Configureer TACACS+ met ISE Gigabit Ethernet-interface

Inhoud

Inleiding

Dit document beschrijft de ISE-TACACS+ configuratie met Gigabit Ethernet-1 interface, waarbij router en Switch als netwerkapparaten werken.

Achtergrondinformatie

Cisco ISE ondersteunt maximaal 6 Ethernet interfaces. Het kan slechts drie obligaties hebben, obligatie 0, obligatie 1 en obligatie 2. Je kunt de interfaces die onderdeel zijn van een obligatie niet

veranderen en ook de rol van de interface in een obligatie niet veranderen.

Voorwaarden

Vereisten

Cisco raadt u aan kennis te hebben over deze onderwerpen:

- Basiskennis van netwerken
- Cisco Identity Service Engine

Gebruikte componenten

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

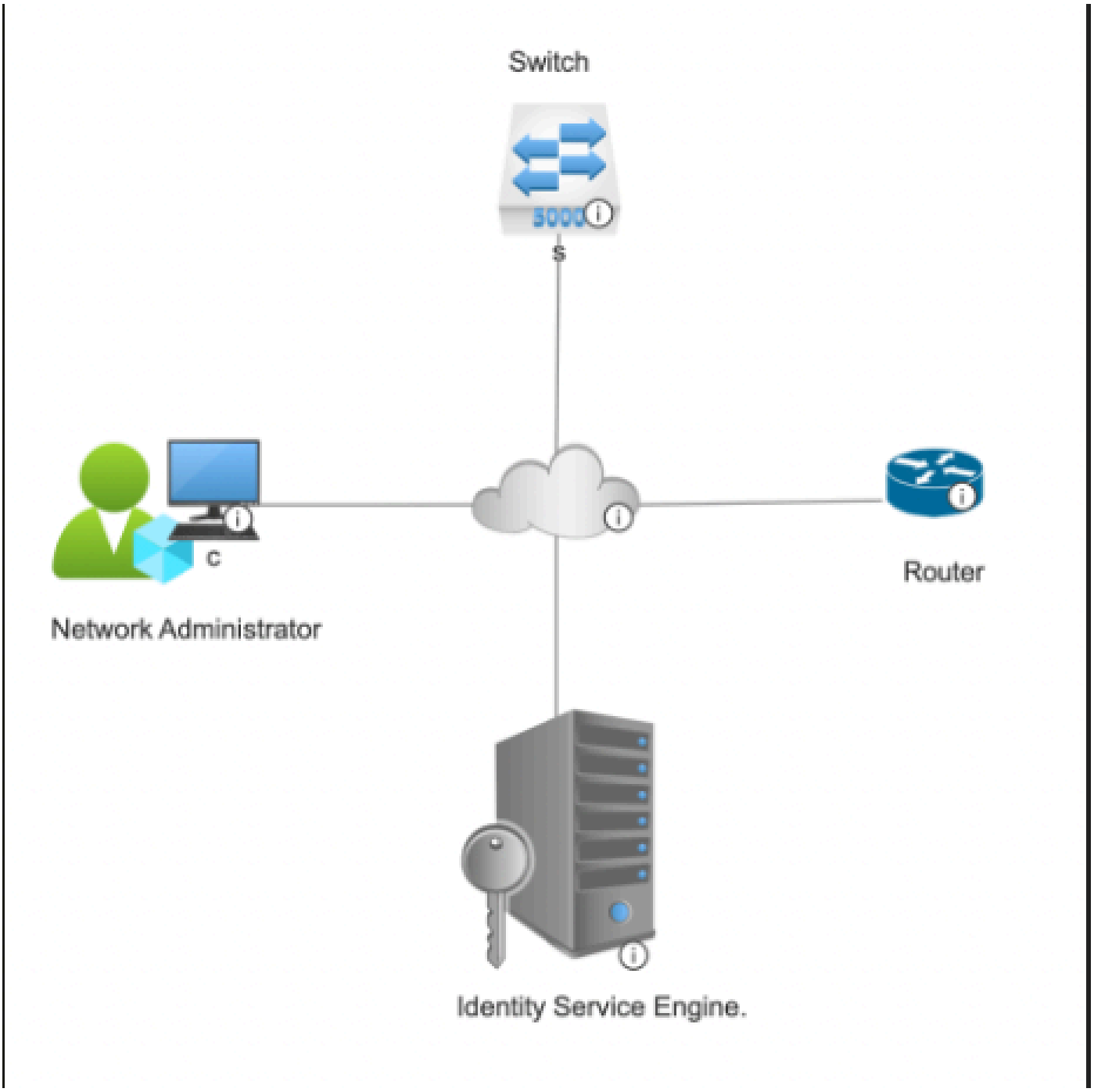
- Cisco Identity Service Engine v3.3
- Cisco IOS®-softwarerelease 17.x
- Cisco C9200 switch

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.

Configureren

Het doel van de configuratie is: Configureer Gigabit Ethernet 1 van ISE voor TACACS+ en controleer switch en router met TACACS+ met ISE als verificatieserver.

Netwerkdiagram

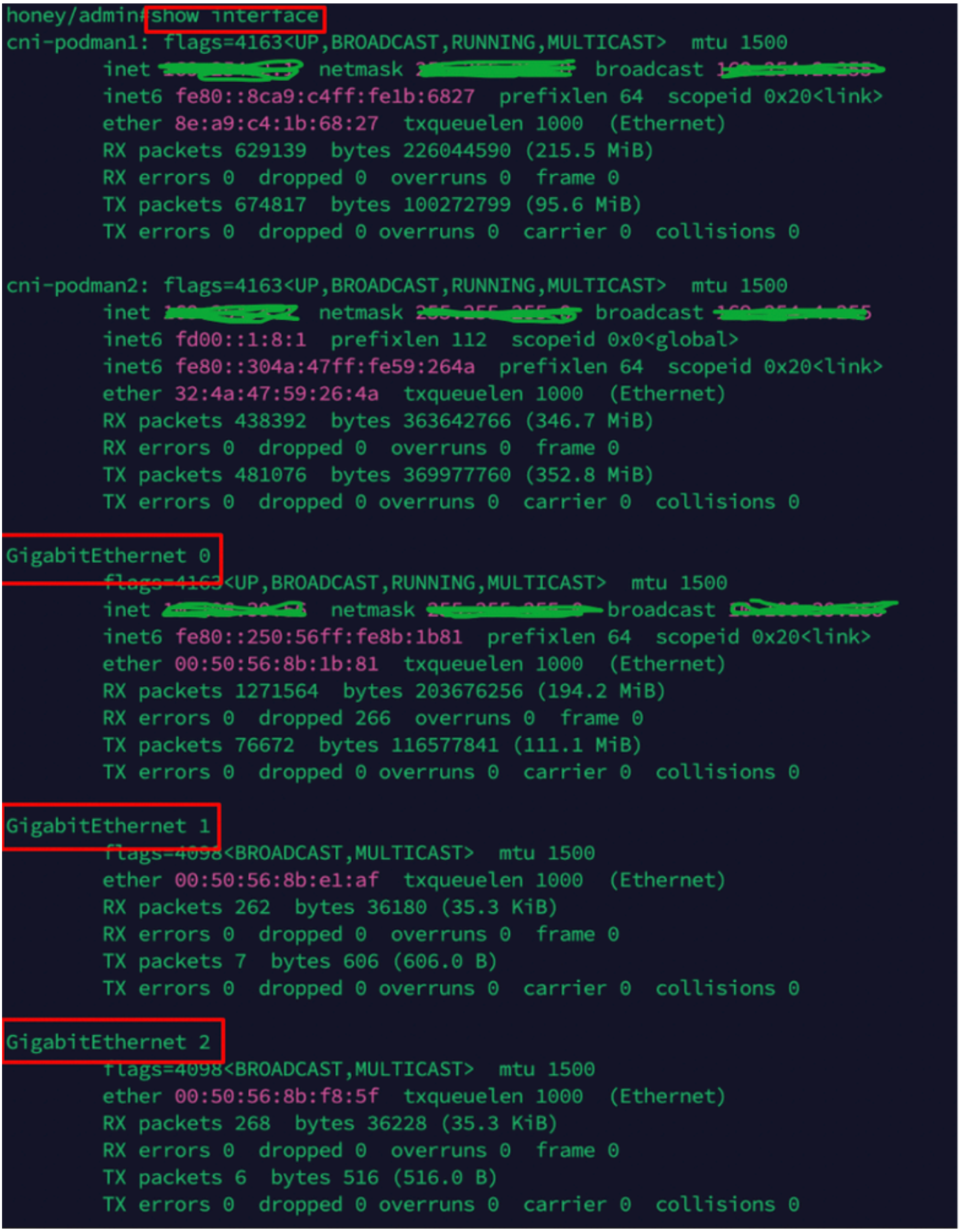


Netwerktopologie

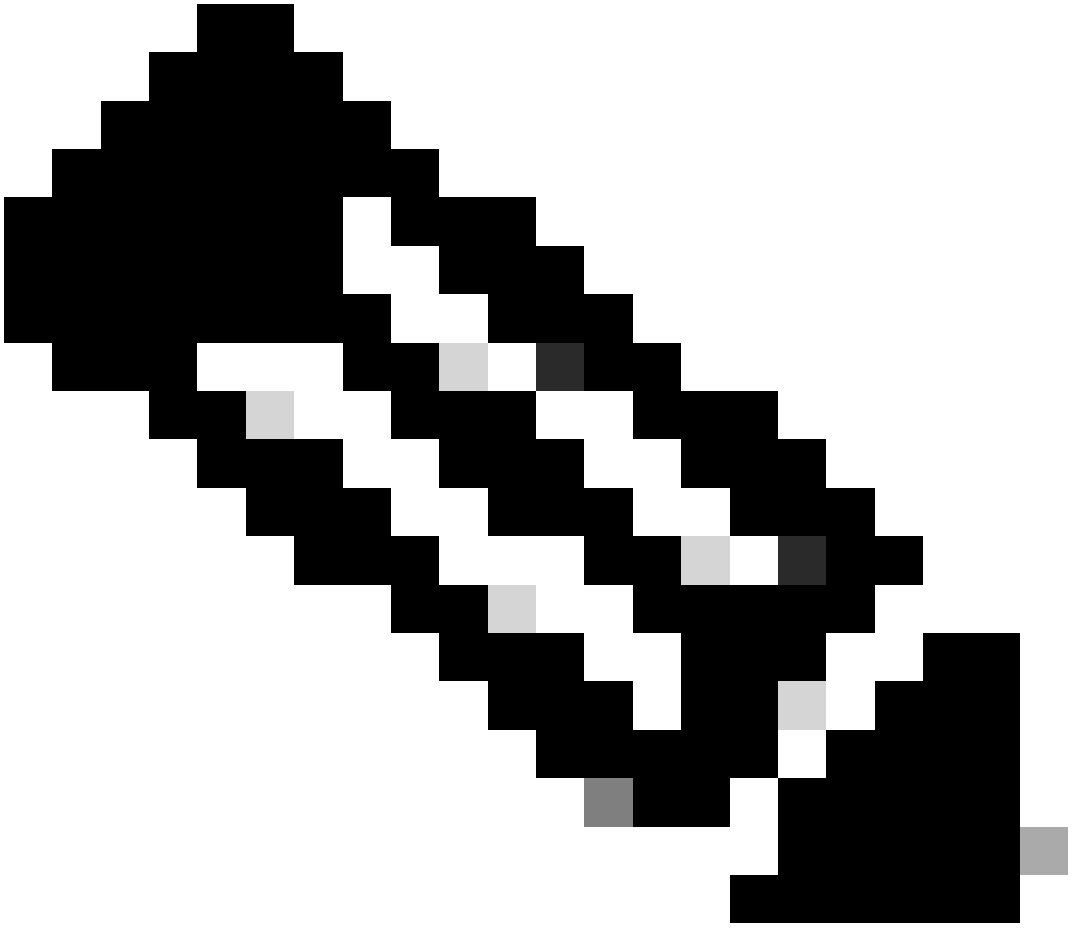
Configuratie van Identity Services Engine voor TACACS+

IP-adres voor Gigabit Ethernet-, 1-interface in ISE configureren

1. Log in op de CLI van de ISE-PSN-knooppunt waar Apparaatbeheer is ingeschakeld en controleer de beschikbare interfaces met de opdracht interface tonen:



Verificatie van interfaces in ISE



Opmerking: In deze configuratie worden slechts drie interfaces geconfigureerd in ISE, met een focus op de Gigabit Ethernet 1-interface. De zelfde procedure kan worden toegepast om het IP adres voor alle interfaces te vormen. Standaard ondersteunt ISE maximaal zes Gigabit Ethernet-interfaces.

---

2. Van CLI van dezelfde PSN-knooppunt kunt u een IP-adres aan de Gigabit Ethernet 1-interface toewijzen met behulp van deze opdrachten:

hostnameFise#configureren

hostnameaccount/beheerder (configuratie)#interface Gigabit Ethernet 1

hostnameaccount/admin (configuratie-Gigabit Ethernet-1)# <ip-adres> <subnetmasker> % Het wijzigen van het IP-adres kan ertoe leiden dat ISE-services opnieuw worden gestart

Doorgaan met wijziging van IP-adres?

