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

# Inhoud

| Inleiding  |
|--|
| Voorwaarden                                      |
| Vereisten  |
| Gebruikte componenten                            |
| Achtergrondinformatie                            |
| Configureren                                     |
| Netwerkdiagram                                   |
| Stap 1: Nexus 9000 configureren                  |
| Stap 2. Identity Service Engine 3.2 configureren |
| Verifiëren                                       |
| Problemen oplossen                               |

# 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



Flow Components Diagram

### Stap 1: Nexus 9000 configureren

#### 1. AAA-configuratie.



Waarschuwing: nadat u de TACACS-verificatie hebt ingeschakeld, stopt het Nexusapparaat 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
                                      permit interface Ethernet1/9
Nexus9000(config-role-interface)#
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
                                      permit interface Ethernet1/29
Nexus9000(config-role-interface)#
Nexus9000(config-role-interface)#
                                      permit interface Ethernet1/30
```

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.

| ≡   | С      | isco     | ISE           |                 | Administr      | ration • Identity Managemen   | A Evaluation Mode 29 Days | Q      | 0 | Q | ٩ |  |
|-----|--------|----------|---------------|-----------------|----------------|-------------------------------|---------------------------|--------|---|---|---|--|
| lde | ntitie | es       | Groups        | External Ide    | entity Sources | Identity Source Sequences     | Settings                  |        |   |   |   |  |
|     | ldenti | ity Grou | ıps           |                 |                | ups > New User Identity Group |                           |        |   |   |   |  |
|     | ΞQ     |          |               |                 | Identity Grou  | up                            |                           |        |   |   |   |  |
|     | < E Ø  |          |               | 🕸<br>ity Groups | * Name         | iseUsers                      |                           |        |   |   |   |  |
|     |        | 🗀 Us     | er Identity G | iroups          | Description    |                               |                           |        |   |   |   |  |
|     |        |          |               |                 |                | (                             | Submit                    | Cancel |   |   |   |  |

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.

| Network Access Users List > New Network Access User |           |   |  |  |  |  |  |  |  |  |  |
|---|-----------|---|--|--|--|--|--|--|--|--|--|
| ✓ Network Access User                               |           |   |  |  |  |  |  |  |  |  |  |
| * Username  | iseiscool |   |  |  |  |  |  |  |  |  |  |
| Status  | Enabled   |   |  |  |  |  |  |  |  |  |  |
| Account Name Alias                                  |           |   |  |  |  |  |  |  |  |  |  |
| Email   |           | - |  |  |  |  |  |  |  |  |  |

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.

| ✓ Passwords   |                 |                   |                   |   |
|---|-----------------|-------------------|-------------------|---|
| Password Type:  | Internal Users  |                   |                   |   |
| Password Lifetime   | :               |                   |                   |   |
| <ul> <li>With Expiration</li> <li>Password will ex</li> </ul> | pire in 60 days |                   |                   |   |
| O Never Expires   |                 |                   |                   |   |
|   |                 |                   |                   |   |
|   | Password        | Re-Enter Password |                   |   |
| * Login Password  |                 |                   | Generate Password | 0 |
| Enable Password   |                 |                   | Generate Password | 0 |
|   |                 |                   |                   |   |

Wachtwoordtoewijzing

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

| ∨ Use | er Groups |   |   |
|-------|-----------|---|---|
| :     | iseUsers  | ~ | ۱ |

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.

| Network Devices          |                     |                |            |
|--------------------------|---------------------|----------------|------------|
|                          |                     |                | Selected 0 |
| 🖉 Edit 🕂 Add 🗓 Duplicate | 山 Import 🏦 Export 〜 | 🔒 Generate PAC | 🗑 Delete 🗸 |
| 🗌 Name \land IP/Mask     | Profile Name        | Location       | Туре       |

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.

| ≡ Cisco ISE             | Work Centers · Device A                   | dministration     | 🛕 Evaluation Mode 27 Days Q 🔗 😼 🕻 |             |  |  |  |  |  |
|-------------------------|---|-------------------|-----------------------------------|-------------|--|--|--|--|--|
| Overview Identities     | User Identity Groups Ext Id Sources       | Network Resources | Policy Elements                   | More $\vee$ |  |  |  |  |  |
| Network Devices         | Network Devices List > New Network Device |                   |                                   |             |  |  |  |  |  |
| Network Device Groups   | Network Devices                           |                   |                                   |             |  |  |  |  |  |
| Default Devices         |   |                   |                                   |             |  |  |  |  |  |
