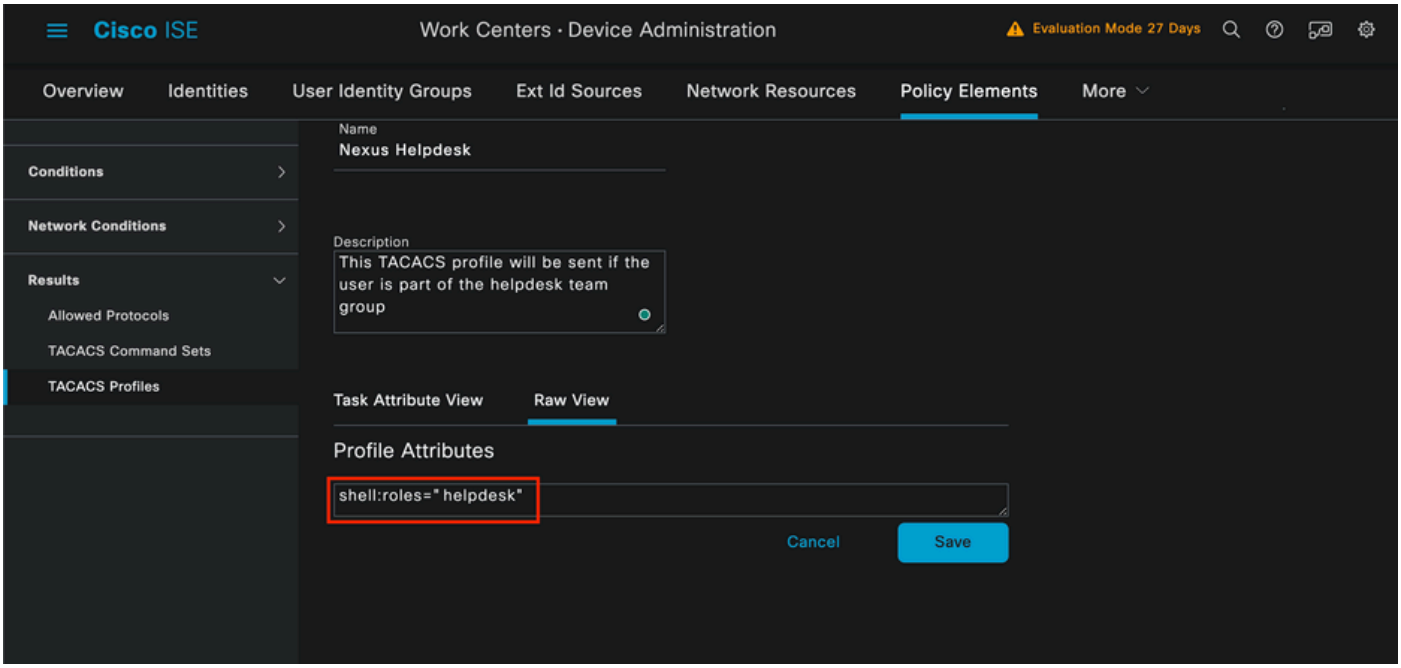
Wijs een naam toe, en optioneel een beschrijving.



Naam Tacacs-profiel

Negeer de sectie Taakkenmerkweergave en navigeer naar de sectie Rauwe weergave.

En voer de value shell in: role="helpdesk".