Doorgaan? [ja,nee] ja

3. Door stap 2 uit te voeren, kunt u de ISE-knooppunten opnieuw opstarten. Om de status van de ISE-diensten te verifiëren, voert u de opdracht toepassingsstatus tonen uit en zorgt u ervoor dat de status van de services actief is volgens deze screenshot:

```
honey/admin#show application status ise

ISE PROCESS NAME                       STATE            PROCESS ID
--------------------------------------------------------------------
Database Listener                      running          1739169
Database Server                        running          102 PROCESSES
Application Server                     running          1755746
Profiler Database                      running          1746379
ISE Indexing Engine                    running          1757121
AD Connector                           running          1759148
M&T Session Database                   running          1752122
M&T Log Processor                      running          1755926
Certificate Authority Service          running          1759026
EST Service                            running          1786647
SXP Engine Service                     disabled
TC-NAC Service                         disabled
PassiveID WMI Service                  disabled
PassiveID Syslog Service               disabled
PassiveID API Service                  disabled
PassiveID Agent Service                disabled
PassiveID Endpoint Service             disabled
PassiveID SPAN Service                 disabled
DHCP Server (dhcpd)                    disabled
DNS Server (named)                     disabled
ISE Messaging Service                  running          1743222
ISE API Gateway Database Service       running          1745409
ISE API Gateway Service                running          1750887
ISE pxGrid Direct Service              running          1874179
Segmentation Policy Service            disabled
REST Auth Service                      disabled
SSE Connector                          disabled
Hermes (pxGrid Cloud Agent)            disabled
McTrust (Meraki Sync Service)          disabled
ISE Node Exporter                      running          1760519
ISE Prometheus Service                 running          1762540
ISE Grafana Service                    running          1765779
ISE MNT LogAnalytics Elasticsearch     running          1768218
ISE Logstash Service                   running          1773207
ISE Kibana Service                     running          1774914
ISE Native IPSec Service               running          1779658
MFC Profiler                           running          1932013
```

Statusverificatie ISE-service

4. Controleer het IP-adres van de Gig1-interface met behulp van de opdracht show interface:

V

```
honey/admin#show interface
cni-podman1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet [redacted]  netmask [redacted]  broadcast [redacted]
        inet6 fe80::8ca9:c4ff:fe1b:6827  prefixlen 64  scopeid 0x20<link>
        ether 8e:a9:c4:1b:68:27  txqueuelen 1000  (Ethernet)
        RX packets 633876  bytes 228753800 (218.1 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 680052  bytes 102100762 (97.3 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

cni-podman2: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet [redacted]  netmask [redacted]  broadcast [redacted]
        inet6 fd00::1:8:1  prefixlen 112  scopeid 0x0<global>
        inet6 fe80::304a:47ff:fe59:264a  prefixlen 64  scopeid 0x20<link>
        ether 32:4a:47:59:26:4a  txqueuelen 1000  (Ethernet)
        RX packets 503576  bytes 516105026 (492.1 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 595701  bytes 383404526 (365.6 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

GigabitEthernet 0
        flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet [redacted]  netmask [redacted]  broadcast [redacted]
        inet6 fe80::250:56ff:fe8b:1b81  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:8b:1b:81  txqueuelen 1000  (Ethernet)
        RX packets 1387052  bytes 213478717 (203.5 MiB)
        RX errors 0  dropped 266  overruns 0  frame 0
        TX packets 136494  bytes 261900250 (249.7 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

GigabitEthernet 1
        flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet [redacted]  netmask [redacted]  broadcast [redacted]
        inet6 fe80::250:56ff:fe8b:e1af  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:8b:e1:af  txqueuelen 1000  (Ethernet)
        RX packets 5165  bytes 1072036 (1.0 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 28  bytes 2260 (2.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Verificatie van ISE Gig2-interface met IP-adres van CLI

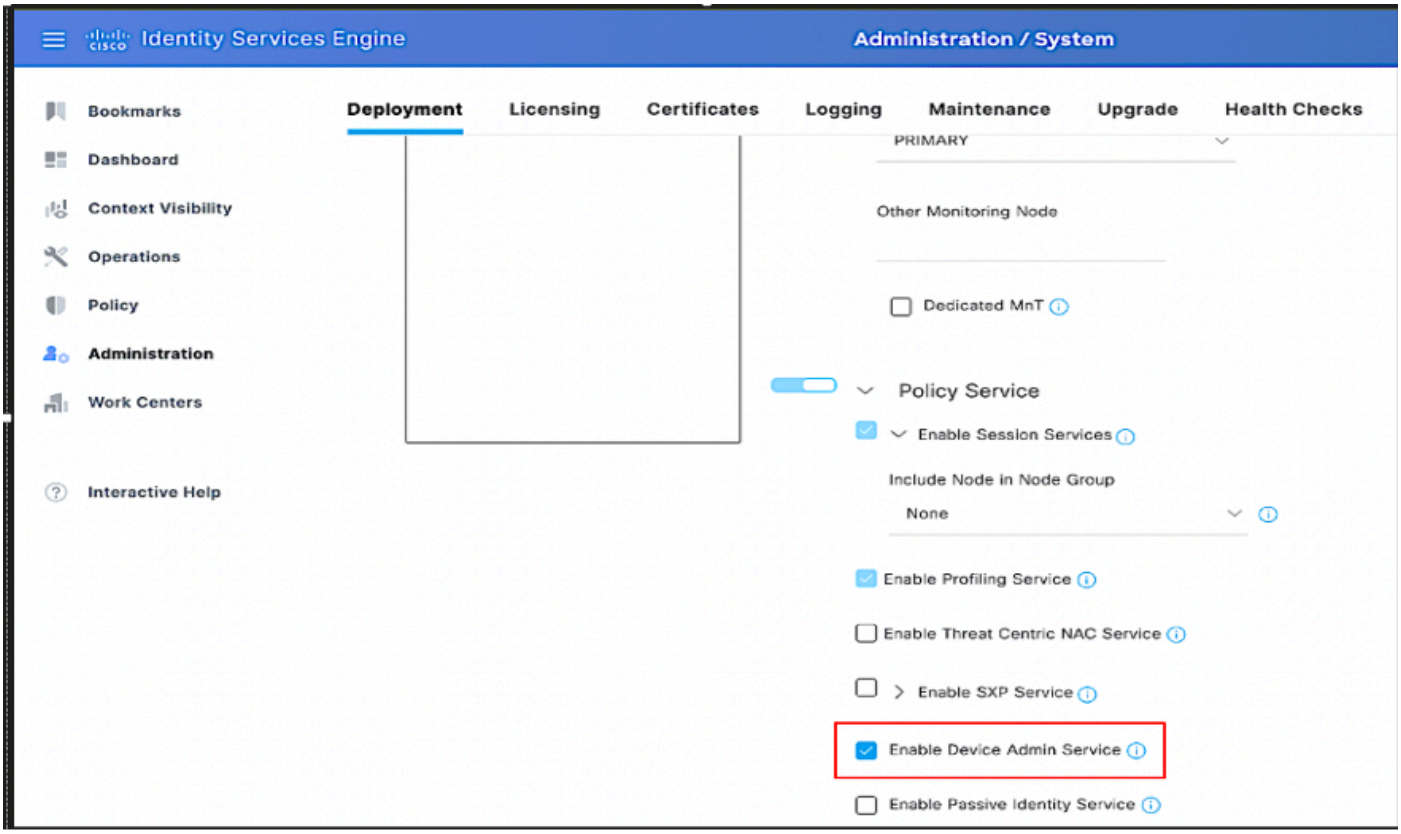
5.Controleer het toestaan van poort 49 in de ISE-knooppunt met behulp van de showpoorten | inc 49 opdracht:

