Configureer aangepaste TACACS-rol voor Nexus 9K met ISE 3.2

Inhoud

Inleiding

Dit document beschrijft hoe u een aangepaste Nexus rol kunt configureren voor TACACS via CLI op NK9.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- TACACS +
- ISE-lijnkaart 3.2

Gebruikte componenten

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

- Cisco Nexus 9000, 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

Licentie-eisen:

Cisco NX-OS - TACACS+ vereist geen licentie.

Cisco Identity Service Engine - voor nieuwe ISE-installaties hebt u een licentie voor een evaluatieperiode van 90 dagen die toegang heeft tot alle ISE-functies, als u geen evaluatielicentie hebt, om de ISE TACACS-functie te kunnen gebruiken, hebt u een Device Admin-licentie nodig voor het knooppunt Policy Server dat de verificatie uitvoert.

Nadat de gebruikers van de Admin/Help-desk op het Nexus-apparaat authenticeren, retourneert ISE de gewenste Nexus-shell-rol.

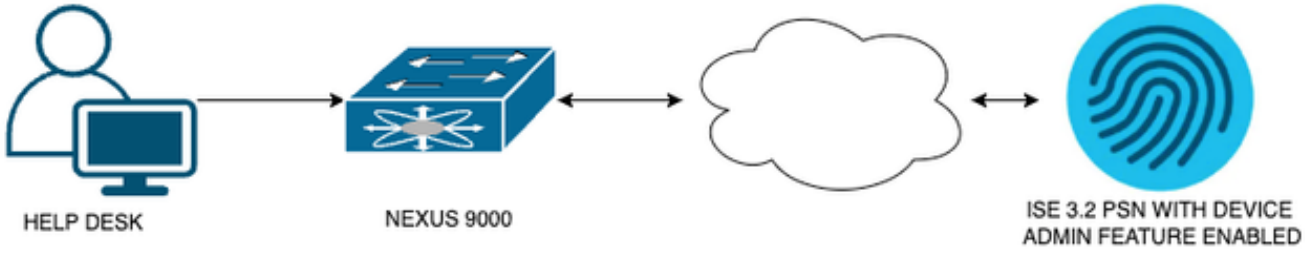
De gebruiker die met deze rol wordt toegewezen kan het basisoplossen van problemen uitvoeren en bepaalde poorten weerkaatsen.

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

- Toegang om terminal te configureren om alleen uitschakeling en geen uitschakelinterfaces vanaf 1/1-1/21 en 1/25-1/30 uit te voeren
- ssh
- sh6
- telnet
- Telnet6
- Traceroute
- Traceroute6
- Ping
- Ping6
- Inschakelen

Configureren

Netwerkdiagram



Stap 1: Nexus 9000 configureren

1. AAA-configuratie.

Waarschuwing: nadat u de TACACS-verificatie hebt ingeschakeld, stopt het Nexus-apparaat met de lokale verificatie en start het met de AAA-servergebaseerde verificatie.

```
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.

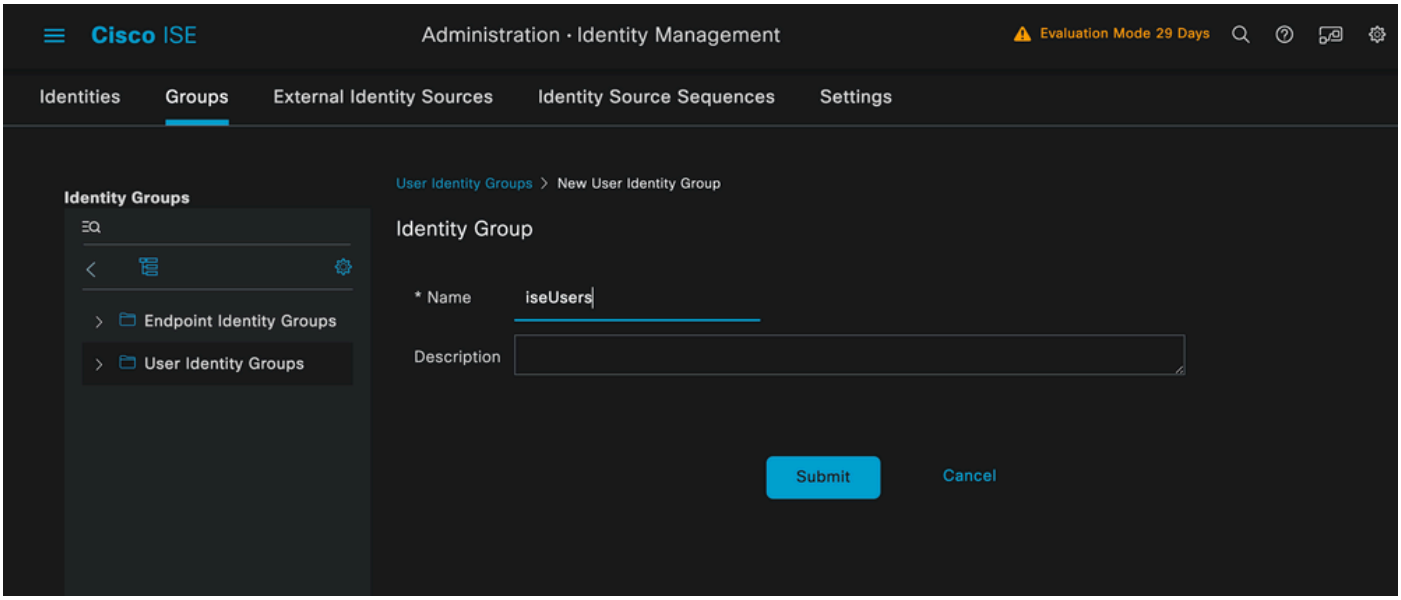
```
Nexus9000(config)# role name helpdesk
Nexus9000(config-role)#   description Can perform basic Toubleshooting and bounce certain  ports
Nexus9000(config-role)# rule 1 permit read
Nexus9000(config-role)# rule 2 permit command enable *
Nexus9000(config-role)# rule 3 permit command ssh *
Nexus9000(config-role)# 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. Identity Service Engine 3.2 configureren

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

Lokale verificatie met ISE wordt gebruikt.

Navigeer naar het tabblad Administratie > Identity Management > Groepen en creëer de groep waar de gebruiker deel van moet uitmaken. De identiteitsgroep die voor deze demonstratie is gemaakt, is ISEGebruikers.

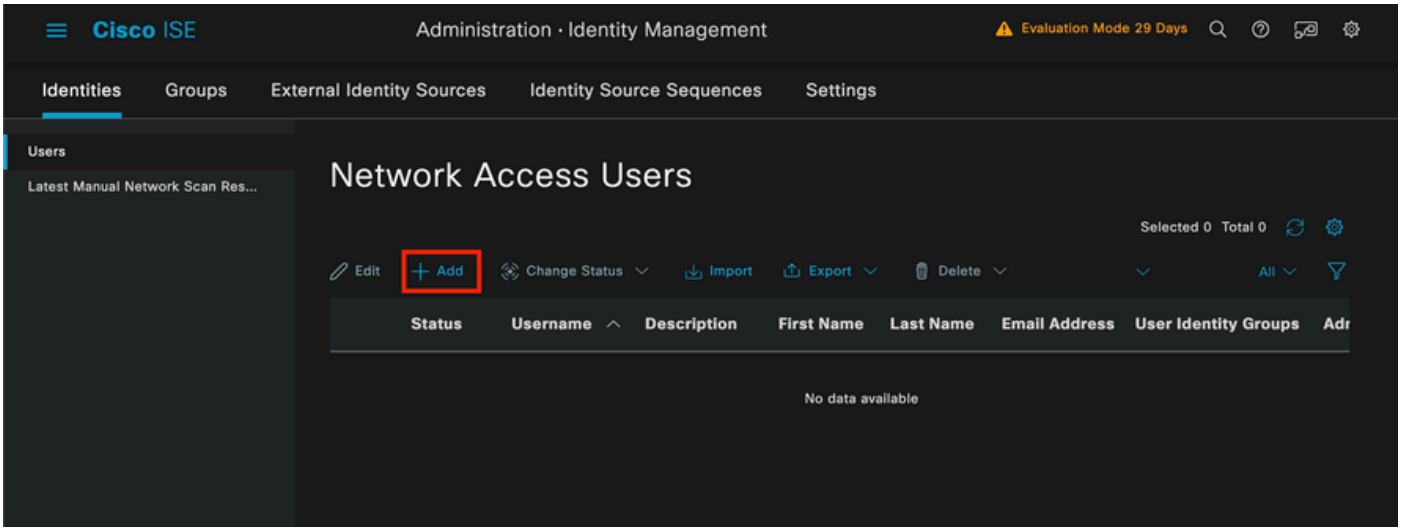


Een gebruikersgroep maken

Klik op de knop Verzenden.