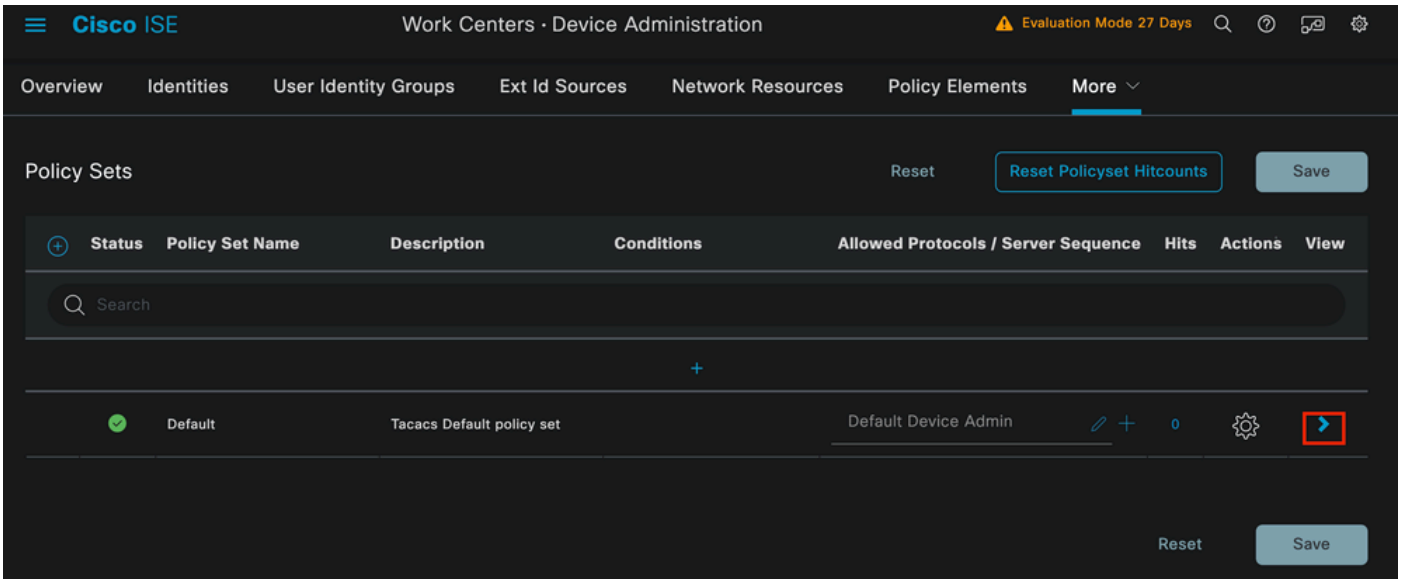
Profielattribuut toevoegen

Configureer de beleidsset die het verificatiebeleid en het autorisatiebeleid bevat.

Ga in het menu ISE naar Work Centers > Apparaatbeheer > Beleidssets apparaatbeheer.

Voor demonstratiedoeleinden wordt de standaardbeleidsset gebruikt. Er kan echter een andere beleidsset worden gemaakt, met voorwaarden die overeenkomen met specifieke scenario's.

Klik op de pijl aan het einde van de rij.

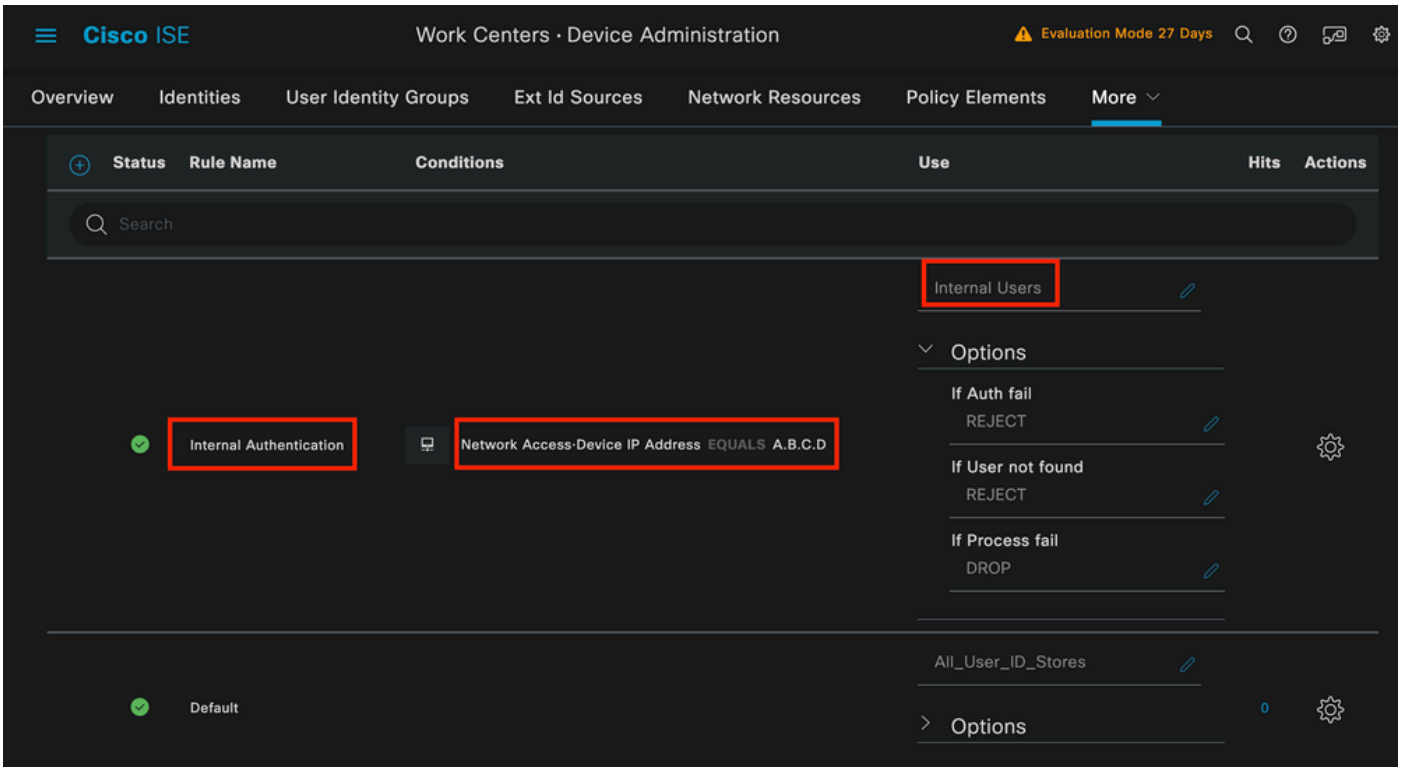


Pagina met beleidssets voor apparaatbeheer

Als u eenmaal in de configuratie van de beleidsinstelling bent, scrolt u naar beneden en vouwt u de sectie Authenticatiebeleid uit.

Klik op het pictogram Toevoegen.