```
honey/admin#show ports | include 49
          tcp: 127.0.0.1:8888, 169.254.4.1:49, 169.254.2.1:49, [redacted]:49, [redacted]:49,
```

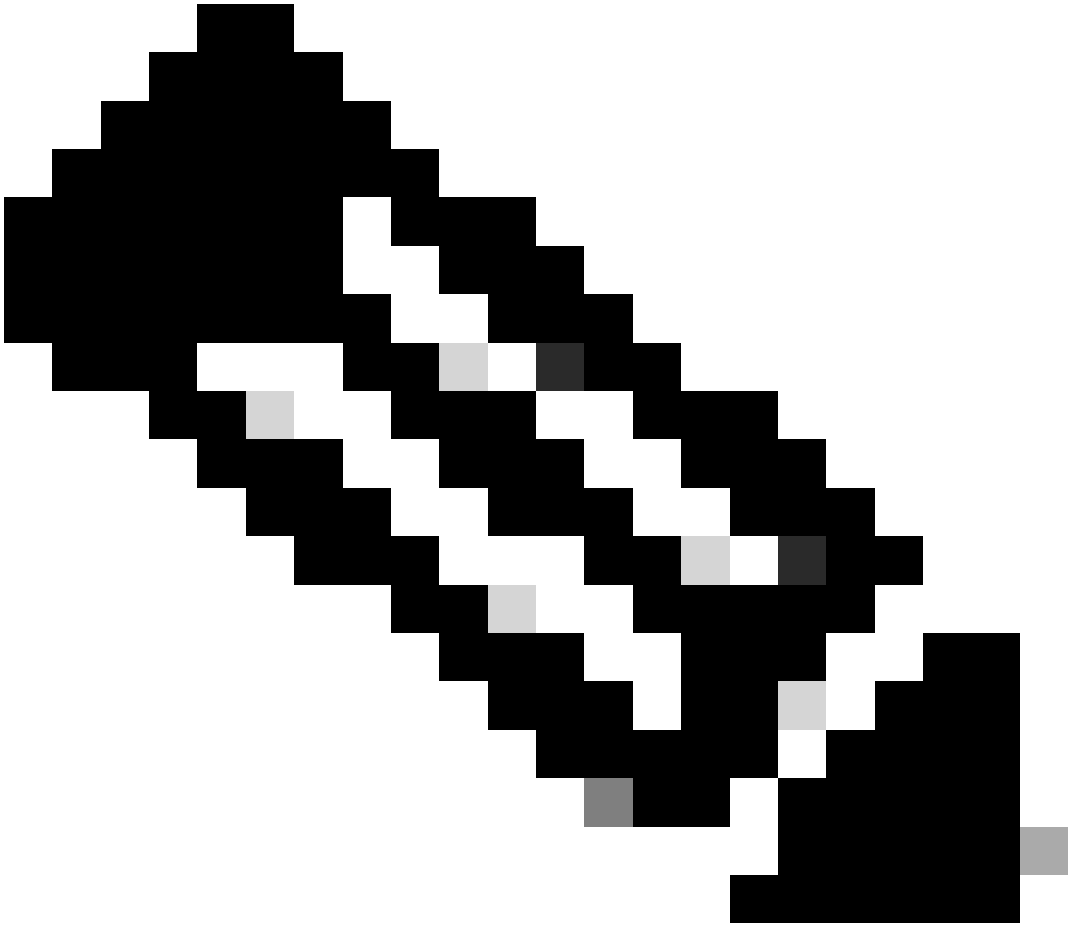
verificatie van de havenvergunning 49 in ISE

Apparaatbeheer in ISE inschakelen

Navigeer naar GUI (GUI) van ISE > Beheer > Implementatie > Selecteer het PSN-knooppunt en controleer vervolgens Apparaatbeheerservice inschakelen:



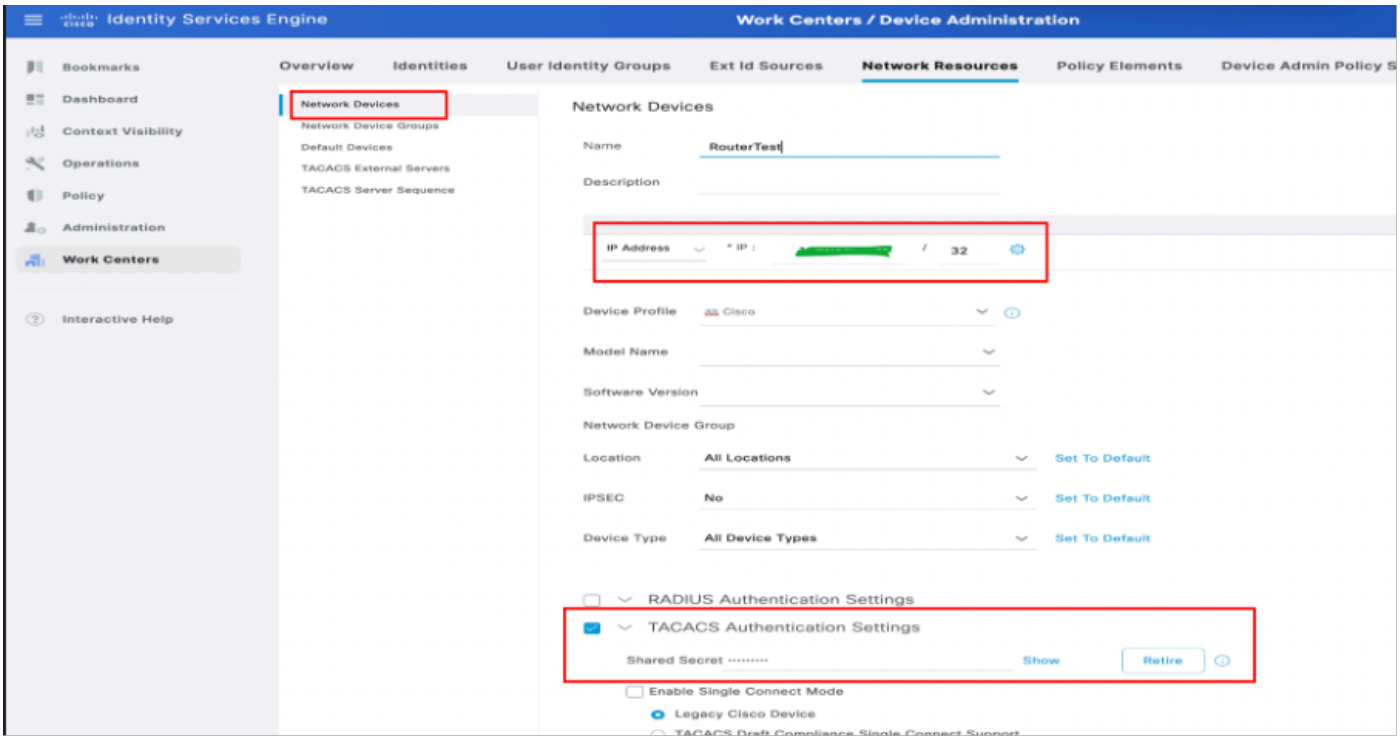
Apparaatbeheerservice inschakelen in ISE



Opmerking: Om de service Apparaatbeheer in te schakelen, is een Apparaatbeheerlicentie vereist.

Een netwerkapparaat toevoegen in ISE

1. Navigeren naar werkcentra > Apparaatbeheer > Netwerkbronnen > Netwerkapparaten. Klik op Add (Toevoegen). Geef naam, IP-adres op. Selecteer het aanvinkvakje TACACS+ verificatie-instellingen en geef de gedeelde geheime sleutel op.



Configuratie van netwerkapparaat in ISE

2. Volg de bovenstaande procedure voor het toevoegen van alle vereiste netwerkapparaten voor TACACS-verificatie.

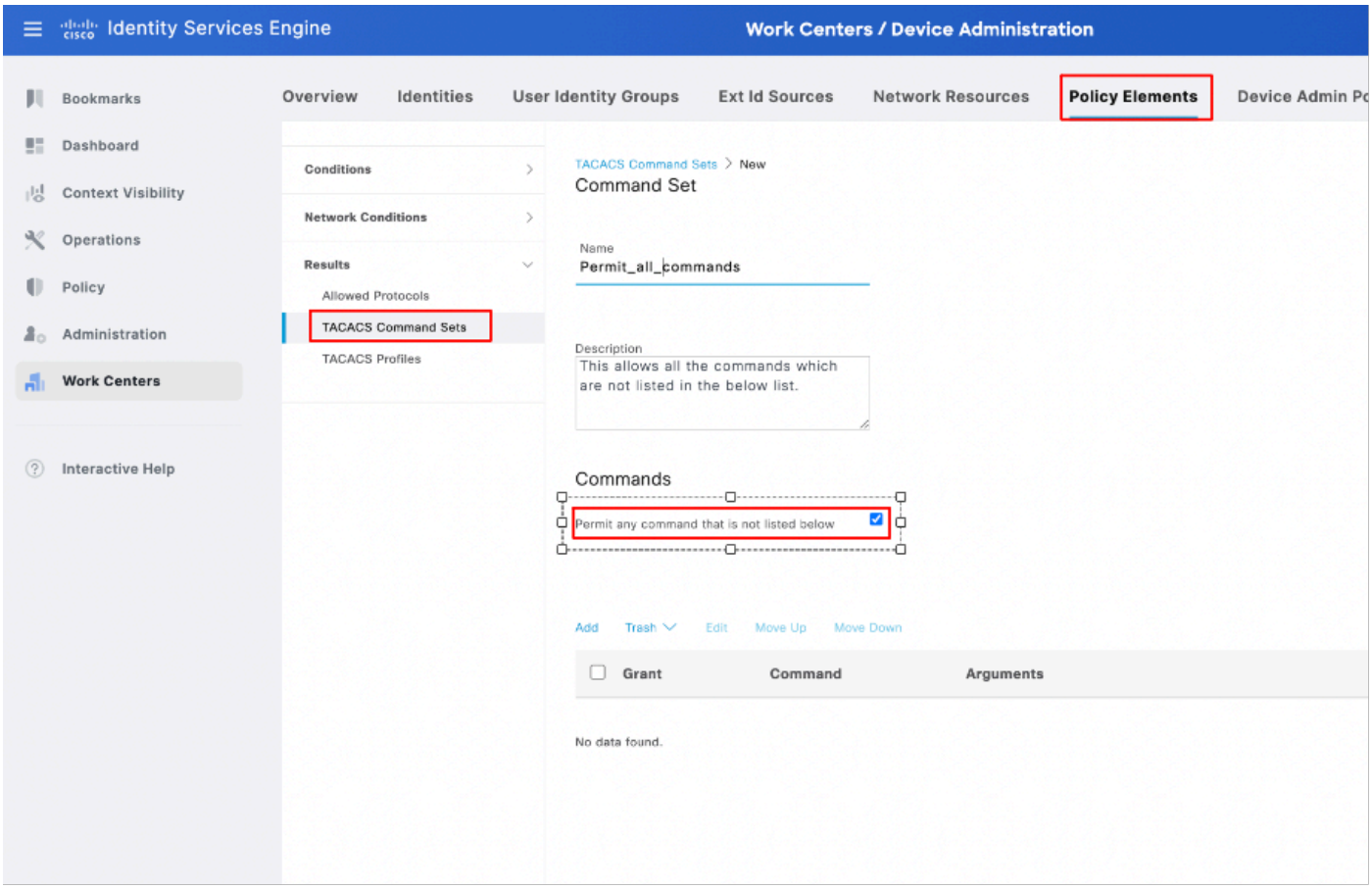
Opdrachtsets voor TACACS+ configureren

Voor deze demonstratie zijn twee opdrachtsets geconfigureerd:

Permit_all_commando's, wordt toegewezen aan de gebruiker admin en staat alle commando's op het apparaat toe.

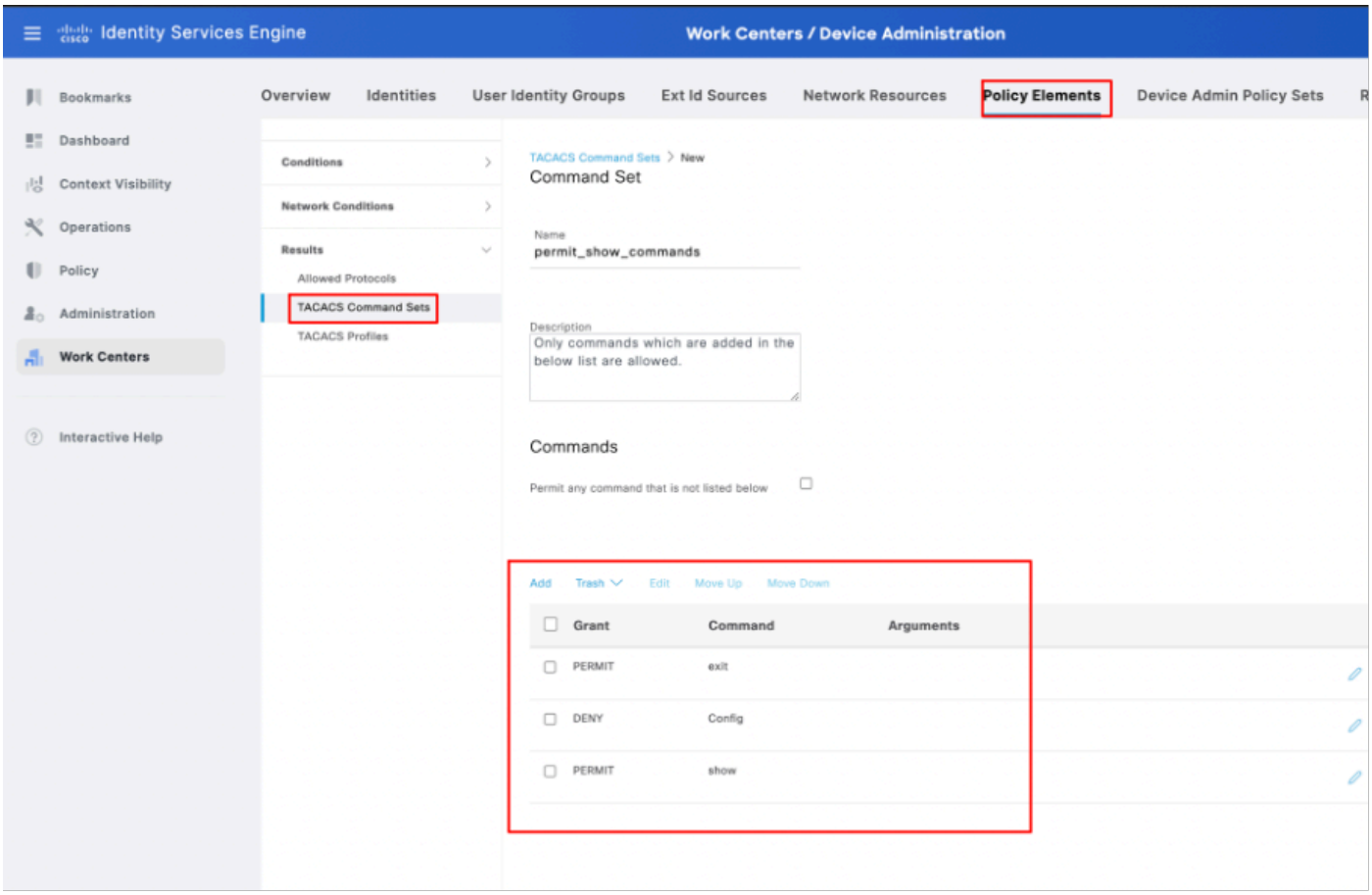
license_show_commando's, wordt toegewezen aan een gebruiker en laat alleen opdrachten zien

1. Navigeer naar Werkcentra > Apparaatbeheer > Beleidsresultaten > Tacacs-opdrachtsets. Klik op Toevoegen. Geef de naam PermitAllCommands op, kies vervolgens het selectievakje Toestaan dat niet in de lijst staat. Klik op Verzenden.



Configuratie van opdrachtsets in ISE

2. Navigeren naar werkcentra > Apparaatbeheer > Beleidsresultaten > Tacacs-opdrachtsets. Klik op Toevoegen. Geef de naam PermitShowCommands op, klik op Add, vervolgens laat u show- en exit-opdrachten toe. Als argumenten standaard leeg blijven, worden alle argumenten opgenomen. Klik op Verzenden.

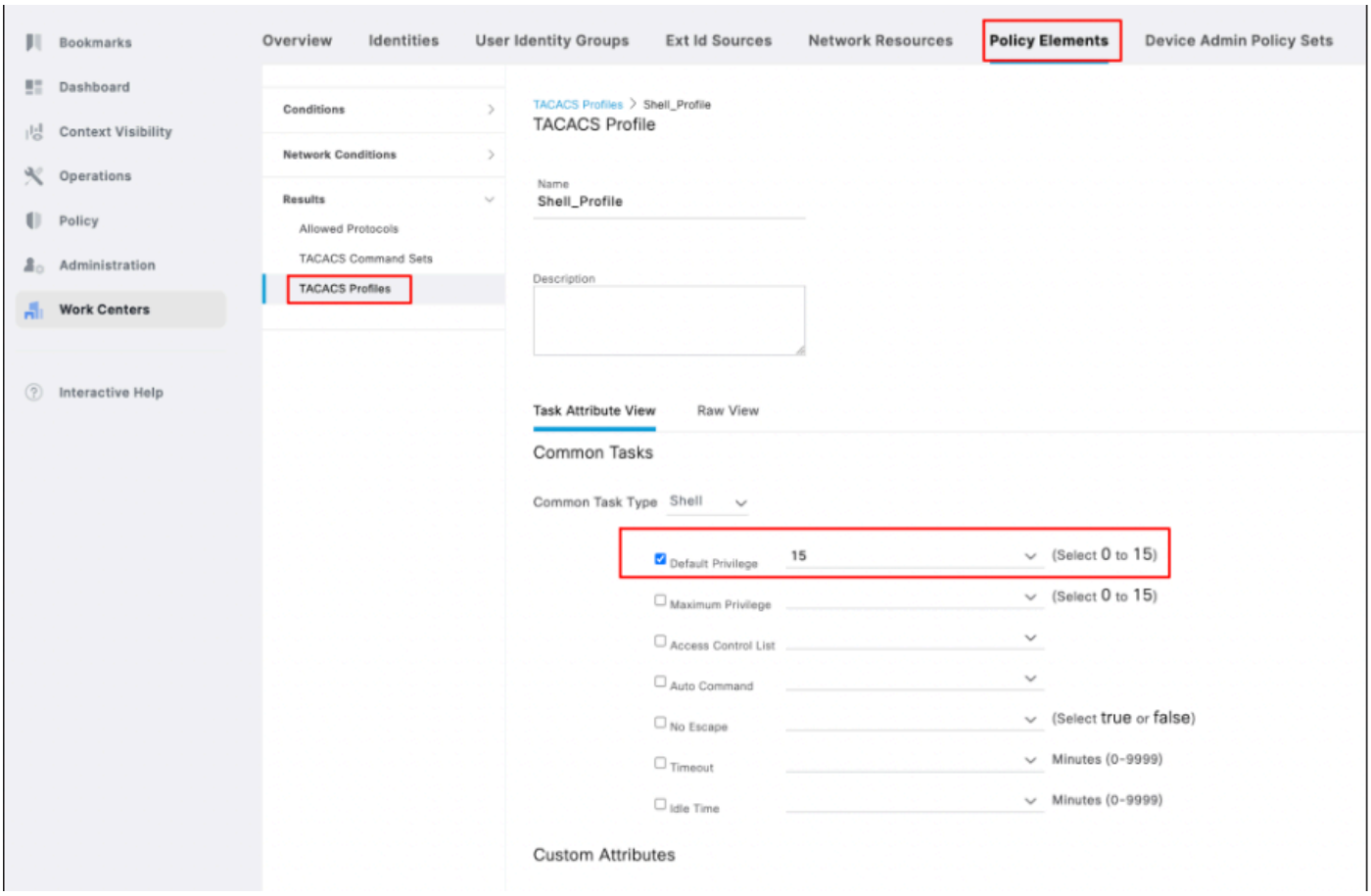


Configuratie van license_show_commando's in ISE

Het TACACS+ profiel configureren

Er wordt één TACACS+ profiel geconfigureerd en de opdrachtautorisatie wordt uitgevoerd via opdrachtsets.

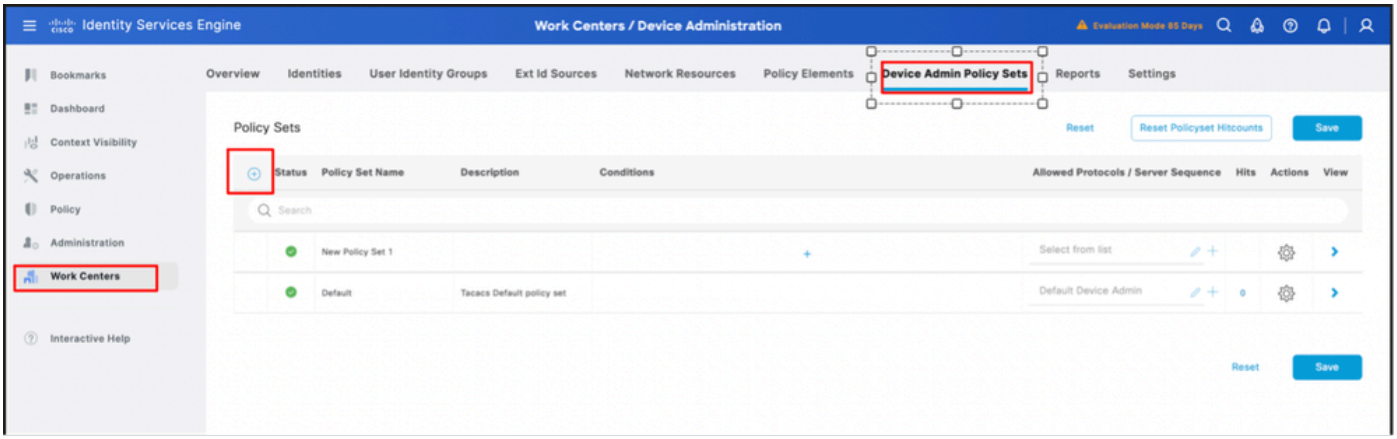
Om een TACACS+ profiel te configureren, navigeer je naar Werkcentra > Apparaatbeheer > Beleidsresultaten > TACACS-profielen. Klik op Add, geef een naam op voor het Shell-profiel, selecteer het aanvinkvakje Default Privilege en voer de waarde 15 in. Klik tot slot op Submit.