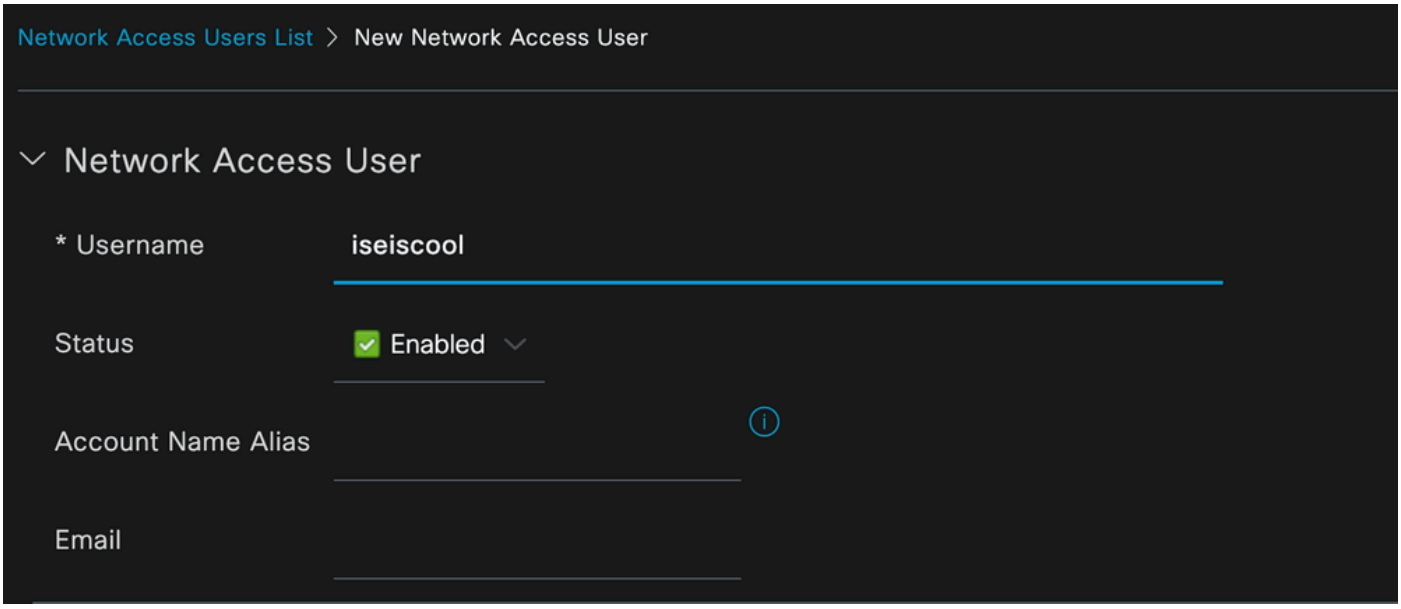
Navigeer vervolgens naar Beheer > Identity Management > Identity tab.

Druk op de knop Toevoegen.



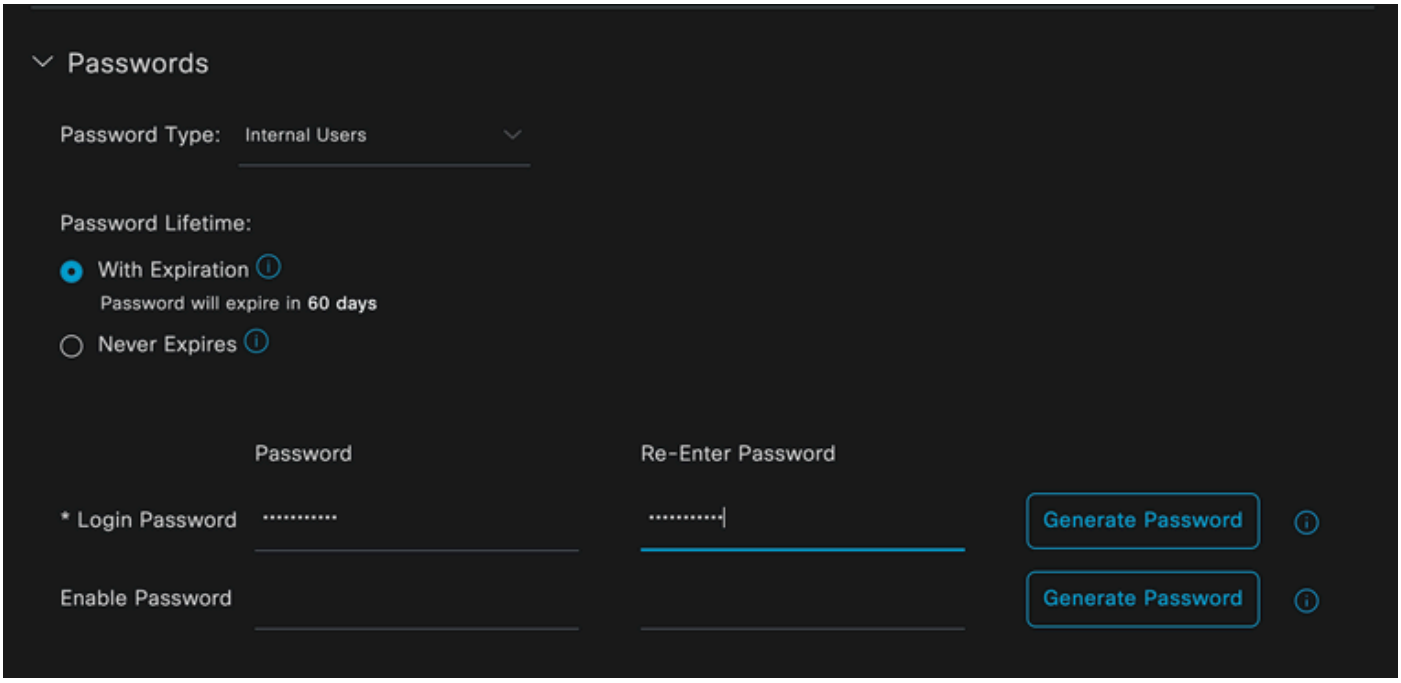
Aanmaken gebruiker

Als deel van de verplichte velden, begin met de naam van de gebruiker, de gebruikersnaam isisiscole wordt gebruikt in dit voorbeeld.



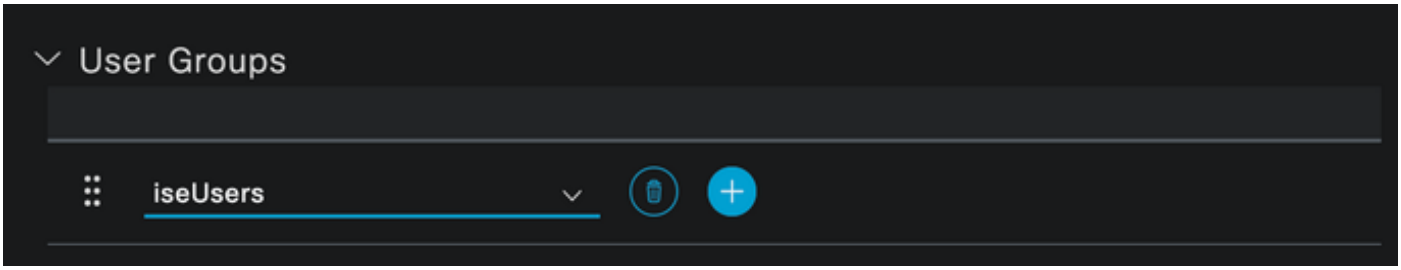
De gebruiker een naam geven en deze maken

De volgende stap is om een wachtwoord toe te wijzen aan de gebruikersnaam die is gemaakt, VainillaISE97 is het wachtwoord dat in deze demonstratie wordt gebruikt.



Wachtwoordtoewijzing

Ten slotte, wijs de gebruiker toe aan de groep die eerder is gemaakt, in dit geval iseGebruikers.