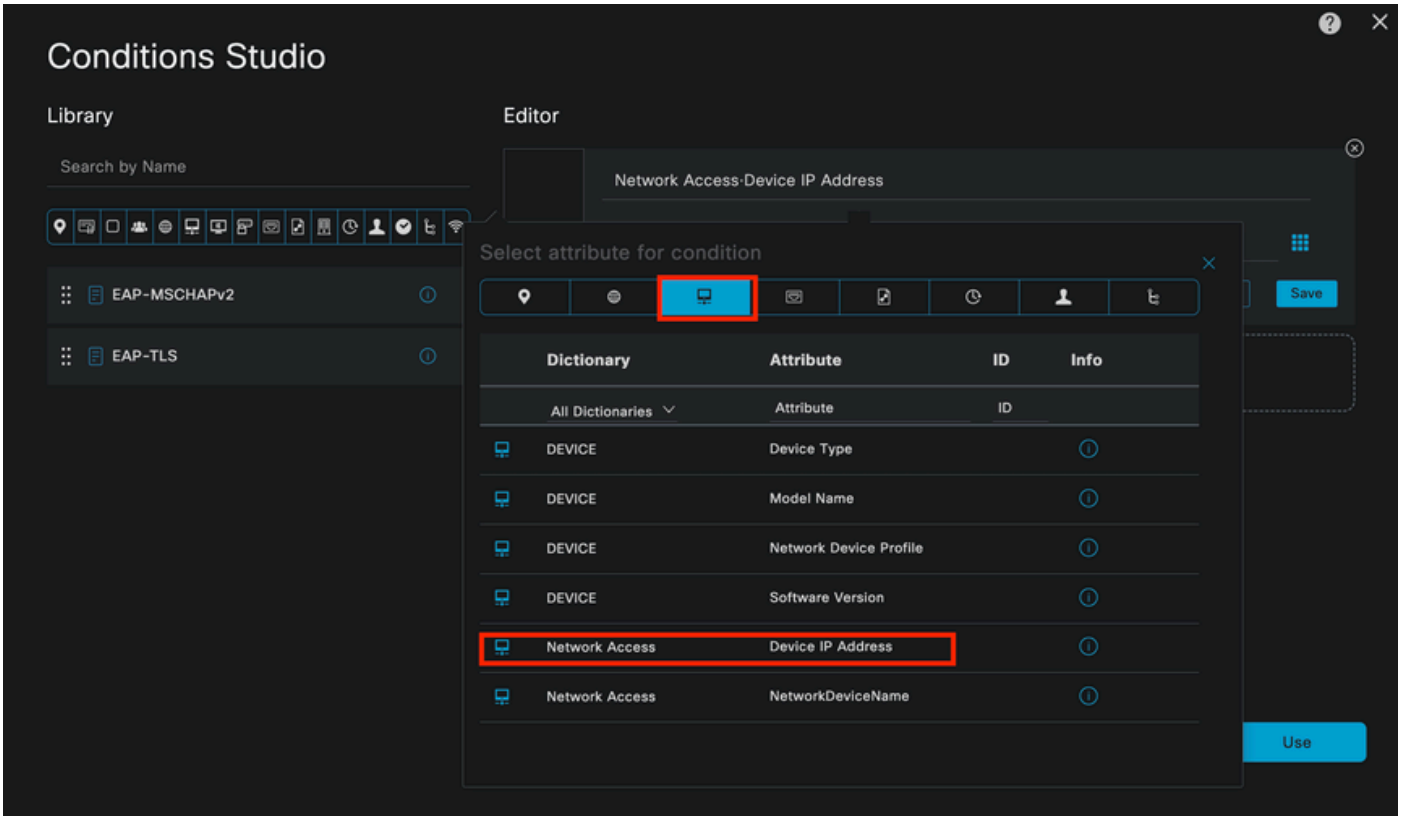
Voor dit configuratievoorbeeld is de waarde Name Internal Authentication en de gekozen voorwaarde is Network Device (Nexus) IP (vervang de A.B.C.D.). Dit verificatiebeleid maakt gebruik van de Internal Users Identity Store.