Configuratie van het TACACS-profiel in ISE

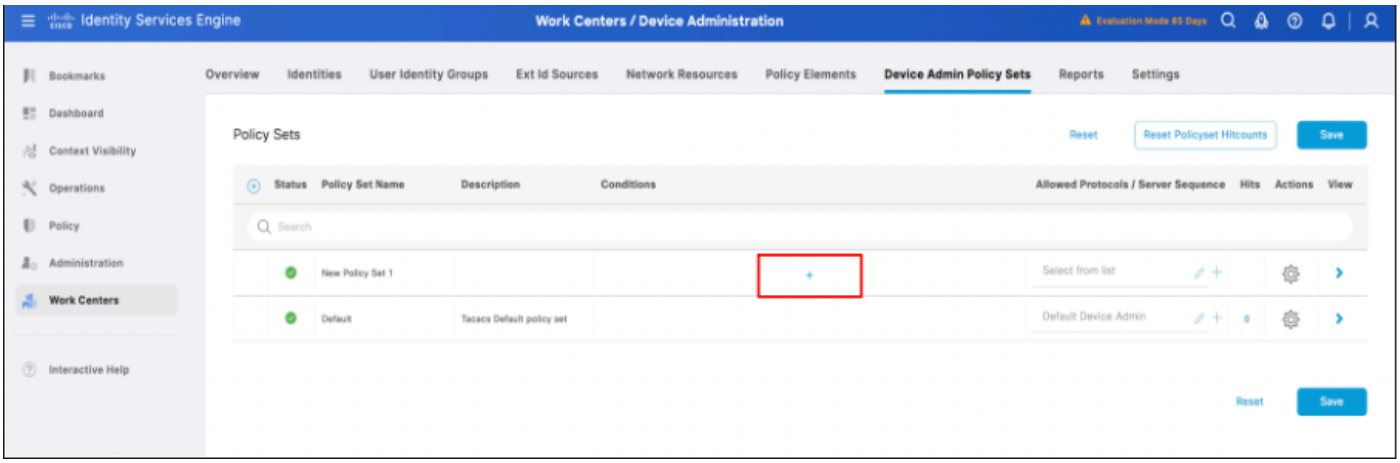
TACACS+-verificatie- en autorisatieprofiel configureren

1. Log in op de ISE PAN GUI -> Beheer -> Werkcentra -> Apparaatbeheer -> Instellingen voor apparaatbeheer. Klik op het + (plus) pictogram om een nieuw beleid te maken. In dit geval wordt de beleidsset Nieuwe Beleidsset 1 genoemd.



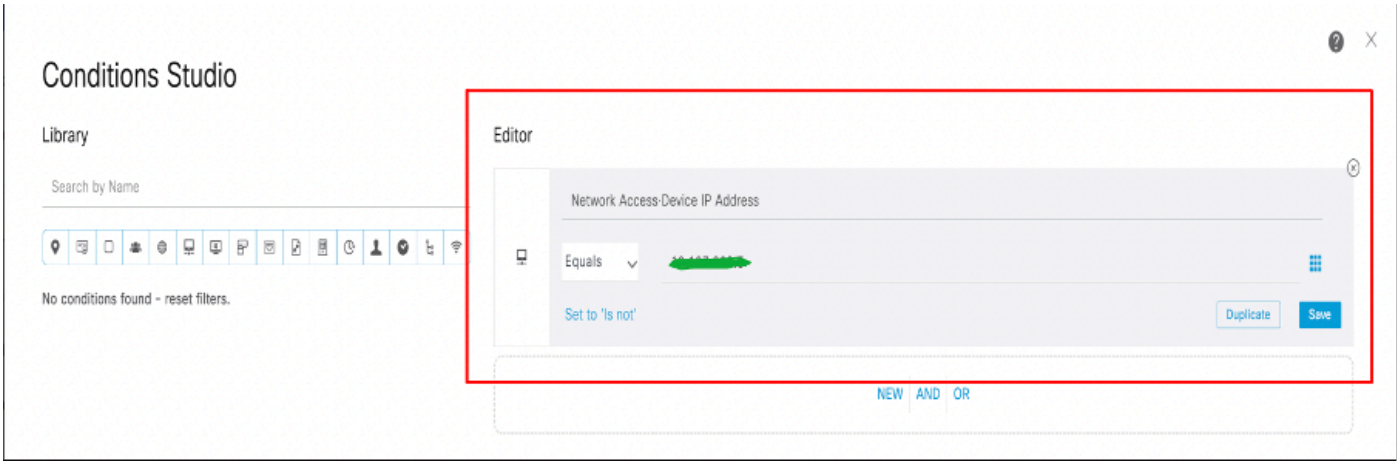
Configuratie van de beleidsset in ISE

2. Alvorens de beleidsset op te slaan, moet u de voorwaarden configureren, zoals in deze schermafbeelding wordt getoond. Klik op het pictogram + (plus) om de voorwaarden voor de beleidsset te configureren.

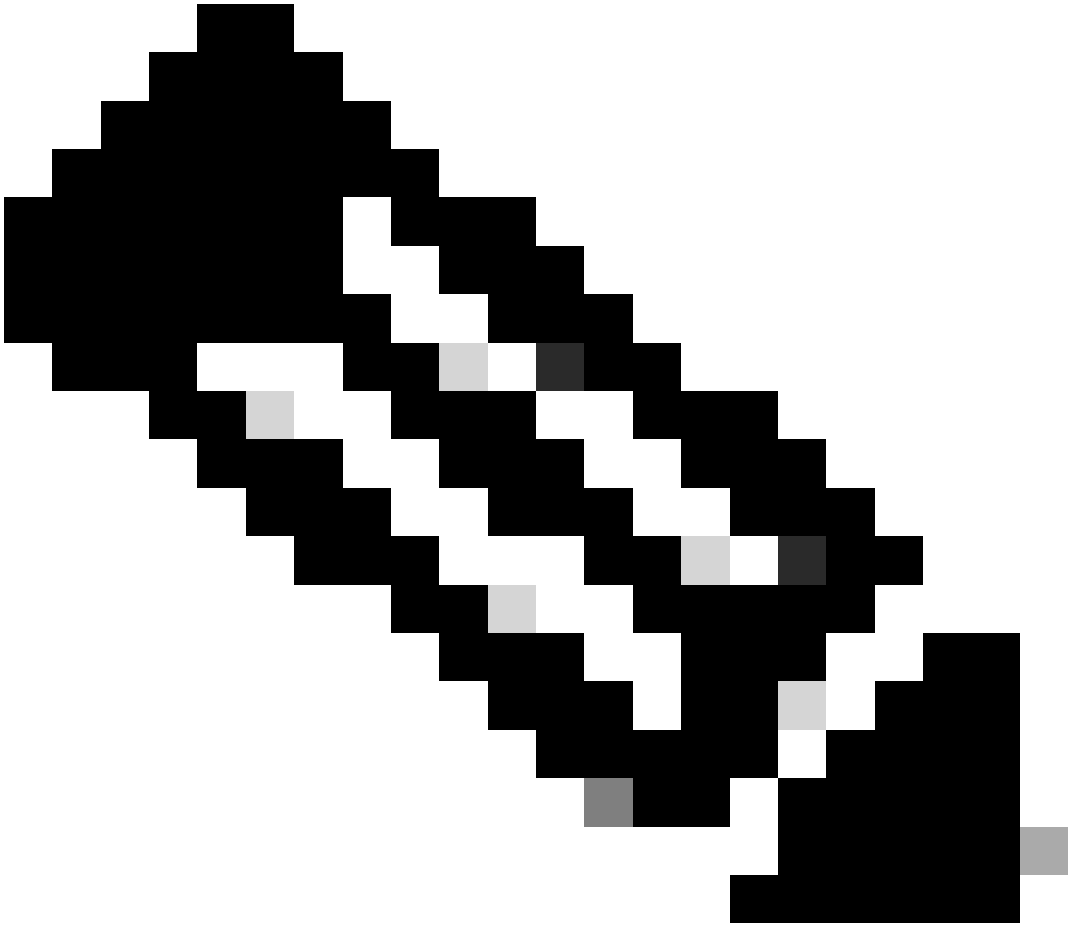


Configuratie van beleidsvoorwaarden in ISE

3. Nadat u op het pictogram + (plus) hebt geklikt zoals in stap 2 is aangegeven, wordt het dialoogvenster voorwaarden studio geopend. Daar, vorm de vereiste voorwaarden. Sla de voorwaarde met de nieuwe of bestaande voorwaarden, scrol op. Klik op Gebruik.



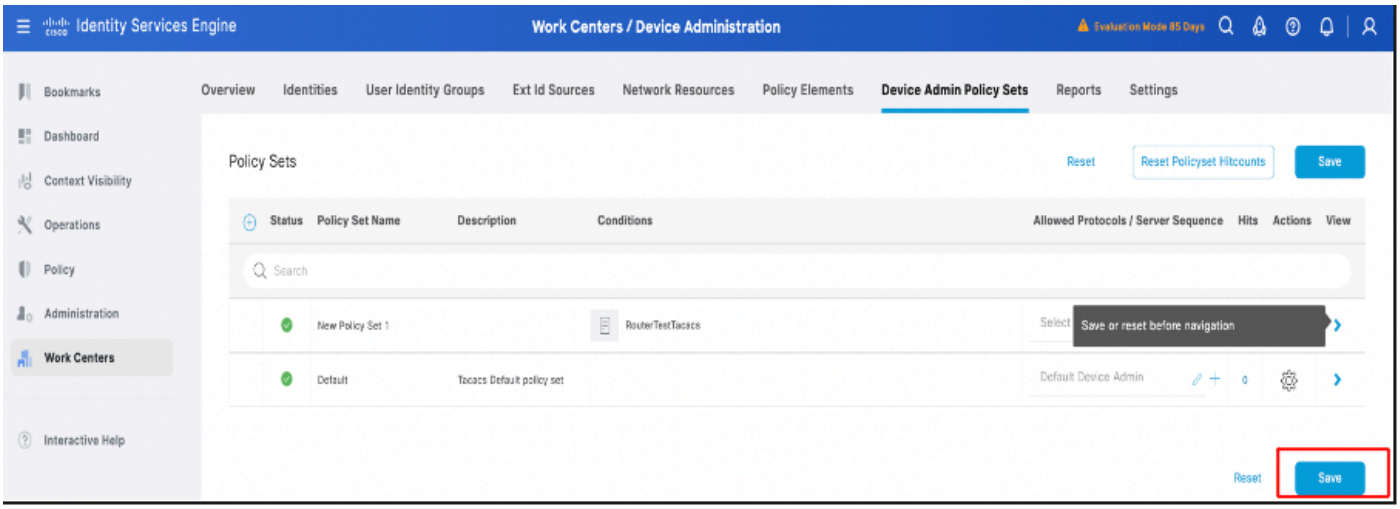
Configuratie van beleidsvoorwaarden in ISE



Opmerking: Voor deze documentatie worden de voorwaarden gekoppeld aan IP-adres van het netwerkapparaat. De voorwaarden kunnen echter worden aangepast aan de inzetvereisten.

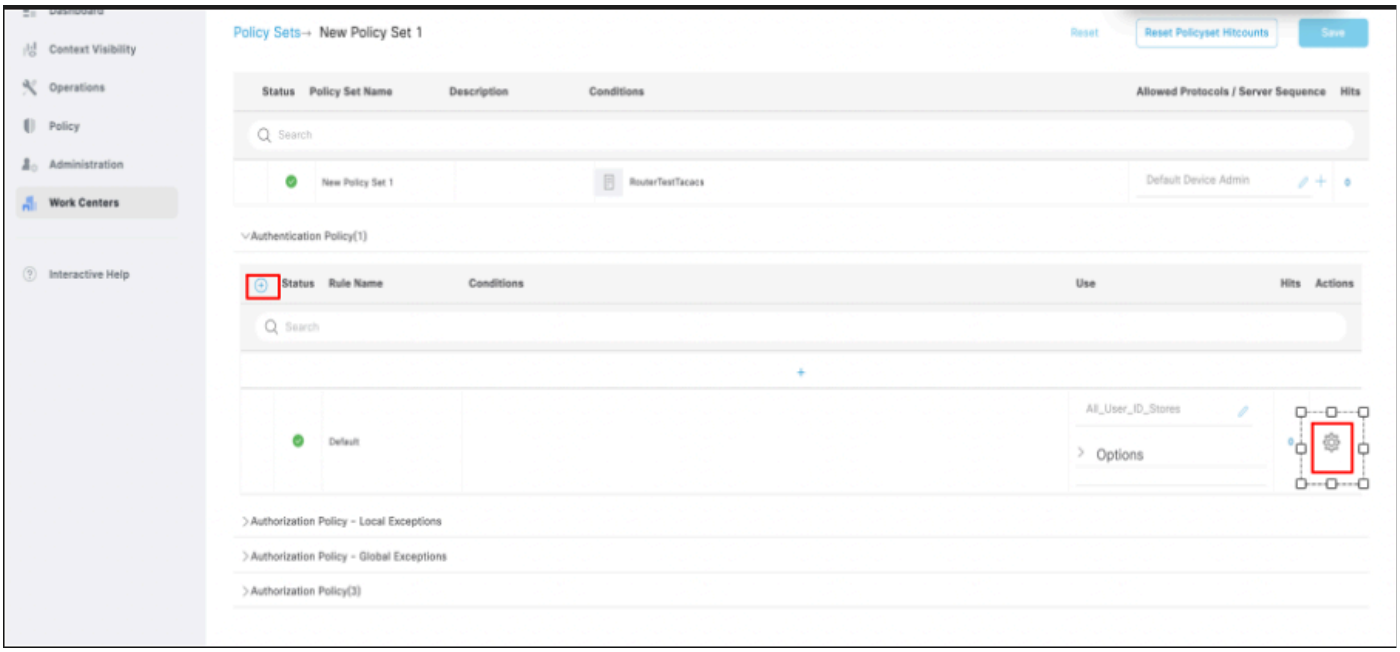
---

4. Nadat de voorwaarden zijn geconfigureerd en opgeslagen, configureer de toegestane protocollen als standaardapparaatbeheerder. Sla de beleidsset op die is gemaakt door op de optie Opslaan te klikken.

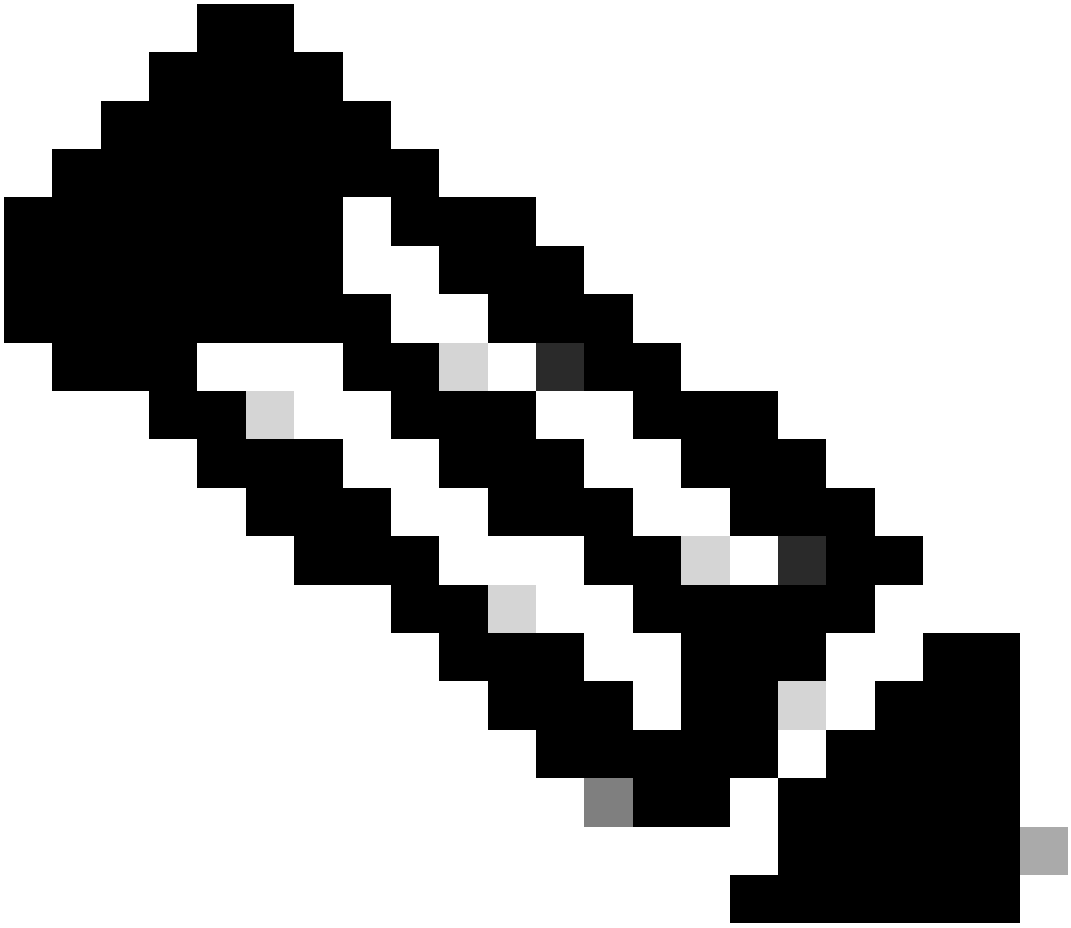


Bevestiging van de beleidsconfiguratie.

5. Breid de nieuwe beleidsset uit -> Verificatiebeleid (1) -> Maak een nieuw verificatiebeleid door op + (plus) pictogram te klikken of door op het tandwielpictogram te klikken, en voer vervolgens hierboven een nieuwe rij in.



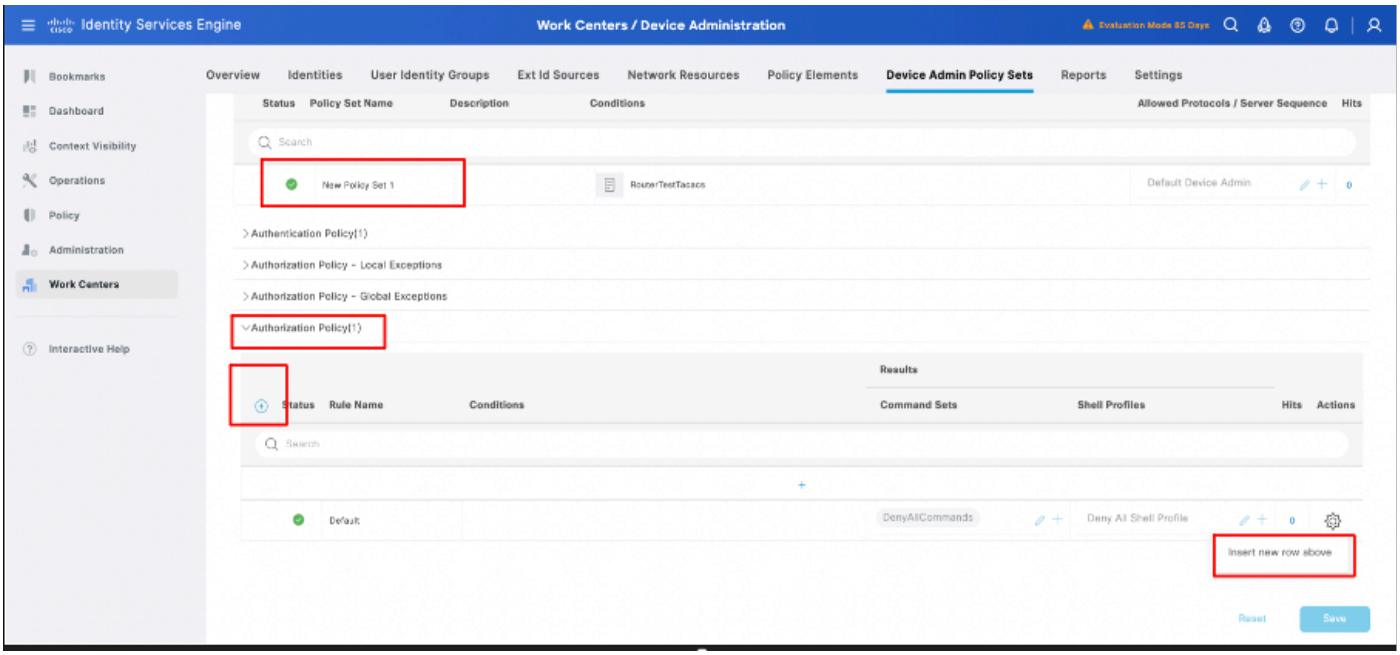
Configuratie van het verificatiebeleid in de beleidsset.



Opmerking: Voor deze demonstratie wordt het standaard verificatiebeleid gebruikt dat is ingesteld met All_User_ID_Stores. Het gebruik van de Identity stores is echter aanpasbaar volgens de implementatievereisten.

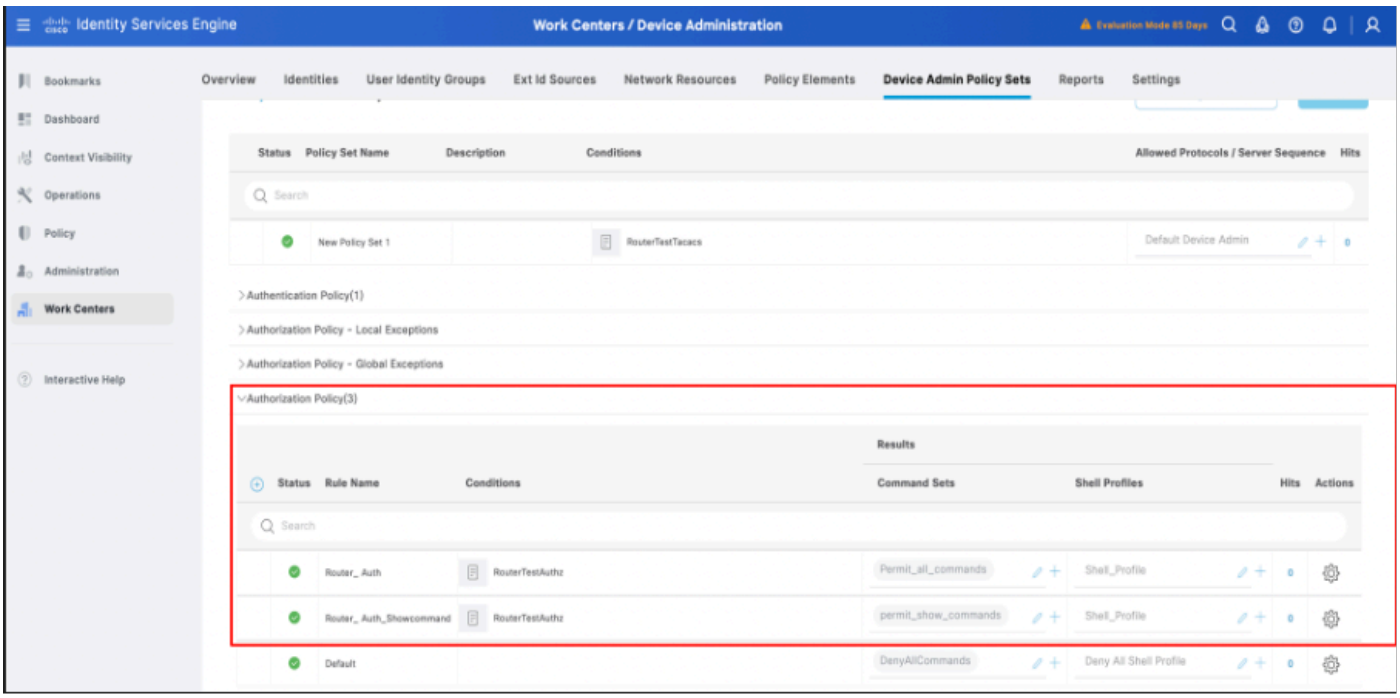
---

6. Breid de nieuwe beleidsset uit -> Autorisatiebeleid (1). Klik op het + (plus) pictogram of klik op het tandwielpictogram. Voeg vervolgens een nieuwe rij toe boven voor het maken van een autorisatiebeleid.