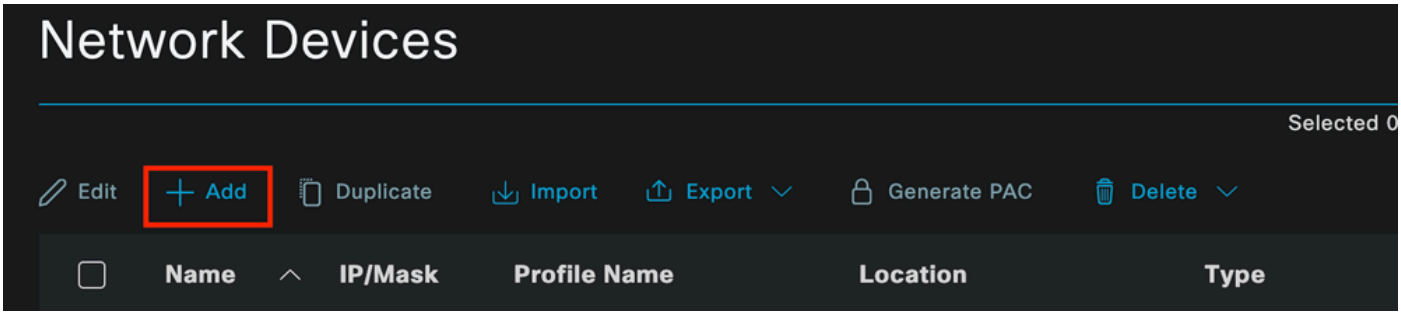


Groepstoewijzing

2. Het netwerkapparaat configureren en toevoegen.

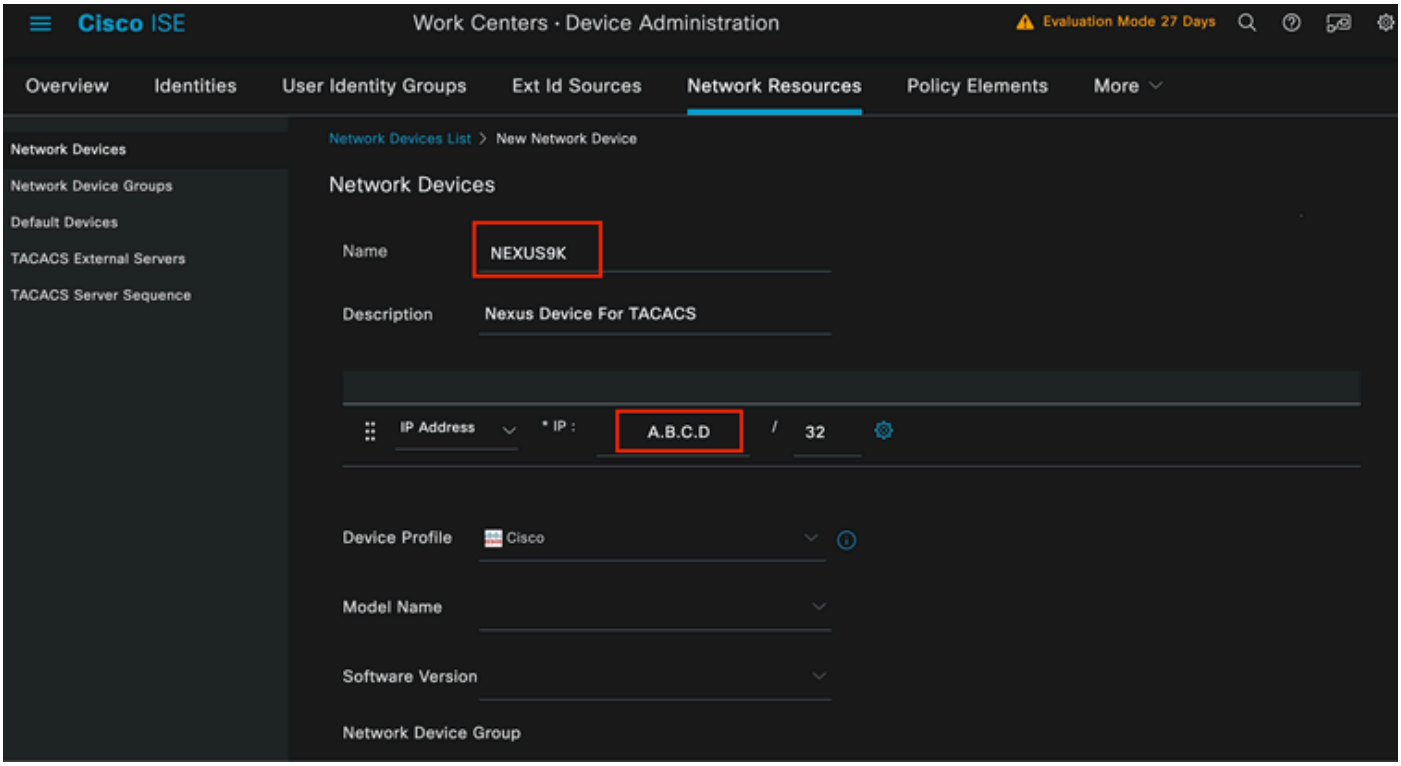
Voeg het NEXUS 9000-apparaat toe aan ISE-beheer > Netwerkbronnen > Netwerkapparaten

Klik op de knop Toevoegen om te beginnen.



Apparaatpagina voor netwerktoegang

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

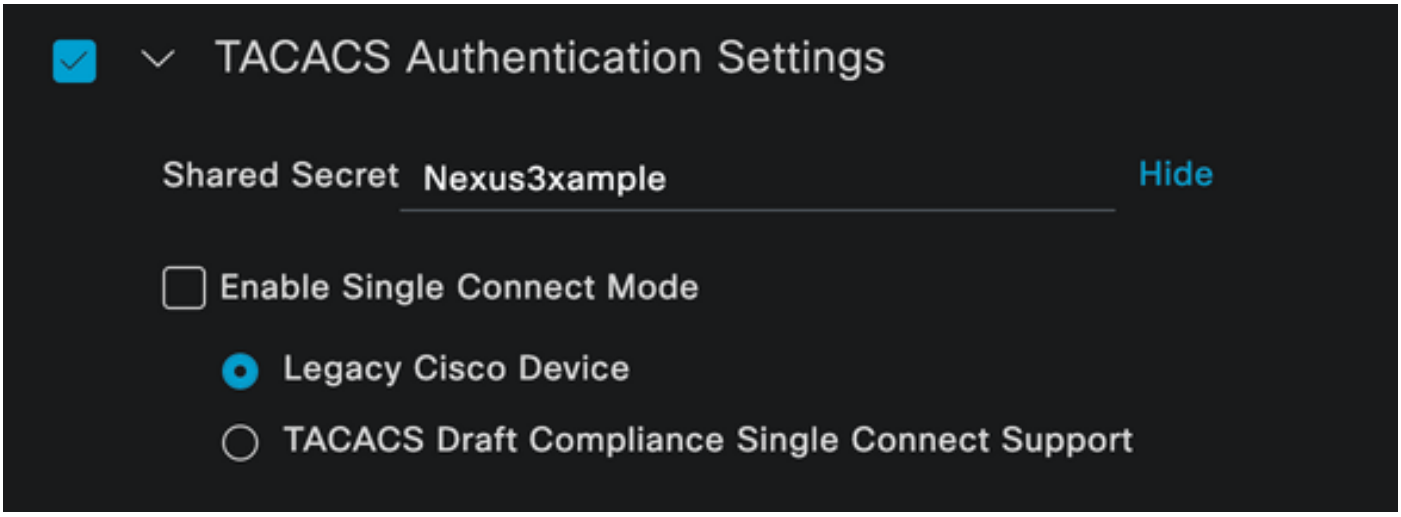


Netwerkapparaat configureren

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.

Selecteer in het menu Beheer > Netwerkbronnen > Netwerkapparaten > Uw en > Instellingen voor TACACS-verificatie.

Voeg het gedeelde geheim toe dat u onder uw NAD-configuratie voor deze demonstratie hebt gebruikt, Nexus3xample wordt in deze demonstratie gebruikt.