Authenticatiebeleid

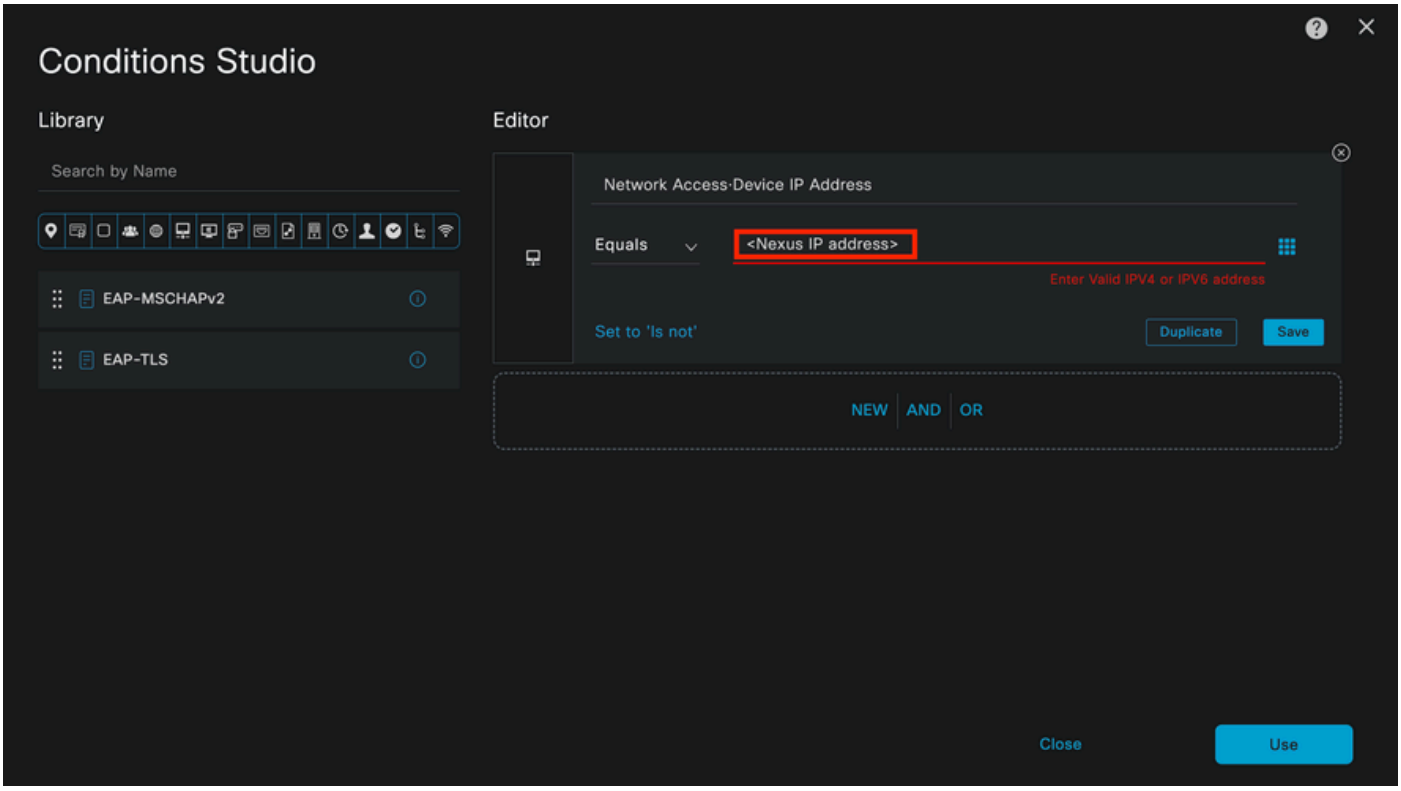
Hier is hoe de conditie werd geconfigureerd.

Selecteer het attribuut Network Access > Device IP Address Dictionary.



Conditie studio voor authenticatiebeleid

Vervang het <Nexus IP-adres> commentaar door het juiste IP-adres.