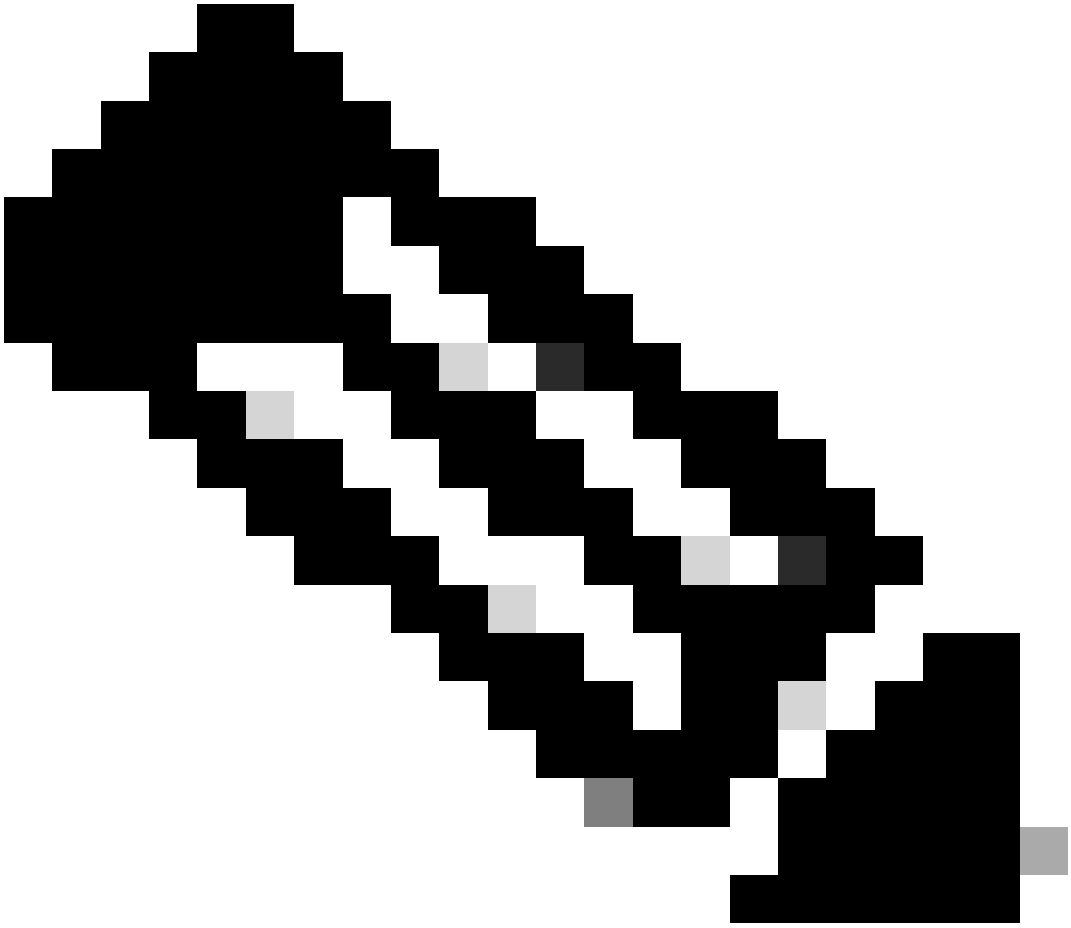


Configuratie van autorisatiebeleid

7. Configureer het autorisatiebeleid met de voorwaarden, opdrachtsets en shell-profiel die aan het autorisatiebeleid zijn toegewezen.



Volledige configuratie van het autorisatiebeleid in ISE



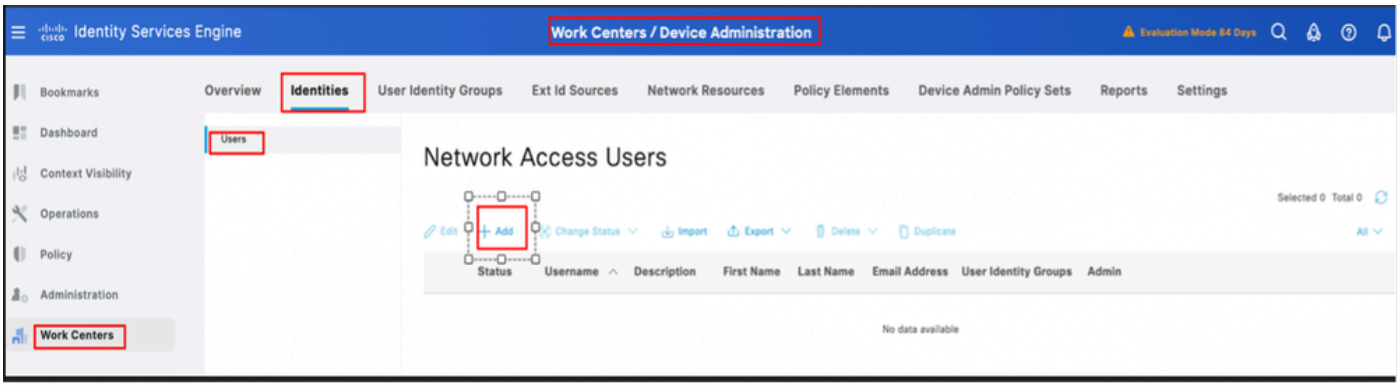
Opmerking: De omstandigheden die zijn ingesteld, zijn in overeenstemming met de laboratoriumomgeving en kunnen worden geconfigureerd volgens de implementatievereisten.

---

8. Volg de eerste 6 stappen voor het configureren van de beleidssets voor switch of een ander netwerkapparaat dat wordt gebruikt voor TACACS+.

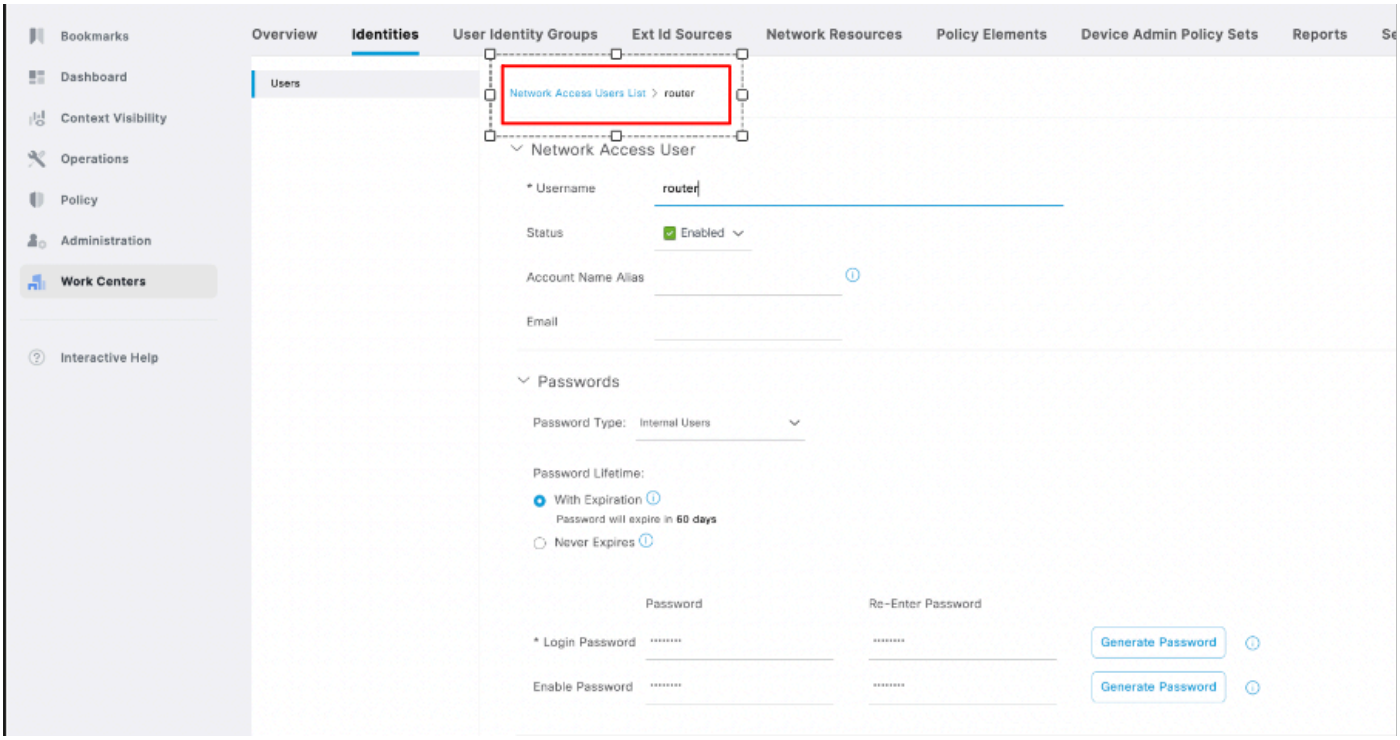
Gebruikers van netwerktoegang configureren voor TACACS-verificatie van NAD in ISE

1. Ga naar Workcenters -> Apparaatbeheer -> Identiteiten -> Gebruikers. Klik op het pictogram +(plus) om een nieuwe gebruiker te maken.



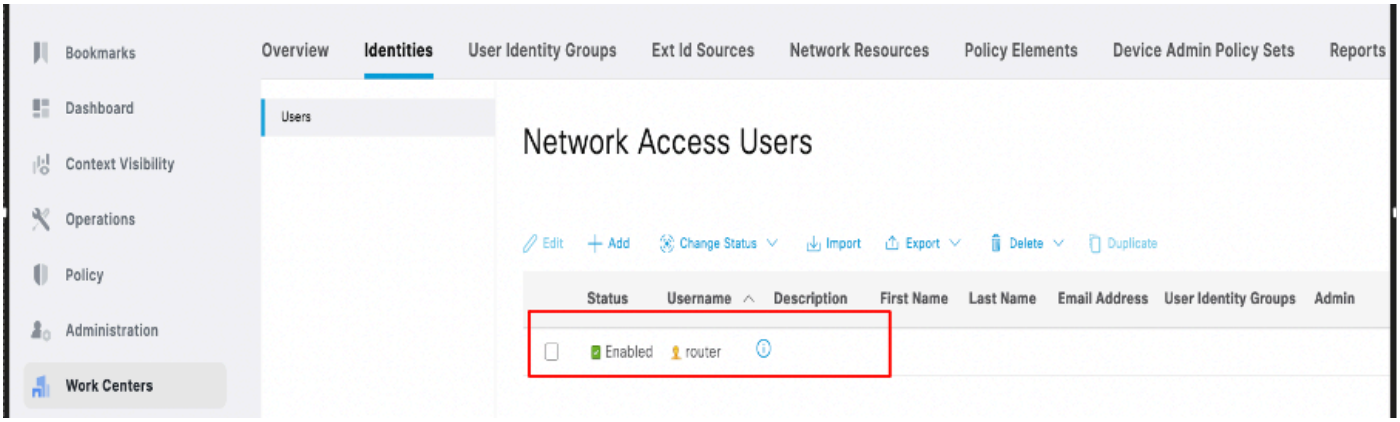
Configureer de gebruikers van netwerktoegang in ISE

2. Geef de gebruikersnaam en het wachtwoord op om deze uit te breiden, wijs de gebruiker toe aan een gebruikersgroep (optioneel) en klik vervolgens op Indienen.



Netwerktoegangsgebruikers configureren - Doorgaan

3. Nadat u de gebruikersnaam in de werkcentra hebt opgegeven -> Identiteiten -> Gebruikers -> Gebruikers van Network Access - wordt de gebruiker zichtbaar geconfigureerd en ingeschakeld.



Configureren router voor TACACS+

Cisco IOS-router voor TACACS+ verificatie en autorisatie configureren

1. Log in op de CLI van de router en voer deze opdrachten uit voor het configureren van TACACS in de router.

ASR 1001-X(configuratie)#aaa nieuw model — opdracht vereist voor inschakelen van AAA in NAD

ASR1001-X(configuratie)#aaa sessie-id gebruikelijk. —opdracht vereist om AAA in NAD in te schakelen.

ASR1001-X(configuratie)#aaa verificatie van de standaardgroep tacacs+ lokaal

ASR 1001-X(configuratie)#aaa-standaardgroep voor exec-tacacs+

ASR 1001-X(Config)#aaa netwerklijst met autorisatienetwerken1 groep-tacacs+

ASR 1001-X(configuratie)#tacacs-server ISE1

ASR1001-X (config-server-tacacs)#address ipv4 <IP-adres van TACACS-server > . — ISE-interface G1 IP-adres.

ASR 1001-X (config-server-tacacs)# toets XXXXX

ASR 1001-X (configuratie)# tac's+ voor een groepsserver

ASR 1001-X(config-sg-tacacs+)#server naam ISE1

ASR 1001-X (config-sg-tacacs+)#ip VRF-doorsturen MGMT-intf