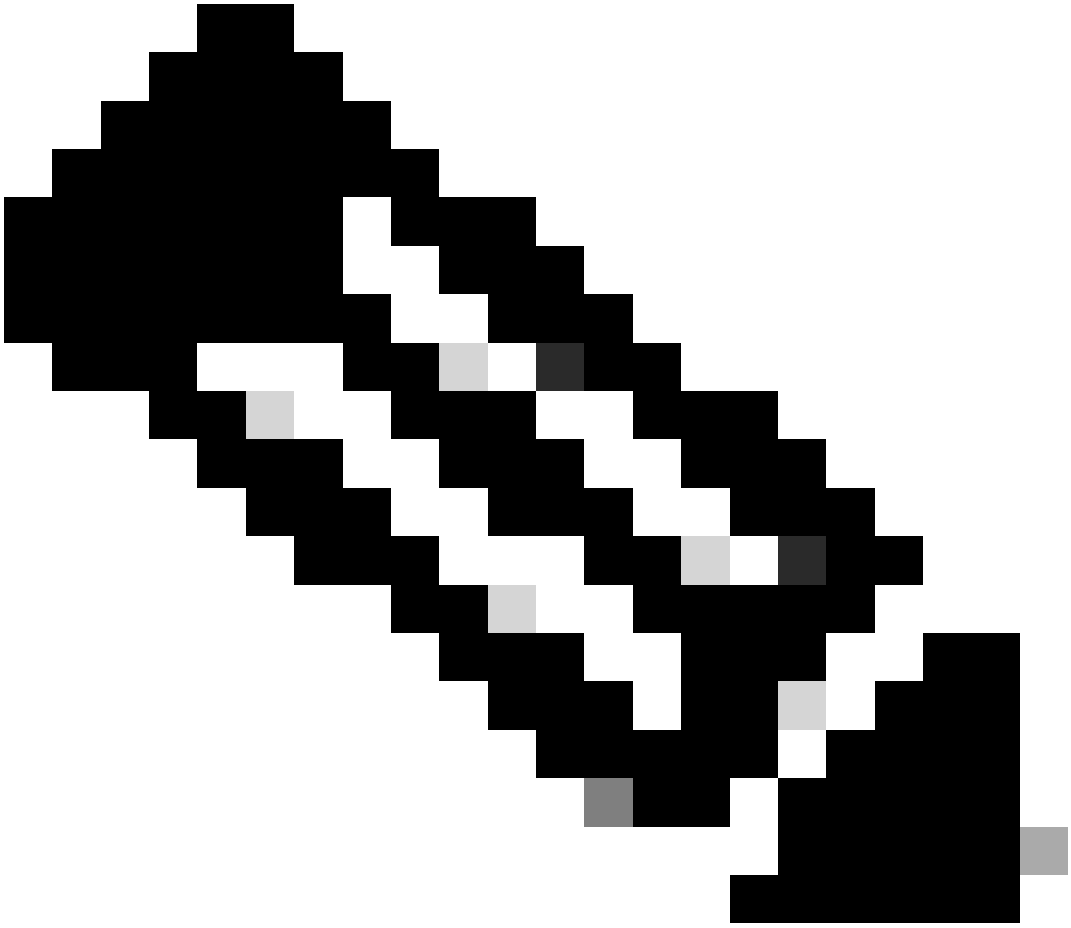


Sectie TACACS-configuratie

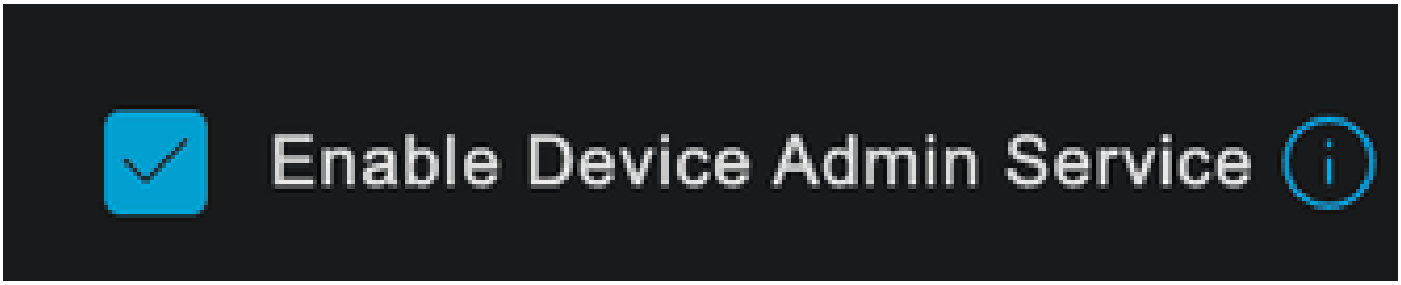
Sla de wijzigingen op door op de knop Verzenden te klikken.

3. TACACS-configuratie op ISE.

Dubbelcontroleer dat de PSN die u in de Nexus 9k hebt geconfigureerd, de optie Device Admin ingeschakeld heeft.



Opmerking: de Service Apparaatbeheer inschakelen veroorzaakt GEEN opnieuw opstarten van ISE.

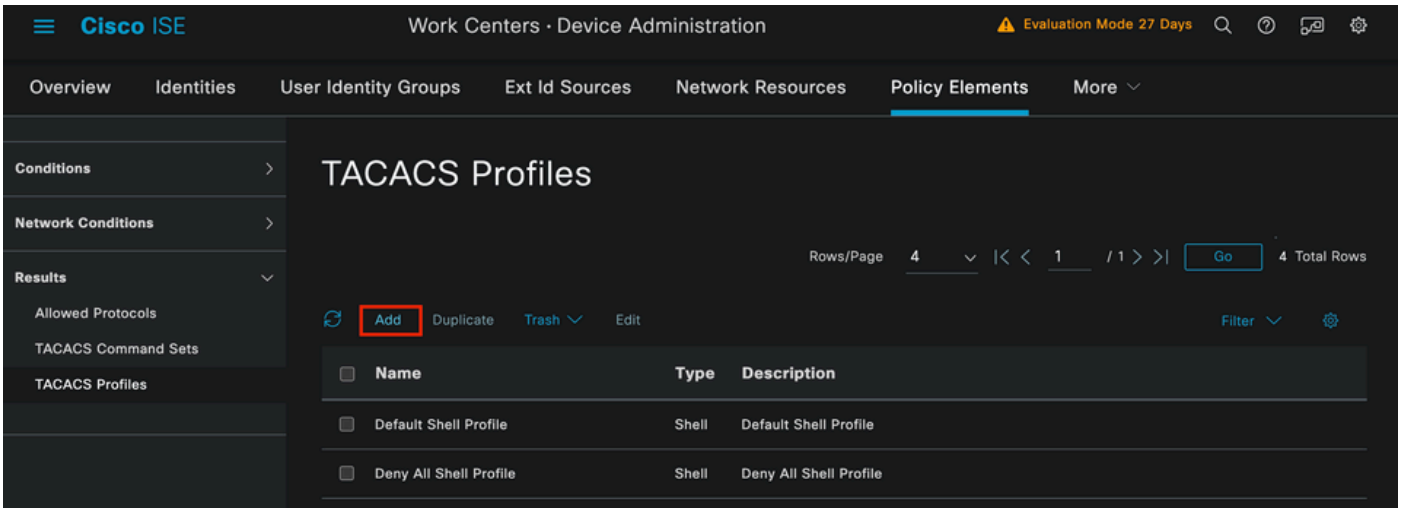


Functiecontrole PSN-apparaatbeheer

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

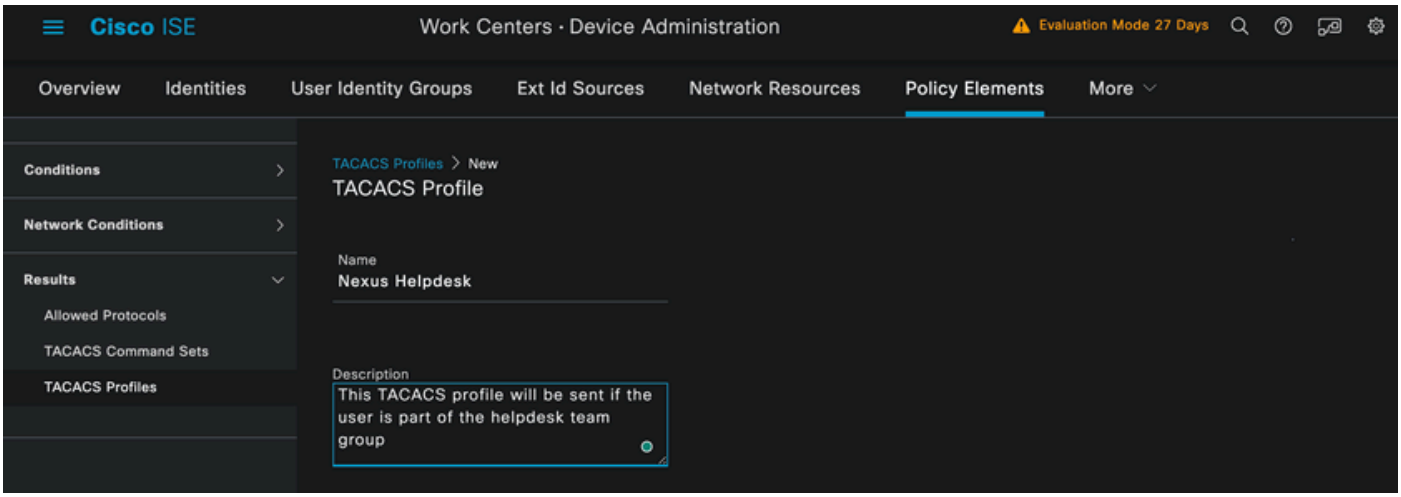
- Maak een TACACS-profiel, dat de rol helpdesk terugbrengt naar het Nexus-apparaat als de verificatie succesvol is.

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



TACACS-profiel

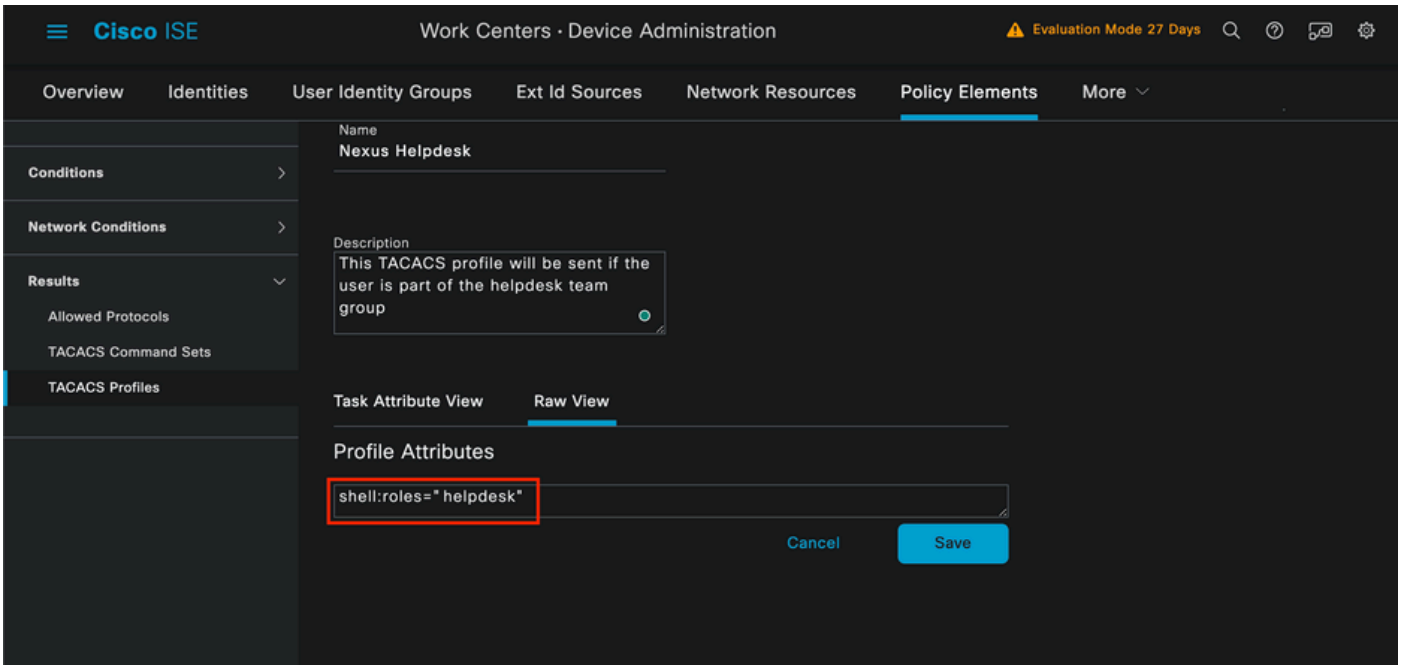
Wijs een Naam, en naar keuze een beschrijving toe.