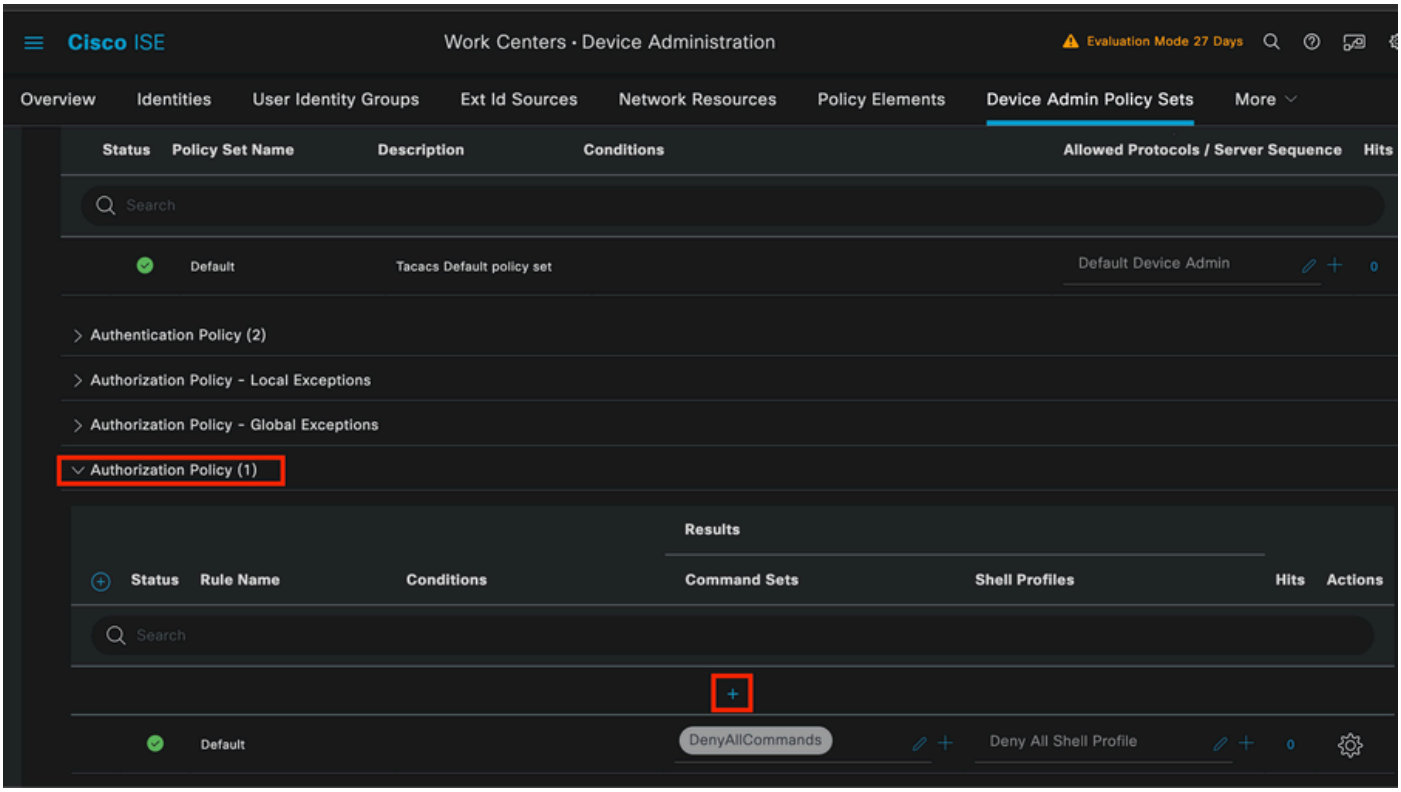
Het IP-filter toevoegen

Klik op de knop Gebruik.

Deze voorwaarde wordt alleen getroffen door het Nexus-apparaat dat u hebt geconfigureerd. Als het doel echter is om deze voorwaarde voor een grote hoeveelheid apparaten mogelijk te maken, overweeg dan een andere voorwaarde.

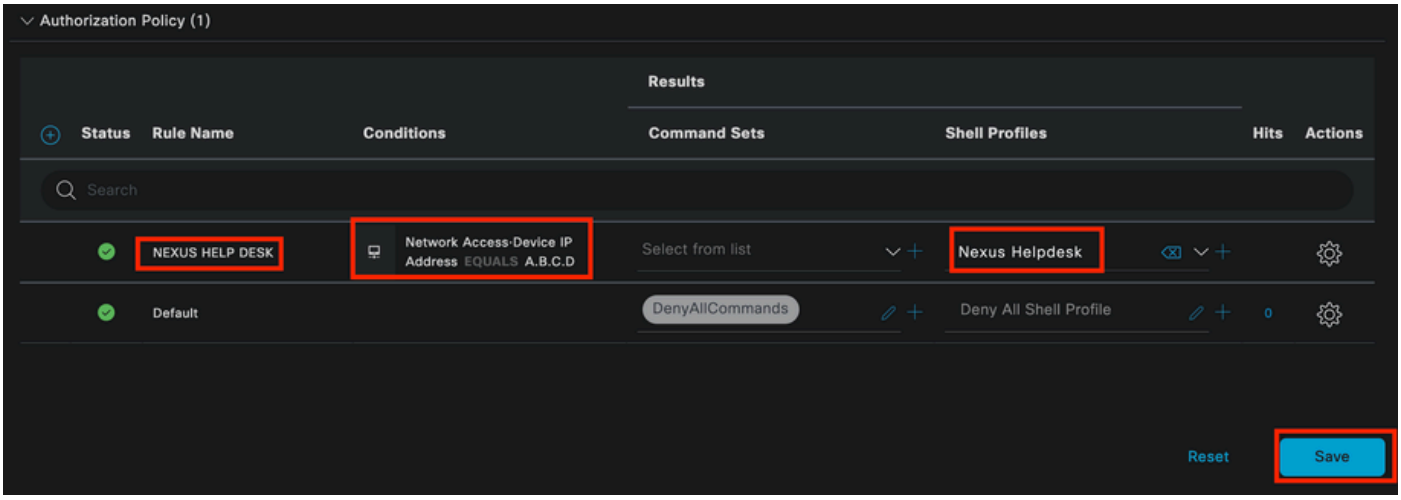
Navigeer vervolgens naar de sectie Autorisatiebeleid en vouw deze uit.

Klik op het + (plus) icoontje.



Sectie Autorisatiebeleid

In dit voorbeeld werd NEXUS HELP DESK als naam van het Autorisatiebeleid gebruikt.



Conditie studio voor autorisatiebeleid

Dezelfde voorwaarde die in het verificatiebeleid is geconfigureerd, wordt gebruikt voor het autorisatiebeleid.

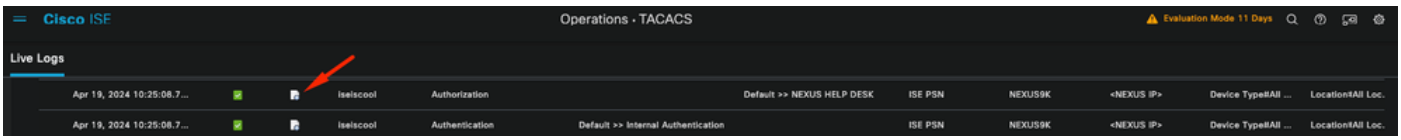
In de kolom Shell-profielen werd het profiel geconfigureerd voordat Nexus Helpdesk werd geselecteerd.