ASR 1001-X (config-sg-tacacs+)#ip tacacs-bron-interface Gigabit Ethernet0

ASR 1001-X (config-sg-tacacs+)#ip tacacs-bron-interface Gigabit Ethernet1

ASR 1001-X (configuratie)#exit

2. Na het opslaan router TACACS+ configuraties, verifieer TACACS+ configuratie door de opdracht show run aaa te gebruiken.

ASR 1001-X#show run aaa

!

aaa verificatie login standaardgroep isegroep lokaal

Standaard aaa-autorisatie exec-groep isegroep

Netwerklijst voor aaa1-groep

gebruikersnaam beheerder wachtwoord 0 XXXXX

!

tacacs-server ise1

IP-adres4 <IP-adres van TACACS-server>

sleutel XXXXX

!

!

tacacs+ isegroep voor aaa-groepsserver

servernaam ise1

IP VRF-doorsturen MGMT-intf

IP-tacacs bron-interface Gigabit Ethernet1

!

!

!

aaa new-model

aaa sessie-id gemeenschappelijk

!

!

Switch voor TACACS+ configureren

Switch configureren voor TACACS+ verificatie en autorisatie

1. Log in op de CLI van de switch en voer deze opdrachten uit voor het configureren van TACACS in de switch.

C9200L-48P-4X#configureren

Voer configuratie-opdrachten in, één per lijn. Einde met CNTL/Z.

C9200L-48P-4X(configuratie)#aaa nieuw model. — opdracht vereist voor het inschakelen van AAA in NAD

C9200L-48P-4X(configuratie)#aaa sessie-id gebruikelijk. — opdracht vereist om AAA in NAD in te

schakelen.

C9200L-48P-4X(configuratie)#aaa verificatie inlognaam standaardgroep lokale groepen

C9200L-48P-4X(configuratie)#aaa-standaardinstelling van exec-groep

C9200L-48P-4X (configuratie)#aaa netwerklijst met autorisatienetwerken1 groepsgroep

C9200L-48P-4X(configuratie)#tacacs-server ISE1

C9200L-48P-4X (config-server-tacacs)#address ipv4 <IP-adres van TACACS-server> — ISE-interface G1 IP-adres.

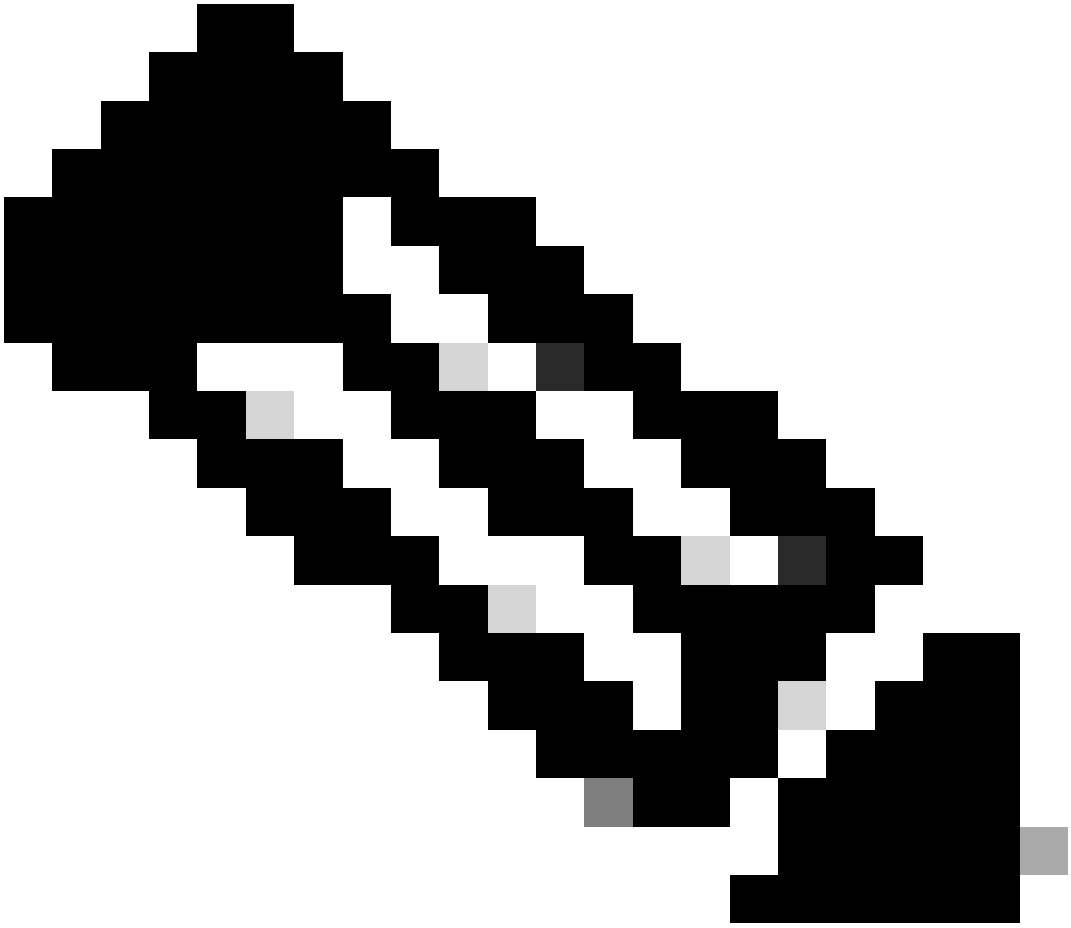
C9200L-48P-4X (config-server-tacacs)#key XXXXX

C9200L-48P(configuratie)#aaa-groepsserver, tacacs+ groep

C9200L-48P(config-sg-tacacs+)#server naam ISE1

C9200L-48P-4X(configuratie)#exit

C9200L-48P-4X#wr-mem



Opmerking: In de NAD TACACS+ configuratie is tacacs+ de groep die kan worden aangepast volgens de implementatievereisten.

---

2. Na het opslaan van de switch TACACS+ configuraties, verifieer TACACS+ configuratie door de opdracht show run aaa te gebruiken.

C9200L-48P#show run aaa

!

aaa verificatie login standaardgroep isegroep lokaal

Standaard aaa-autorisatie exec-groep isegroep

Netwerklijst voor aaa1-groep

gebruikersnaam beheerder wachtwoord 0 XXXXX