Tacacs-profiel benoemen

Negeer het gedeelte Taakkenmerken bekijken en navigeer naar het gedeelte Raw View.

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



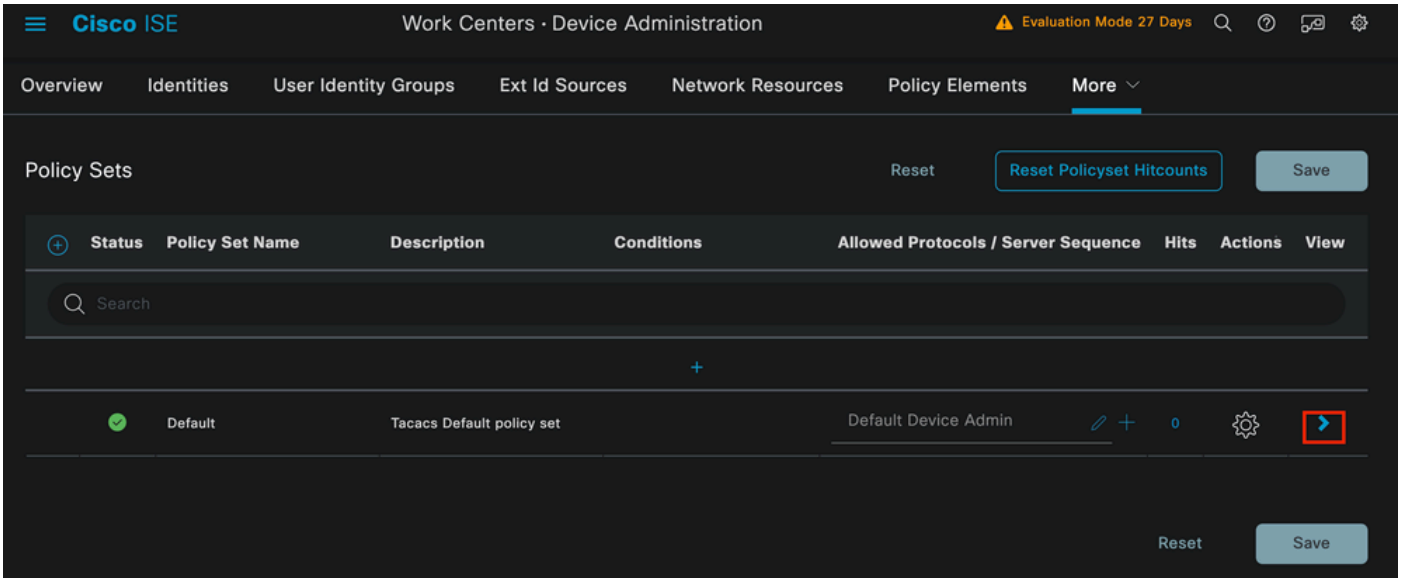
Profielkenmerk toevoegen

Configureer de beleidsset die het verificatiebeleid en het autorisatiebeleid bevat.

In het ISE-menu Werkcentra > Apparaatbeheer > Beleidssets voor Apparaatbeheer.

Voor demonstratiedoeleinden wordt de reeks Default Policy gebruikt. Er kan echter een andere beleidsset worden gemaakt, met voorwaarden om specifieke scenario's aan te passen.

Klik op de pijl aan het einde van de rij.

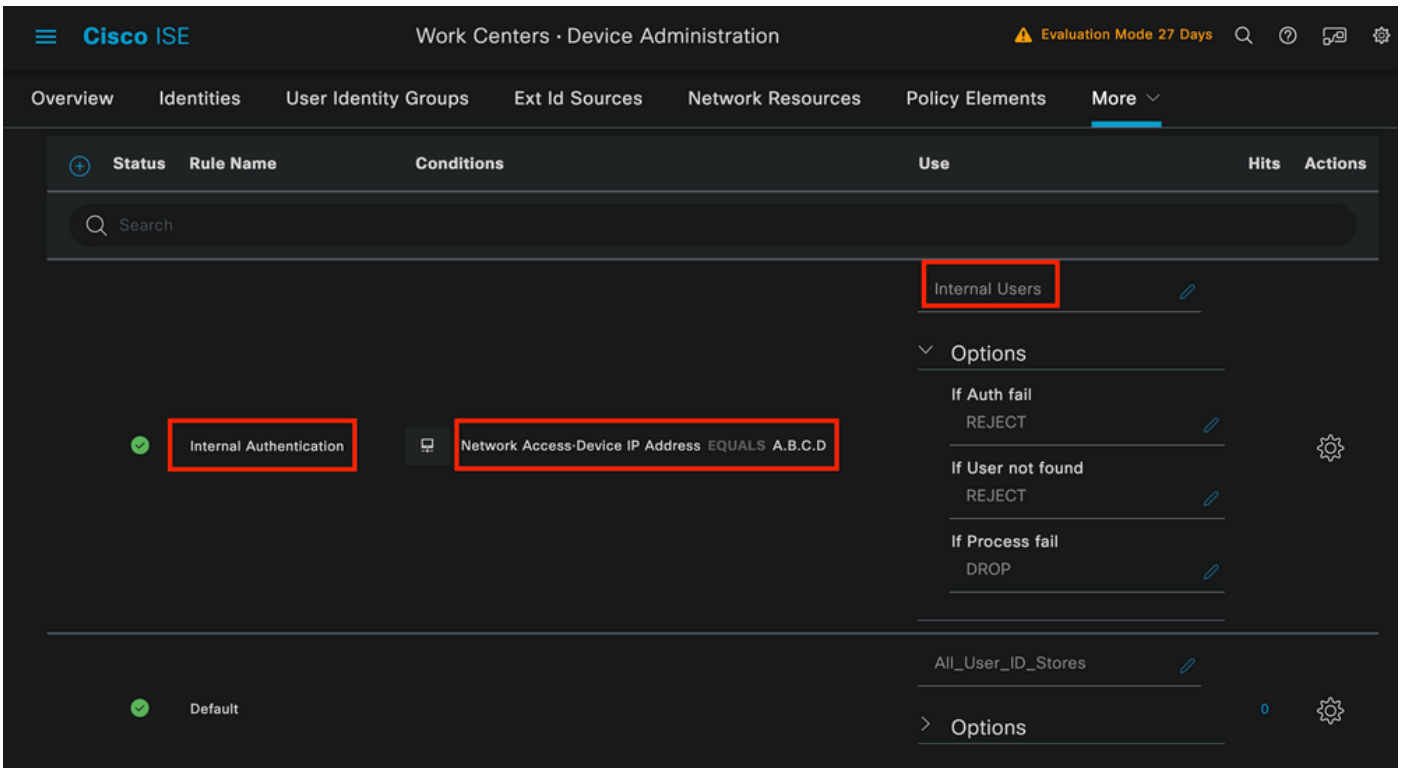


Pagina met beleidssets voor apparaatbeheer

Eens binnen de beleid vastgestelde configuratie scrolt naar beneden en breid de sectie van het Beleid van de Verificatie uit.

Klik op het pictogram Toevoegen.