Klik ten slotte op de knop Opslaan.

Verifiëren

Gebruik deze sectie om te controleren of uw configuratie goed werkt.

Navigeer vanuit de ISE GUI naar Operations > TACACS > Live Logs. Identificeer de record die overeenkomt met de gebruikte gebruikersnaam en klik op de Live Log Details van de autorisatie-gebeurtenis.



TACACS Live Log

Als onderdeel van de details die dit rapport bevat, is het te vinden in een sectie Response, waar u kunt zien hoe ISE de value shell heeft geretourneerd: role="helpdesk"

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

Live log Detail Response

Op het Nexus-apparaat:

```
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)#
```

Problemen oplossen

- Controleer of ISE bereikbaar is vanaf het Nexus-apparaat:

```
Nexus9000# ping <Uw ISE IP>
PING <Uw ISE IP> (<Uw ISE IP> ﷺ 56 gegevensbytes
64 bytes van <Uw ISE IP>: icmp_seq=0 ttl=59 time=1,22 ms
64 bytes van <Uw ISE IP>: icmp_seq=1 ttl=59 time=0,739 ms
64 bytes van <Uw ISE IP>: icmp_seq=2 ttl=59 time=0,686 ms
64 bytes van <Uw ISE IP>: icmp_seq=3 ttl=59 time=0,71 ms
64 bytes van <Uw ISE IP>: icmp_seq=4 ttl=59 time=0,72 ms
```

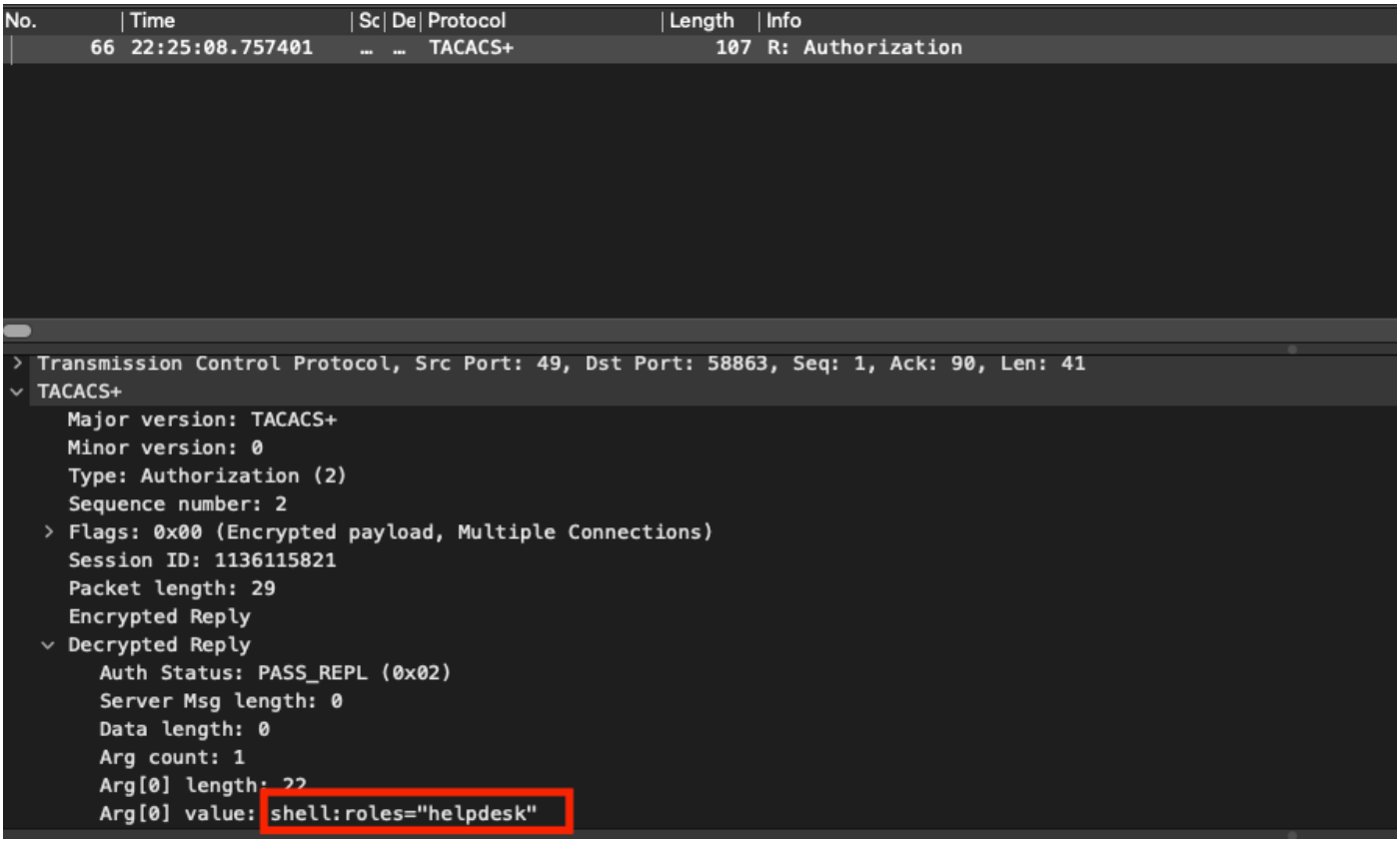
- Controleer of poort 49 is geopend tussen ISE en het Nexus-apparaat:
  Nexus9000# telnet <Uw ISE IP> 49
  <Uw ISE IP> wordt geprobeerd...
  Verbonden met <Uw ISE IP>.
  Escape-teken is '^]'.
- Gebruik deze debugs:

Foutopsporing TACACS+ ALL
Nexus9000#
Nexus9000# 2024 Apr 19 22:50:44.199329 tacacs: event_loop(): aanroepingsproces_rd_fd_set
2024 apr 19 22:50:44.199355 tacacs: process_rd_fd_set: call back voor fd 6
2024 apr 19 22:50:44.199392 tacacs: fsrv didnt Consumpt 8421 opcode
2024 apr 19 22:50:44.199406 tacacs: process_implicit_cfs_session_start: invoeren...
2024 Apr 19 22:50:44.199414 tacacs: process_implicit_cfs_session_start: afsluiten; we zijn in distributie uitgeschakeld
2024 Apr 19 22:50:44.199424 tacacs: process_aaa_tplus_request: invoeren voor aaa sessie-id 0

2024 Apr 19 22:50:44.199438 tacacs: process_aaa_tplus_request: Controleren op status van mgmt0 poort met servergroep IsePsnServers
2024 apr 19 22:50:44.199451 tacacs: tacacs_global_config(4220): invoeren ...
2024 apr 19 22:50:44.199466 tacacs: tacacs_global_config(4577): GET_REQ...
2024 Apr 19 22:50:44.208027 tacacs: tacacs_global_config(4701): kreeg de retourwaarde van de wereldwijde protocolconfiguratie terug: succes
2024 apr 19 22:50:44.208045 tacacs: tacacs_global_config(4716): REQ:num server 0
2024 apr 19 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 apr 19 22:50:44.208070 tacacs: tacacs_global_config: REQ:num deadtime 0
2024 apr 19 22:50:44.208078 tacacs: tacacs_global_config: REQ:num encryption_type 7
2024 apr 19 22:50:44.208086 tacacs: tacacs_global_config: return retval 0
2024 Apr 19 22:50:44.208098 tacacs: process_aaa_tplus_request:group_info is ingevuld in aaa_req, dus Het gebruik van servergroep IsePsnServers
2024 apr 19 22:50:44.208108 tacacs: tacacs_servergroup_config: invoeren voor servergroep, index 0
2024 apr 19 22:50:44.208117 tacacs: tacacs_servergroup_config: GETNEXT_REQ voor Protocol server group index: 0 naam:
2024 apr 19 22:50:44.208148 tacacs: tacacs_pss2_move2key: rcode = 40480003 syserr2str = geen dergelijke PSS-sleutel
2024 apr 19 22:50:44.208160 tacacs: tacacs_pss2_move2key: bellen naar pss2_getKey
2024 Apr 19 22:50:44.208171 tacacs: tacacs_servergroup_config: GETNEXT_REQ kreeg Protocol server group index:2 naam: IsePsnServers
2024 Apr 19 22:50:44.208184 tacacs: tacacs_servergroup_config: de retourwaarde van de protocolgroepsbewerking teruggekregen: SUCCES
2024 Apr 19 22:50:44.208194 tacacs: tacacs_servergroup_config: retour 0 voor protocolservergroep: IsePsnServers
2024 Apr 19 22:50:44.208210 tacacs: process_aaa_tplus_request: Group IsePsnServers gevonden. corresponderende vrf is standaard, source-intf is 0
2024 apr 19 22:50:44.208224 tacacs: process_aaa_tplus_request: controleren op mgmt0 vrf: beheer tegen vrf: default van aangevraagde groep
2024 apr 19 22:50:44.208256 tacacs: process_aaa_tplus_request:mgmt_if 83886080
2024 apr 19 22:50:44.208272 tacacs: process_aaa_tplus_request: global_src_intf: 0, local src_intf is 0 en vrf_name is standaard
2024 Apr 19 22:50:44.208286 tacacs: create_tplus_req_state_machine(902): invoeren voor aaa sessie-id 0
2024 apr 19 22:50:44.208295 tacacs: staat machine telling 0
2024 apr 19 22:50:44.208307 tacacs: init_tplus_req_state_machine: invoeren voor aaa sessie-id 0
2024 Apr 19 22:50:44.208317 tacacs: init_tplus_req_state_machine(1298):tplus_ctx is NULL het zou moeten zijn als auteur en test
2024 apr 19 22:50:44.208327 tacacs: tacacs_servergroup_config: invoeren voor servergroepIsePsnServers, index 0
2024 Apr 19 22:50:44.208339 tacacs: tacacs_servergroup_config: GET_REQ voor Protocol server group index: 0 naam: IsePsnServers
2024 Apr 19 22:50:44.208357 tacacs: find_tacacs_servergroup: invoeren voor servergroep IsePsnServers