```
!

!

tacacs-server ise1

 IP-adres4 <IP-adres van TACACS-server>

 sleutel XXXXX

!

!

tacacs+ isegroep voor aaa-groepsserver

 servernaam ise1

!

!

!

aaa new-model

aaa sessie-id gemeenschappelijk

!

!
```

Verificatie

Verificatie via router

Van de CLI van de router, waarheidsauthenticatie van TACACS+ tegen ISE met Gigabit Ethernet 1 interface door de nieuwe opdracht van de gebruikersnaam van de testgroep tacacsgroupname te gebruiken.

Hier is de voorbeelduitvoer van Router & ISE:

Verificatie van poort 49 vanaf router:

ASR 1001-X#telnet ISE-gig 1-interface IP-telefoon 49

Probeert naar ISE GIg 1 interface IP, 49... Open (Openstaand)

ASR 1001-X#test aaa groep isegroup router XXXX nieuw

Wachtwoord verzenden

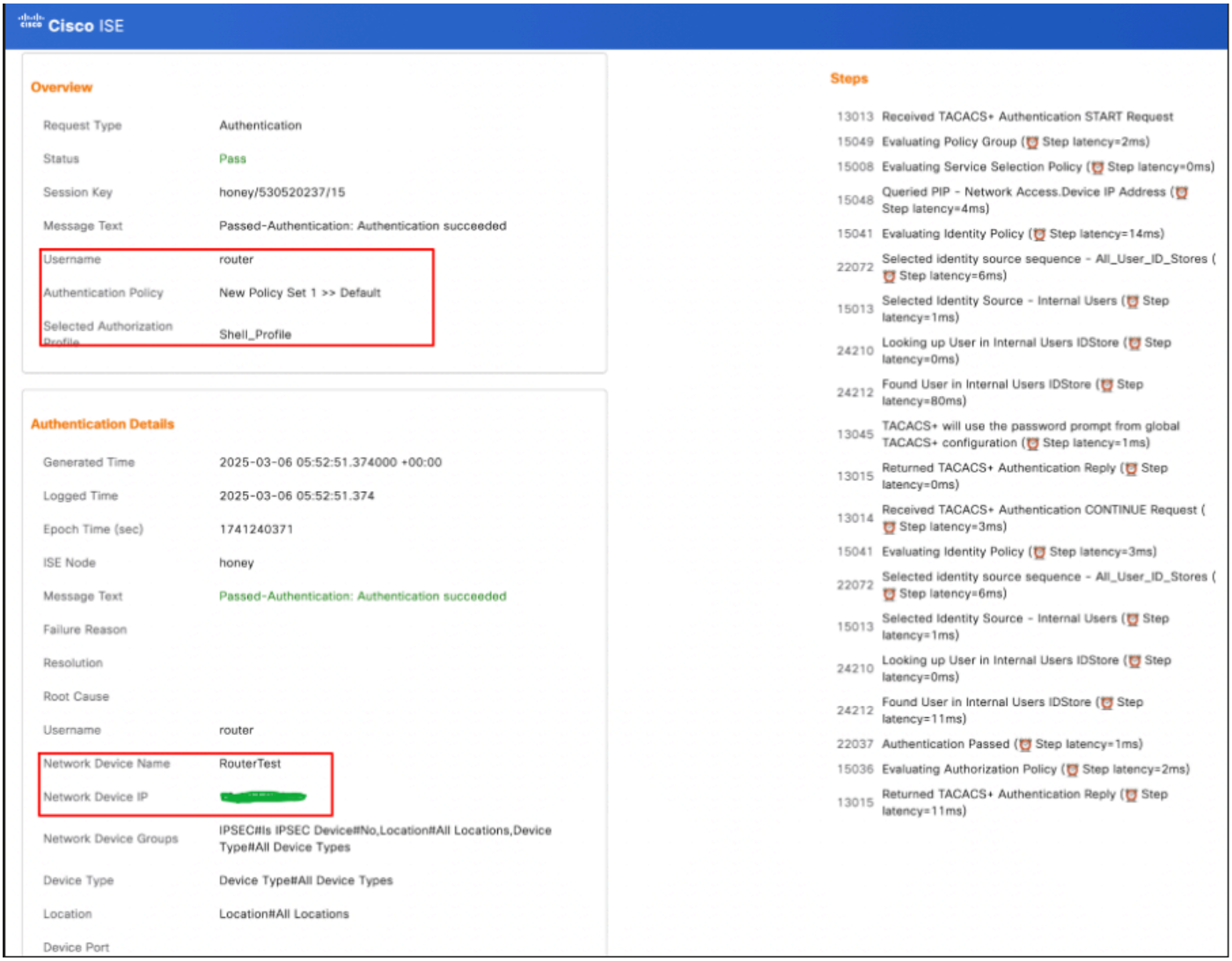
Gebruiker geverifieerd

GEBRUIKERSKENMERKEN

gebruikersnaam 0 "router"

antwoordbericht 0 "Wachtwoord:"

Voor verificatie vanaf ISE meldt u zich aan bij de GUI -> Operations -> Live Tacacs-logbestanden, en vervolgens filtert u met router IP in het veld Network Device Details.



Live Tacacs-logs van ISE - routerverificatie.

Verificatie van de Switch

Controleer vanuit de CLI van switch de verificatie van TACACS+ tegen ISE met Gigabit Ethernet 1-interface met behulp van de nieuwe opdracht voor gebruikersnaam en wachtwoord voor testgroep tacacs Group:

Hier is voorbeelduitvoer van switch & ISE.

Controle van haven 49 vanaf switch:

C920L-48P# telnet ISE-Gig1-interface IP-telefoon 49

Probeer ISE Gig1 interface IP, 49... Open (Openstaand)

C9200L-48P#test aaa groep isegroep switch XXXX nieuw

Wachtwoord verzenden

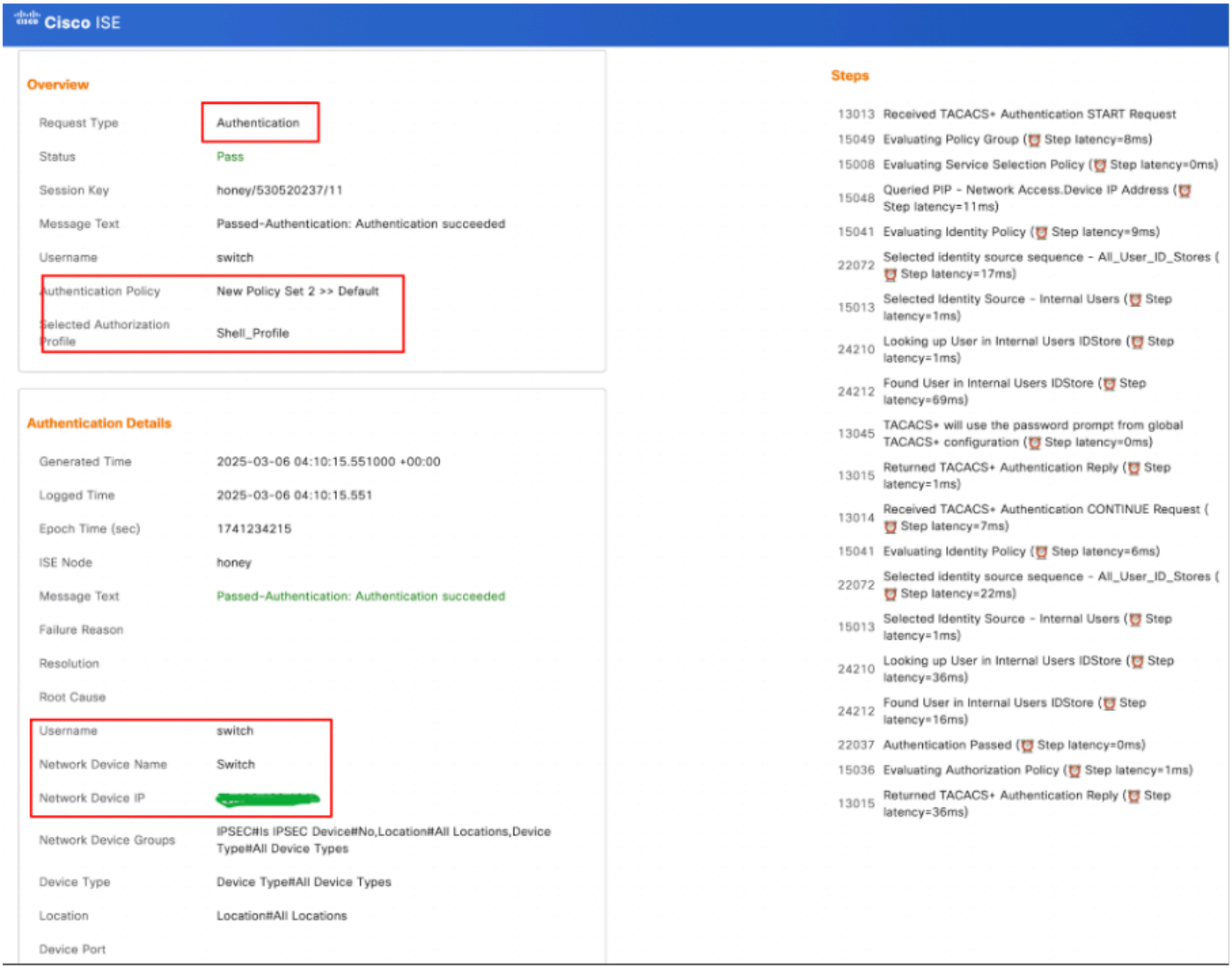
Gebruiker geverifieerd

GEBRUIKERSKENMERKEN

gebruikersnaam 0 "switch"

antwoordbericht 0 "Wachtwoord:"

Log voor verificatie van ISE in op de GUI -> Operations -> Live Tacacs-logbestanden, en filter vervolgens met switch IP in het veld Netwerkapparaatgegevens.



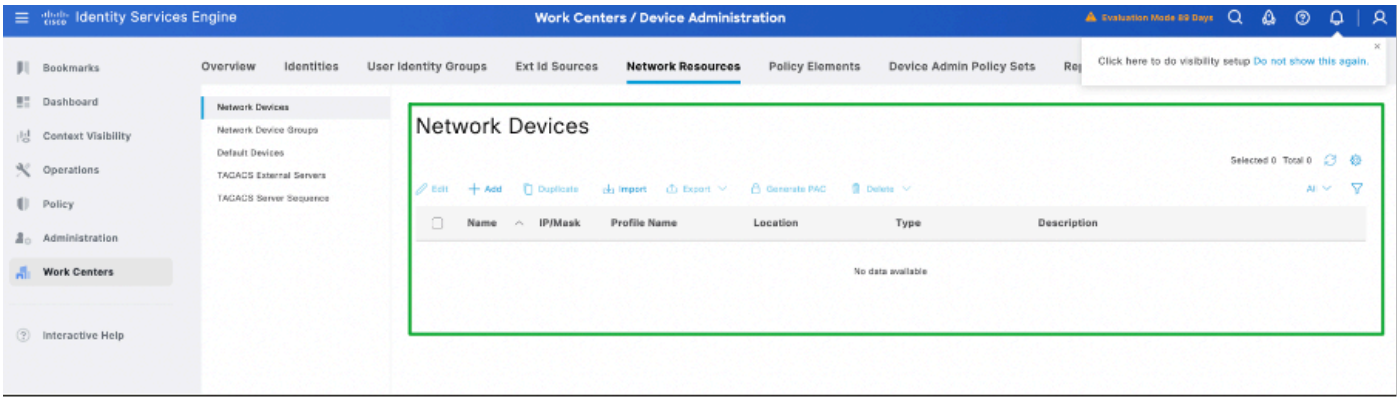
Tacacs live logs van ISE - Switch verificatie.

Problemen oplossen

In dit gedeelte worden enkele veel voorkomende problemen met betrekking tot TACACS+-verificaties besproken.

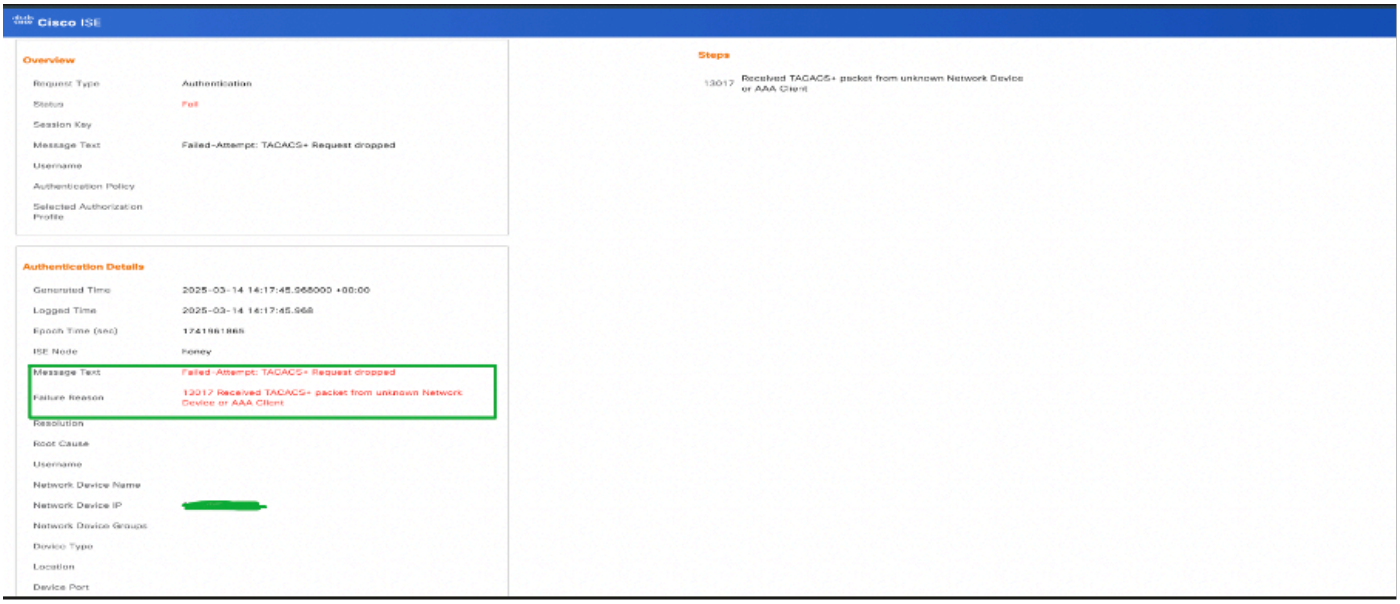
Scenario 1: De authenticatie van TACACS+ mislukt met "Fout: 13017 Ontvangen TACACS+ pakket van onbekend netwerkapparaat of AAA-client".

Dit scenario treedt op wanneer het netwerkapparaat niet wordt toegevoegd als netwerkbronnen in ISE. Zoals in deze screenshot wordt getoond, wordt de switch niet toegevoegd aan de netwerkbronnen van ISE.



Probleemoplossing - Netwerkapparaten worden niet toegevoegd in ISE.