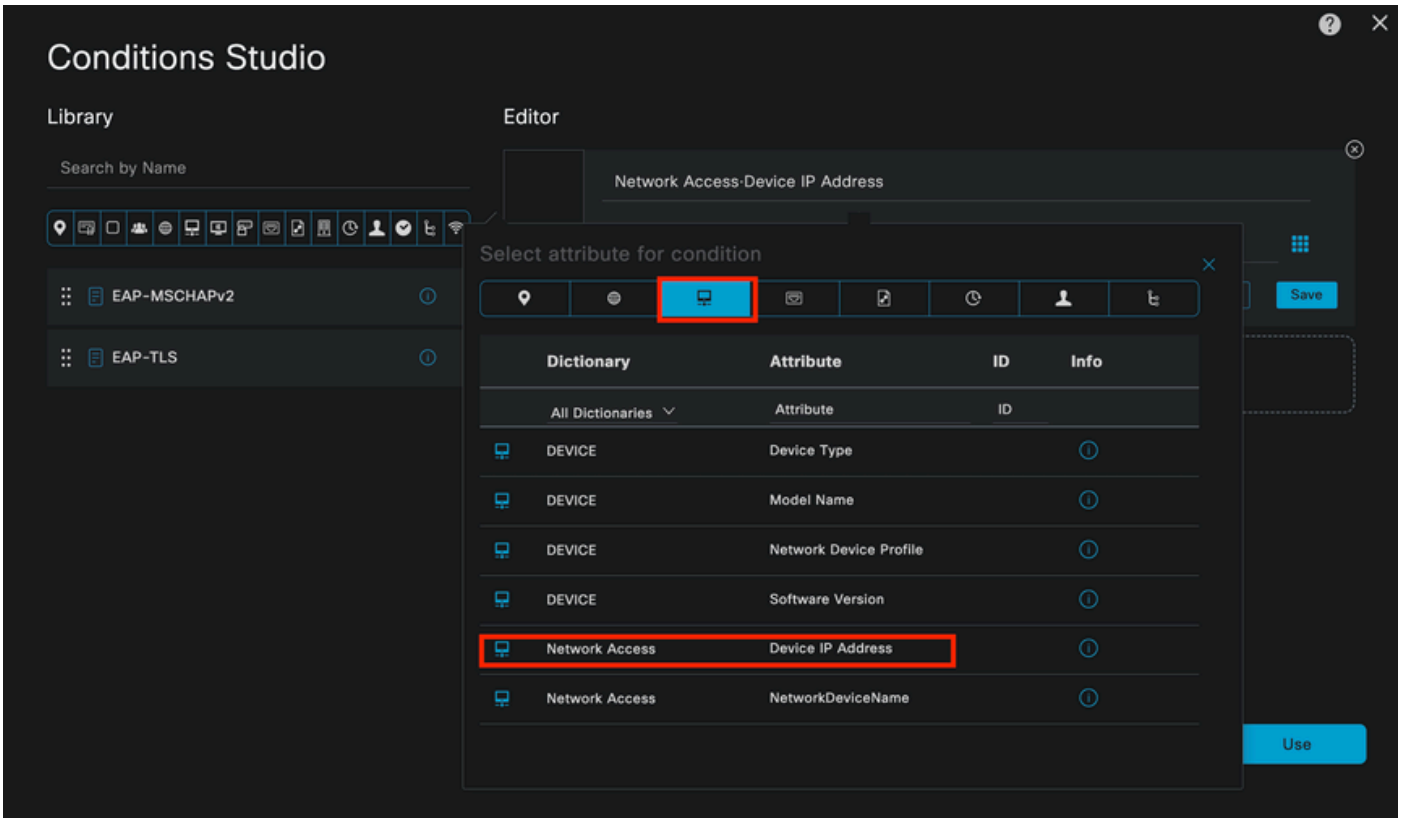
In dit configuratievoorbeeld is de waarde Naam Interne Verificatie en de gekozen voorwaarde is het Netwerkapparaat (Nexus) IP (het A.B.C.D.). Dit verificatiebeleid maakt gebruik van de Interne Gebruikers Identity Store.



Verificatiebeleid

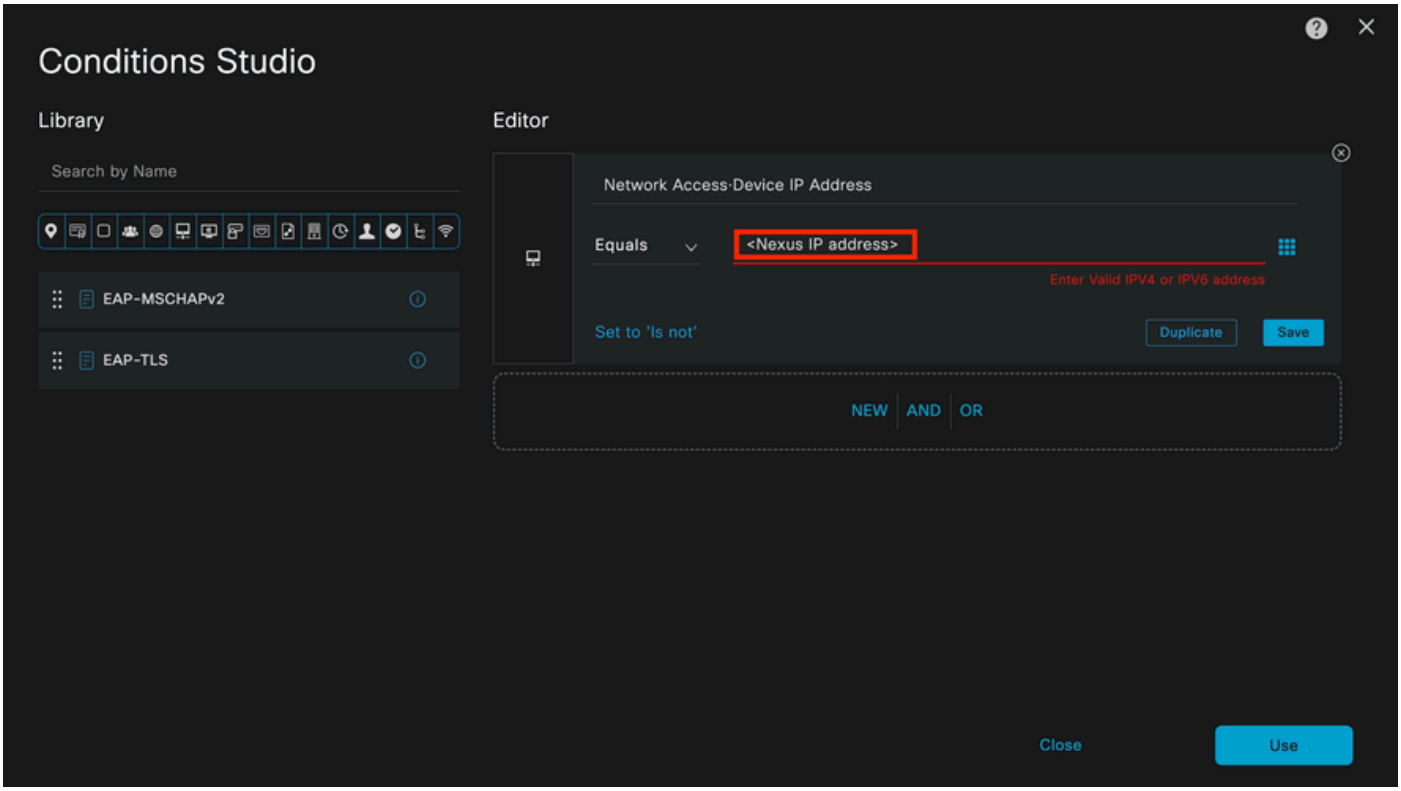
Dit is hoe de situatie was ingesteld.

Selecteer het woordenboekkenmerk Netwerktoegang > IP-adres van het apparaat.



Condition studio voor authenticatiebeleid

Vervang de opmerking <Nexus IP-adres> door het juiste IP-adres.