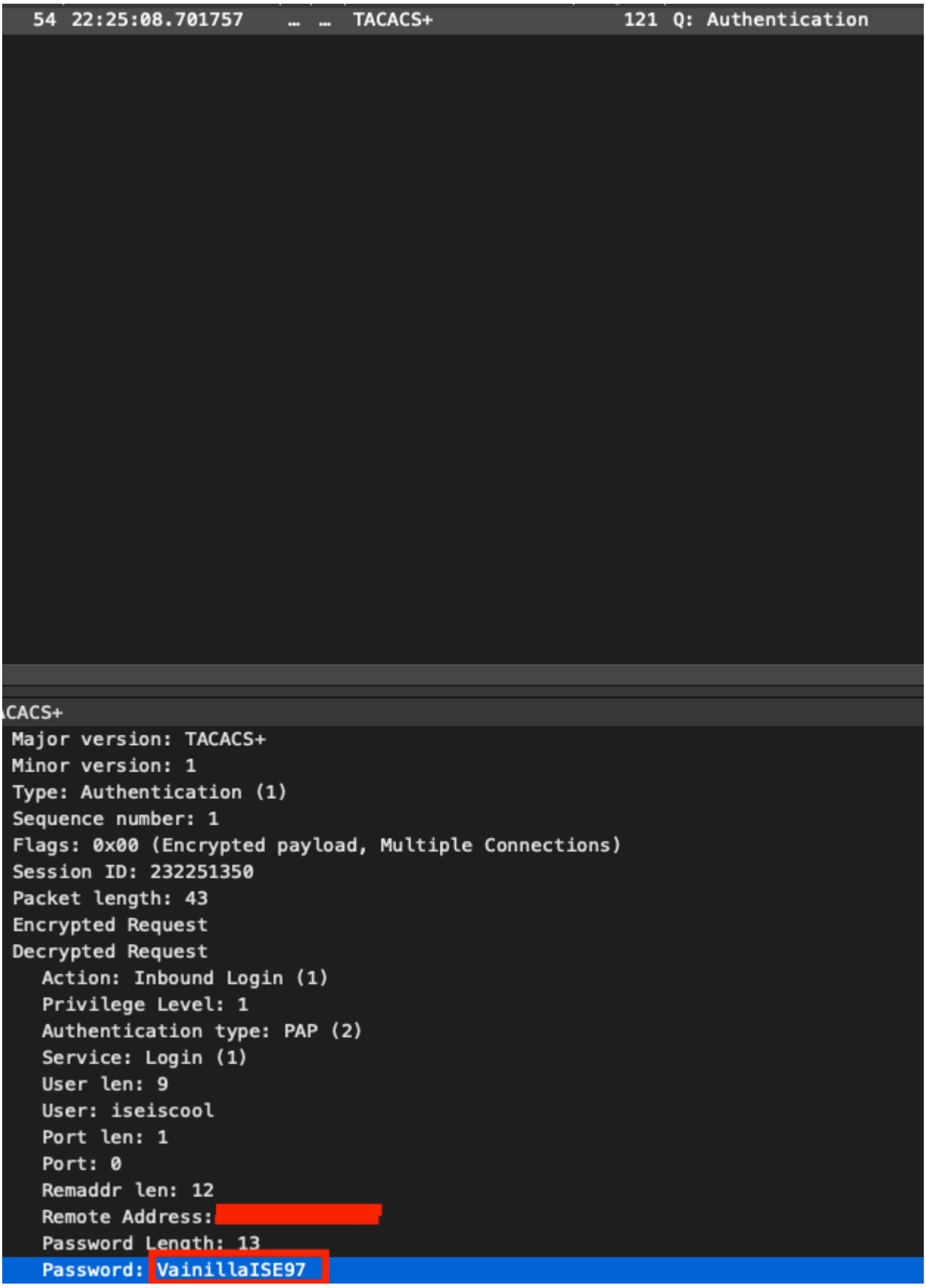
2024 apr 19 22:50:44.208372 tacacs: tacacs_pss2_move2key: rcode = 0 syserr2str = SUCCES
2024 Apr 19 22:50:44.208382 tacacs: find_tacacs_servergroup: afsluiten voor servergroep IsePsnServers index is 2
2024 Apr 19 22:50:44.208401 tacacs: tacacs_servergroup_config: GET_REQ: find_tacacs_servergroup error 0 voor Protocol server groep IsePsnServers
2024 apr 19 22:50:44.208420 tacacs: tacacs_pss2_move2key: rcode = 0 syserr2str = SUCCES
2024 Apr 19 22:50:44.208433 tacacs: tacacs_servergroup_config: GET_REQ got Protocol server group index:2 naam: IsePsnServers
2024 A2024 apr 19 22:52024 apr 19 22:52024 apr 19 22:5
Nexus9000#

- Voer een pakketopname uit. (Om de pakketgegevens te bekijken, moet u WireShark TACACS+-voorkeuren wijzigen en de gedeelde sleutel bijwerken die wordt gebruikt door de Nexus en ISE.)



TACACS-autorisatiepakket

- Controleer of de gedeelde sleutel hetzelfde is aan de ISE- en Nexus-kant. Dit kan ook worden gecontroleerd in Wireshark.



verificatiepakket

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.