Wanneer u nu de verificatie vanaf de switch / het netwerkapparaat test, bereikt het pakket ISE zoals verwacht. De verificatie mislukt echter met de fout "Fout: 13017 Ontvangen TACACS+ pakket van onbekend netwerkapparaat of AAA-client" zoals in deze screenshot:



Levende logboeken TACACS - Mislukking wanneer het netwerkapparaat niet aan ISE wordt toegevoegd.

Verificatie via het netwerkapparaat (Switch)

Switch #test aaa groep isegroup switch XXXXXX nieuw
Gebruiker geweigerd

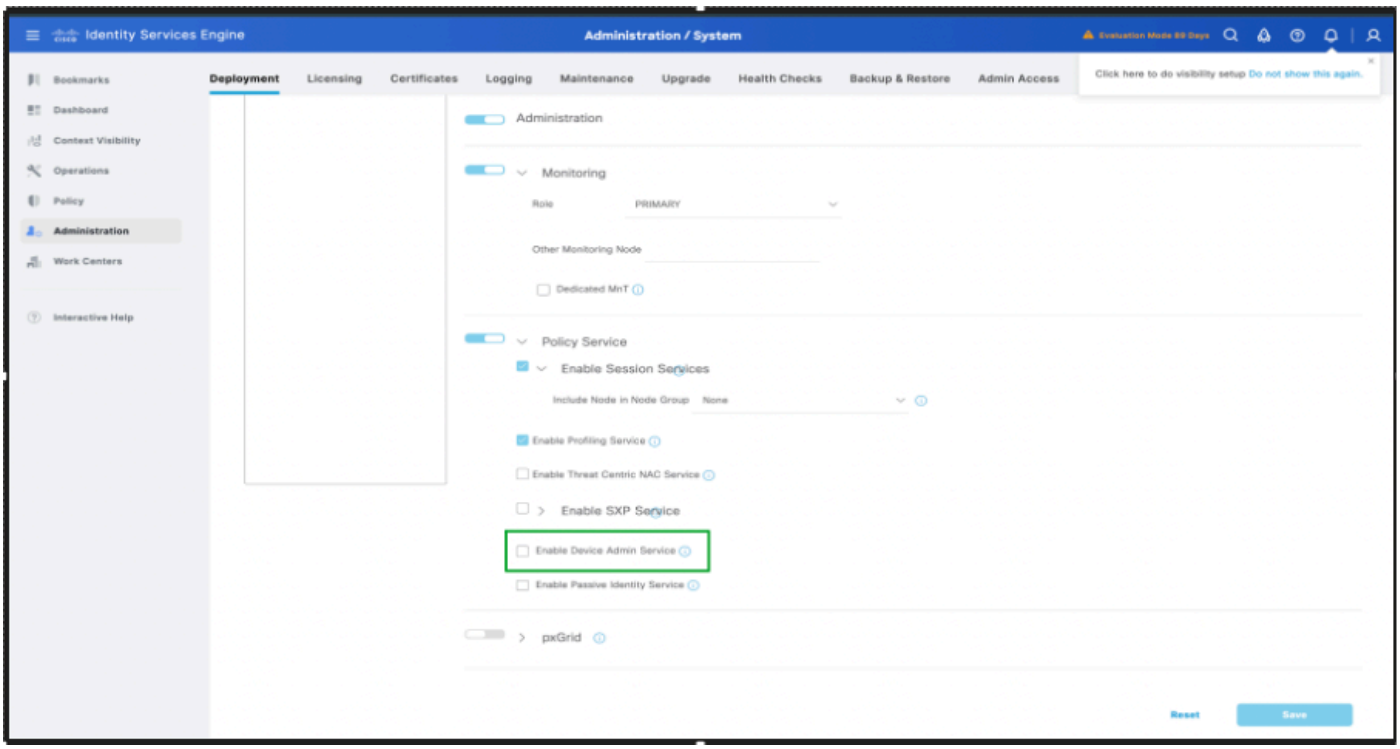
Oplossing: Controleer of de switch / router / het netwerkapparaat is toegevoegd als het

netwerkapparaat in ISE. Als het apparaat niet wordt toegevoegd, voegt u het netwerkapparaat toe aan de lijst met netwerkapparaten van ISE.

Scenario 2: ISE laat het TACACS+ pakket stil vallen zonder enige informatie.

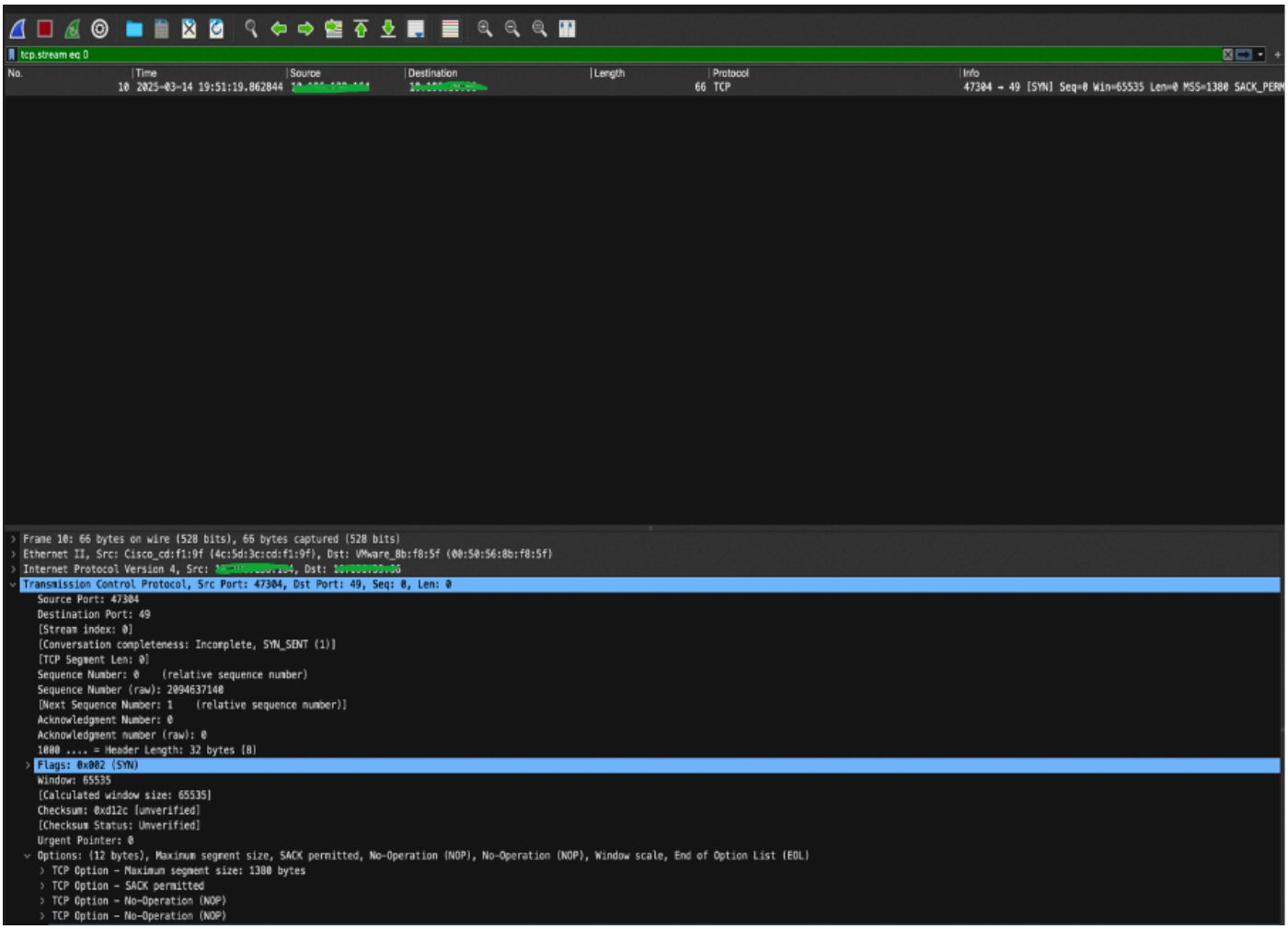
Dit scenario komt voor wanneer de Dienst van het Apparaatbeheer in ISE onbruikbaar wordt gemaakt. In dit scenario wordt het pakket door ISE verlaagd en worden geen actieve logbestanden weergegeven, ook al wordt de verificatie gestart vanaf het netwerkapparaat dat wordt toegevoegd aan de netwerkbronnen van ISE.

Zoals in deze screenshot wordt getoond, is Apparaatbeheer uitgeschakeld in ISE.



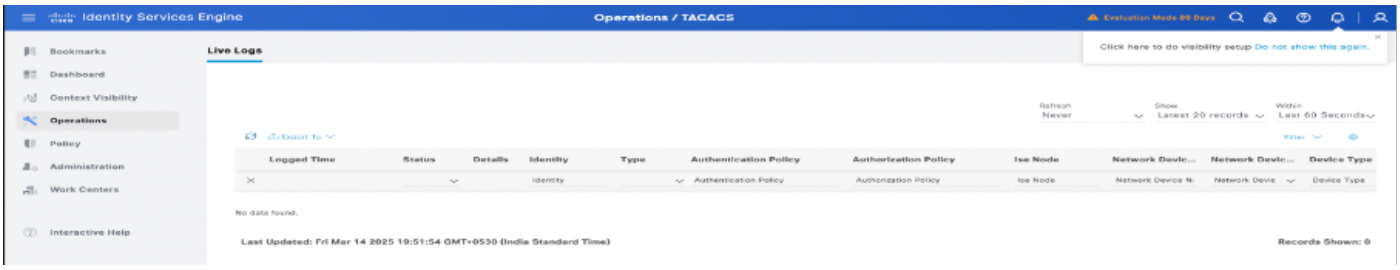
Scenario, het apparatenbeleid wordt niet toegelaten in ISE.

Wanneer een gebruiker de verificatie vanaf het netwerkapparaat initieert, laat ISE de pakketten stilzwijgend vallen zonder enige informatie in de bewegende logbestanden en ISE reageert niet op het Syn-pakket dat door het netwerkapparaat wordt verzonden om het TACACS-verificatieproces te voltooien. Raadpleeg deze screenshot:



ISE-droppingspakketten in stilte tijdens TACACS

ISE verschijnt tijdens de verificatie geen actieve logbestanden.



Geen levende logbestanden TACACS - Verificatie via ISE

Verificatie via het netwerkapparaat (Switch)

Switch#
Switch #test aaa groep isegroup switch XXXX nieuw
Gebruiker geweigerd
Switch#
*14 mrt. 13.54:28.144: T+: Versie 192 (0xC0), type 1, vervolg 1, encryptie 1, SC 0
*14 mrt. 13.54:28.144: T+: Session_id 10158877 (0x9B031D), Dlen 14 (0xE)
*14 mrt. 13.54:28.144: T+: type:AUTHEN/START, priv_lvl:15 actie:LOGIN ascii
*14 mrt. 13.54:28.144: T+: svc:LOGIN user_len:6 port_len:0 (0x0) radr_len:0 (0x0) data_len:0
*14 mrt. 13.54:28.144: T+: gebruiker: switch
*14 mrt. 13.54:28.144: T+: port:
*14 mrt. 13.54:28.144: T+: rem_addr:
*14 mrt. 13.54:28.144: T+: gegevens:
*14 mrt. 13.54:28.144: T+: Eindpakket

Oplossing: Schakel Apparaatbeheer in ISE in.

Referentie

- Problemen met TACACS-verificatie oplossen
- Beheerdershandleiding voor Cisco Identity Services Engine, release 3.3
- VRF voor TACACS-servers

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.