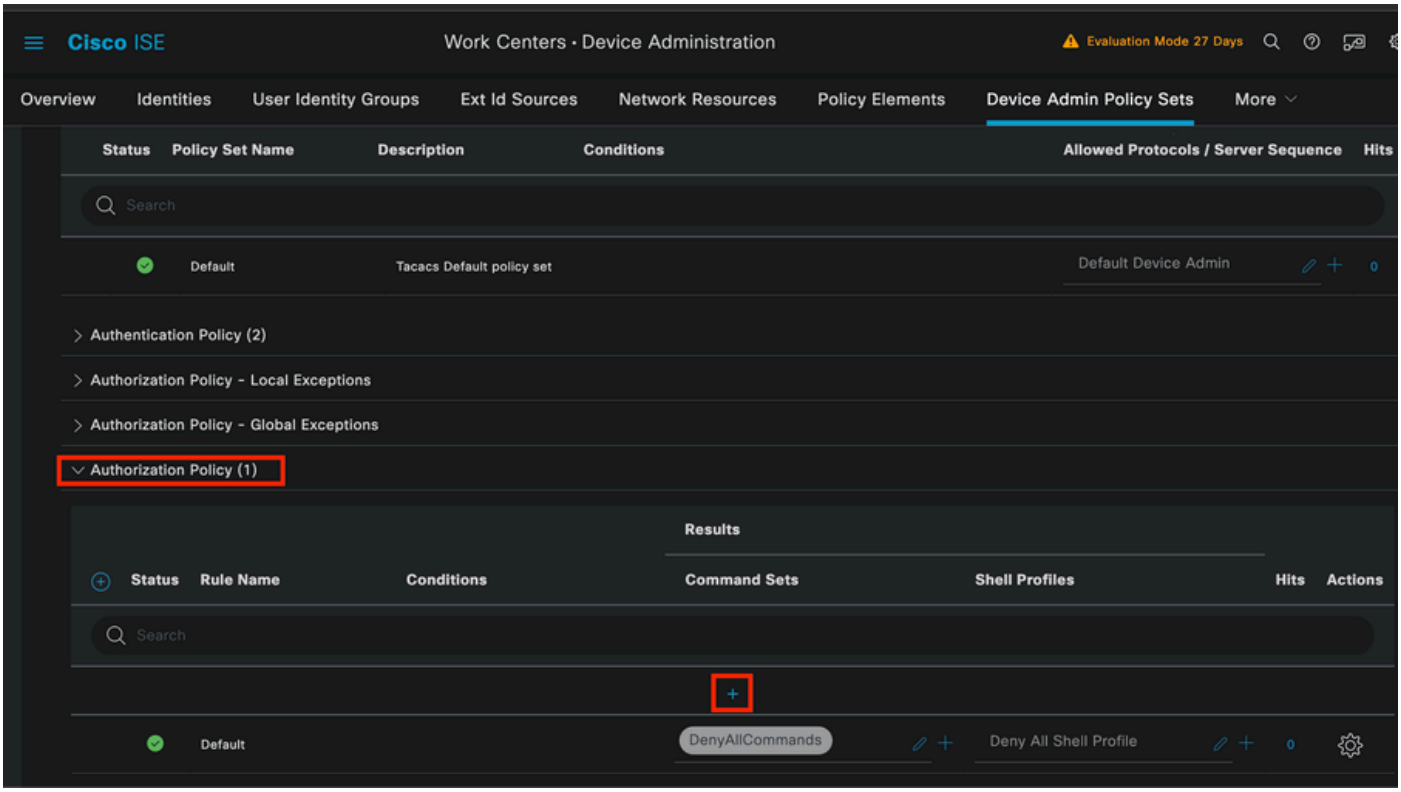
Het IP-filter toevoegen

Klik op de knop Gebruik.

Deze conditie wordt alleen geraakt door het Nexus-apparaat dat u hebt geconfigureerd, maar als het doel is om deze conditie in te schakelen voor een grote hoeveelheid apparaten, moet een andere conditie worden overwogen.

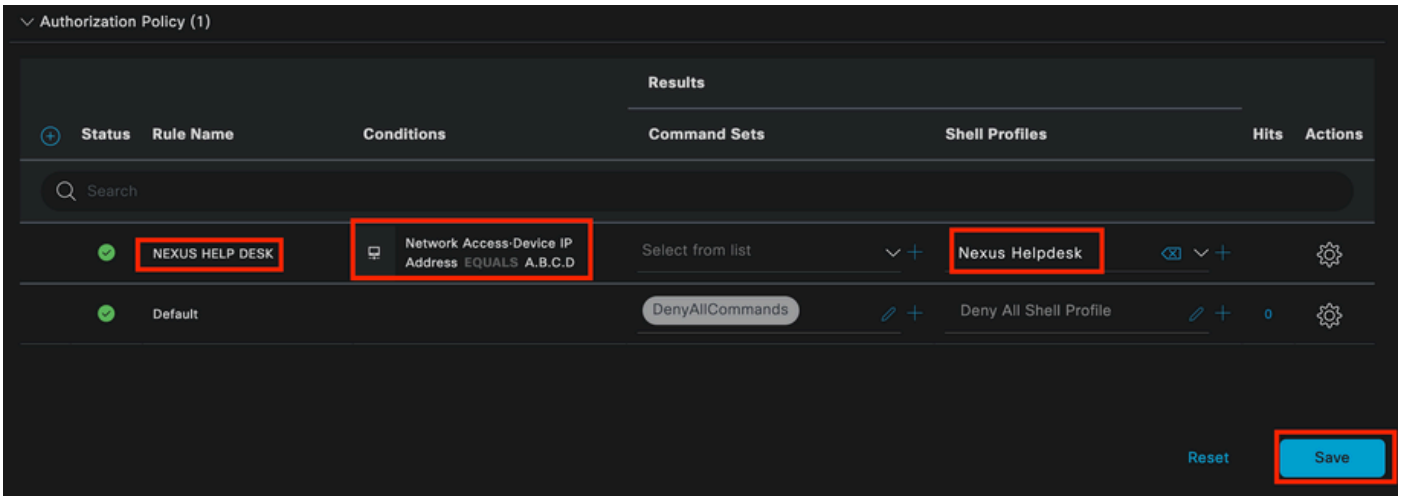
Navigeer vervolgens naar het gedeelte Autorisatiebeleid en vouw dit uit.

Klik op het + (plus) pictogram.



Sectie Vergunningsbeleid

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



Condition studio voor autorisatiebeleid

De zelfde voorwaarde die in het Beleid van de Verificatie werd gevormd wordt gebruikt voor het Beleid van de Vergunning.

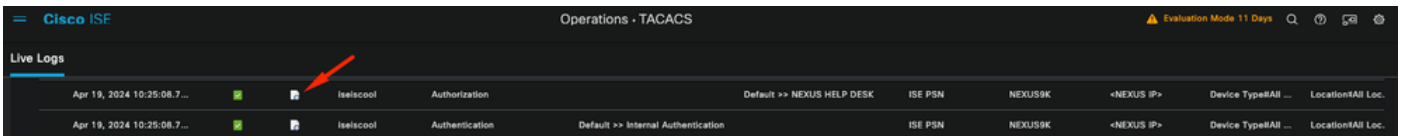
In de kolom Shell Profiles werd het profiel geconfigureerd voordat Nexus Helpdesk werd geselecteerd.

Klik tot slot op de knop Opslaan.

Verifiëren

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

Van ISE GUI, navigeer naar Operations > TACACS > Live Logs, identificeer de record die overeenkomt met de gebruikte gebruikersnaam en klik op het Live Log Detail van de autorisatie-gebeurtenis.



Levend logboek TACACS

Als onderdeel van de details die dit rapport omvat, kan het worden gevonden in een Response-sectie, waar u kunt zien hoe ISE de waarde shell:rollen="helpdesk" heeft teruggegeven

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

Respons bewegende loggegevens

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)#
```

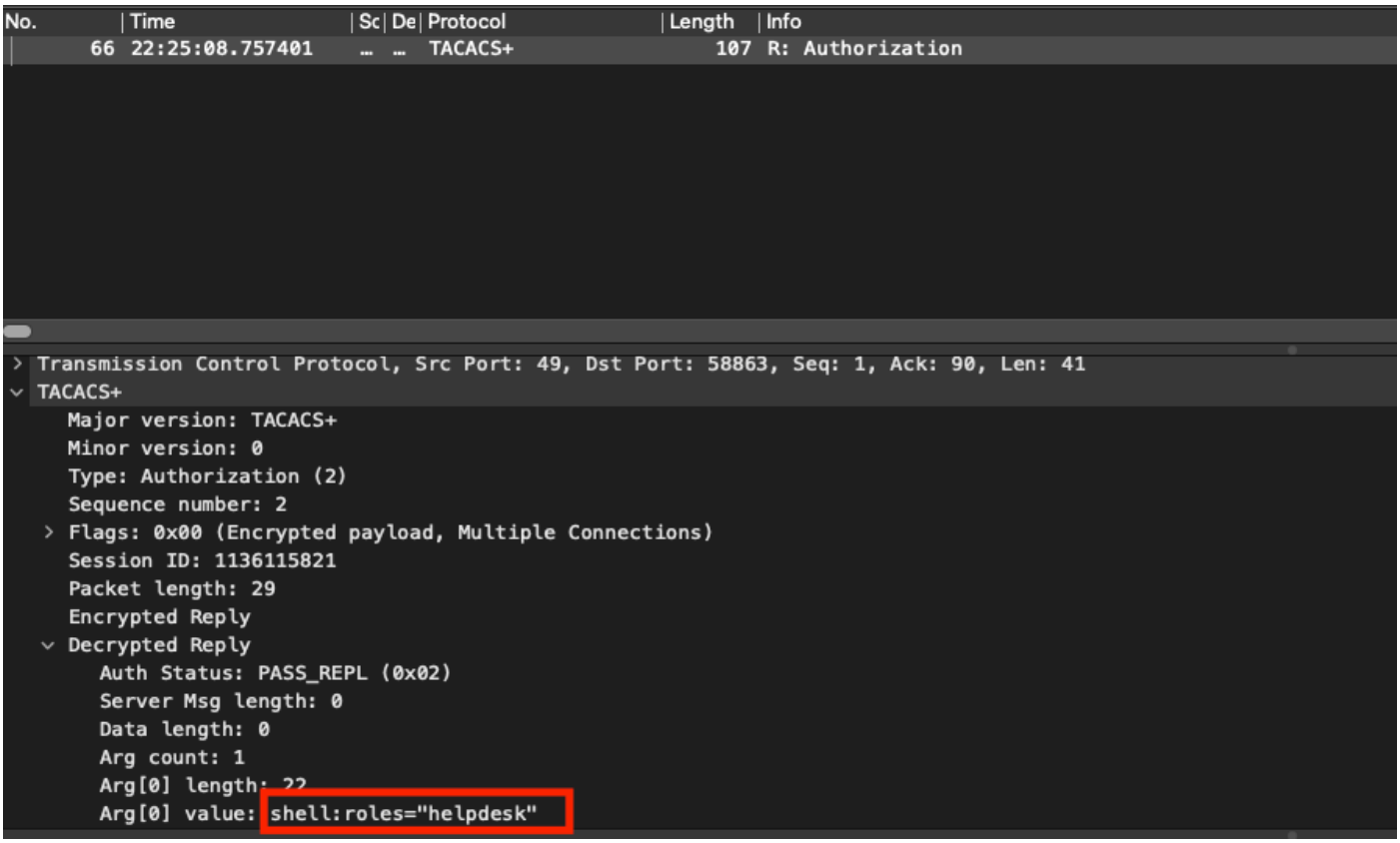
Problemen oplossen

- Controleer of ISE bereikbaar is vanaf het Nexus-apparaat.Nexus 9000# ping <Your ISE IP>
  PINGEN <Uw ISE-IP> (<Uw ISE-IP> 56 gegevensbytes
  64 bytes vanaf <Uw ISE-id>: icmp_seq=0 ttl=59 time=1.22 ms
  64 bytes vanaf <Uw ISE-id>: icmp_seq=1 ttl=59 time=0.739 ms
  64 bytes vanaf <Uw ISE-id>: icmp_seq=2 ttl=59 time=0.686 ms
  64 bytes vanaf <Uw ISE-id>: icmp_seq=3 ttl=59 time=0.71 ms
  64 bytes vanaf <Uw ISE-id>: icmp_seq=4 ttl=59 time=0.72 ms
- Controleer of poort 49 is geopend tussen ISE en het Nexus apparaat.
  Nexus 9000# telnet <uw ISE-netwerkmodule> 49
  Proberen <uw ISE-IP> ...
  Verbonden met <uw ISE-id>.
  Escape is '^]'.
- Gebruik deze debugs:

debug tacacs+ all
Nexus 9000#
Nexus 9000# 2024 apr 19 22:50:44.199329 tacacs: event_loop(): aanroepend process_rd_fd_set
2024 apr 19 22:50:44.199355 tacacs: process_rd_fd_set: callback voor fd 6
2024 apr 19 22:50:44.199392 tacacs: fsrv didnt consume 8421 opcode
2024 apr 19 22:50:44.199406 tacacs: process_implicit_cfs_sessie_start: enter...
2024 apr 19 22:50:44.199414 tacacs: process_implicit_cfs_sessie_start: exiting; we zijn in distributie gehandicapte staat
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): binnenkomst ...
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): terug de terugkeerwaarde van de globale protocolconfiguratie operatie: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 groep 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 encryptie_type 7
2024 apr 19 22:50:44.208086 tacacs: tacacs_global_config: retourneren retval 0
2024 apr 19 22:50:44.208098 tacacs: process_aaa_tplus_request:group_info is ingevuld in aaa_req, dus Gebruik servergroep IsePsnServers

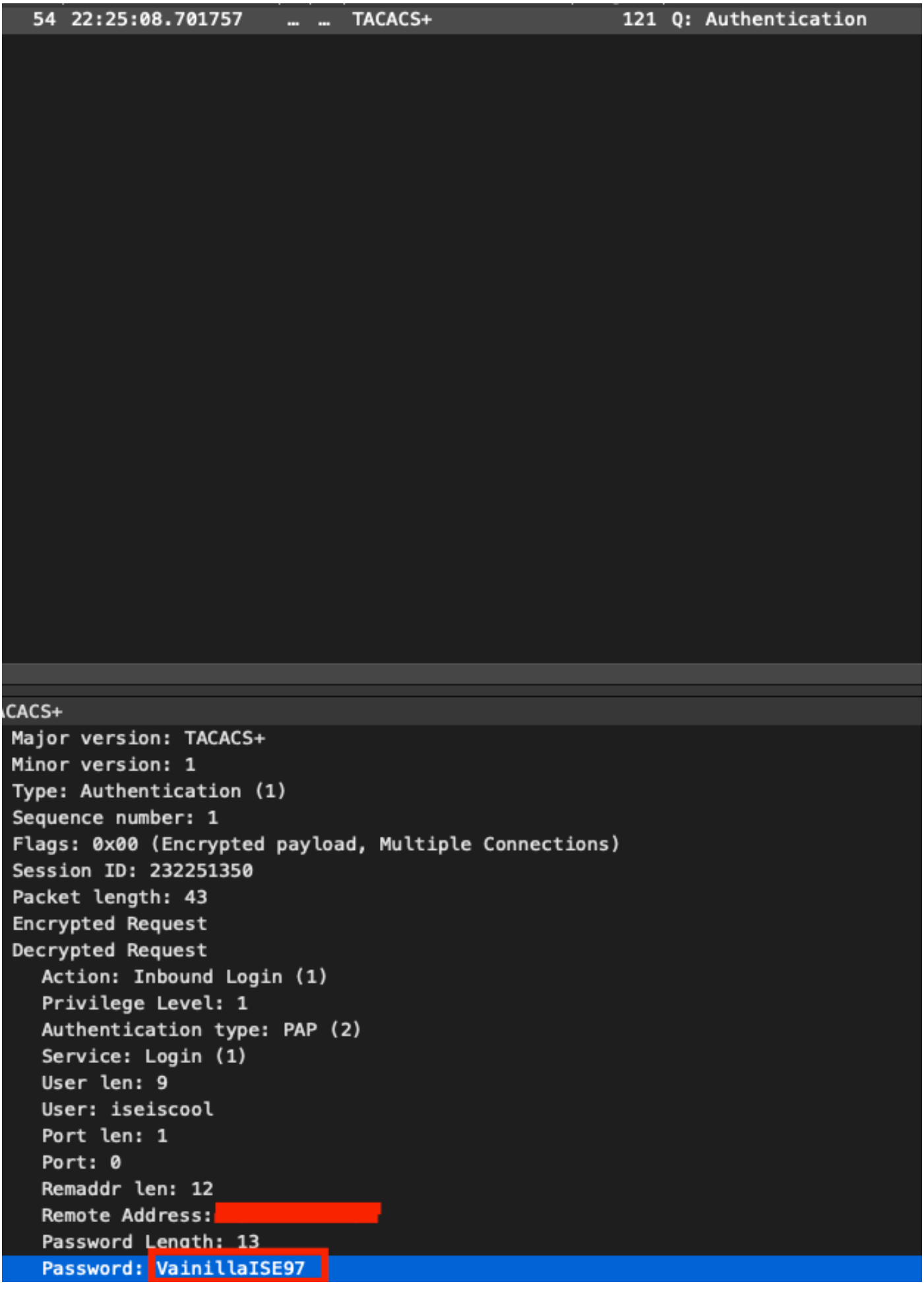
2024 apr 19 22:50:44.208108 tacacs: tacacs_servergroup_config: invoeren voor server groep, index 0
2024 apr 19 22:50:44.208117 tacacs: tacacs_servergroup_config: GETNEXT_REQ voor Protocol server group index:0 naam:
2024 apr 19 22:50:44.208148 tacacs: tacacs_pss2_move2key: rcode = 40480003 syserr2str = geen pss key
2024 apr 19 22:50:44.208160 tacacs: tacacs_pss2_move2key: het oproepen van pss2_getkey
2024 apr 19 22:50:44.208171 tacacs: tacacs_servergroep_config: GETNEXT_REQ kreeg Protocol server group index:2 naam:IsePsnServers
2024 apr 19 22:50:44.208184 tacacs: tacacs_servergroup_config: kreeg terug de retourwaarde van Protocol groep operatie:SUCCES
2024 apr 19 22:50:44.208194 tacacs: tacacs_servergroup_config: retourneren retval 0 voor Protocol server group: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: checken voor mgmt0 vrf:management tegen vrf:default van de gevraagde 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 default
2024 apr 19 22:50:44.208286 tacacs: creative_tplus_req_state_machine(902): invoeren voor aaa sessie id 0
2024 apr 19 22:50:44.208295 tacacs: state machine count 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 moet 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_servergroep_config: GET_REQ voor Protocol server group index:0 naam:IsePsnServers
2024 apr 19 22:50:44.208357 tacacs: find_tacacs_servergroup: enter voor server groep 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: Exiting for server group IsePsnServers index is 2
2024 apr 19 22:50:44.208401 tacacs: tacacs_servergroep_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_servergroep_config: GET_REQ kreeg Protocol server group index:2 naam:IsePsnServers
2024 A2024 apr 19 22:52024 apr 19 22:52024 apr 19 22:5
Nexus 9000#

- Voer een pakketopname uit (om de pakketdetails te zien, moet u Wireshark TACACS+ Voorkeuren wijzigen en de gedeelde sleutel die door Nexus en ISE wordt gebruikt, bijwerken)



TACACS-autorisatiepakket

- Controleer of de gedeelde sleutel hetzelfde is aan de kant van ISE en Nexus. 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.