| TACACS External Servers | Name NEXUS9K                              |                   |                                   |             |  |  |  |  |  |
| TACACS Server Sequence  | Description Nexus Device For TA           | CACS              |                                   |             |  |  |  |  |  |
|                         |   |                   |                                   |             |  |  |  |  |  |
|                         | IP Address V * IP :                       | A.B.C.D / 32      |                                   |             |  |  |  |  |  |
|                         |   |                   |                                   |             |  |  |  |  |  |
|                         | Device Profile Eisco                      |                   |                                   |             |  |  |  |  |  |
|                         | Model Name                                |                   |                                   |             |  |  |  |  |  |
|                         | Software Version                          |                   |                                   |             |  |  |  |  |  |
|                         | Network Device Group                      |                   |                                   |             |  |  |  |  |  |

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.

| ≡ Cisco ISE         | Work Centers · Device Ad            | ministration                 | 🛕 Evaluation Mode 27 Days 🔾 🧑 🕫 전 |   |  |  |  |  |
|---------------------|-------------------------------------|------------------------------|-----------------------------------|---|--|--|--|--|
| Overview Identities | User Identity Groups Ext Id Sources | Network Resources            | Policy Elements More V            |   |  |  |  |  |
| Conditions          | > TACACS Profiles                   |                              |                                   |   |  |  |  |  |
| Network Conditions  |                                     |                              |                                   |   |  |  |  |  |
| Results             |                                     | Rows/Page                    |                                   | 8 |  |  |  |  |
| Allowed Protocols   | 🛱 🗚 Duplicate Trash 🗸 Edit          |                              |                                   |   |  |  |  |  |
| TACACS Command Sets |                                     |                              |                                   |   |  |  |  |  |
| TACACS Profiles     | Name Name                           | Type Description             |                                   |   |  |  |  |  |
|                     | Default Shell Profile               | Shell Default Shell Profile  |                                   |   |  |  |  |  |
|                     | Deny All Shell Profile              | Shell Deny All Shell Profile |                                   |   |  |  |  |  |

TACACS-profiel

Wijs een Naam, en naar keuze een beschrijving toe.

| ≡ Cisco ISE         | Work Centers · Device Admini                           | stration 🔺                       | ivaluation Mode 27 Days 🔾 ၇ 🕫 🛱 |
|---------------------|--|----------------------------------|---------------------------------|
| Overview Identities | User Identity Groups Ext Id Sources No                 | etwork Resources Policy Elements | More $\vee$                     |
| Conditions          | > TACACS Profiles > New<br>TACACS Profile              |                                  |                                 |
| Network Conditions  |  |                                  |                                 |
| Results             | Name<br>V Nexus Helpdesk                               |                                  |                                 |
| Allowed Protocols   |  |                                  |                                 |
| TACACS Command Sets |  |                                  |                                 |
| TACACS Profiles     | Description<br>This TACACS profile will be sent if the |                                  |                                 |
|                     | user is part of the helpdesk team                      |                                  |                                 |
|                     | group  |                                  |                                 |

Tacacs-profiel benoemen

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

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

| ≡ Cisco           | ISE                  |    | Work Ce                                      | enters · Device Ac                     | 🛕 Eva             | 🛕 Evaluation Mode 27 Days Q 🔗 💭 |             |  |  |  |  |
|-------------------|----------------------|----|--|--|-------------------|---------------------------------|-------------|--|--|--|--|
| Overview          | Identities           | Us | er Identity Groups                           | Ext Id Sources                         | Network Resources | Policy Elements                 | More $\vee$ |  |  |  |  |
|                   |                      |    | Name   |  |                   |                                 |             |  |  |  |  |
| Conditions        |                      |    | Nexus Helpdesk                               |  |                   |                                 |             |  |  |  |  |
| Network Condition | Network Conditions > |    | Description                                  |  |                   |                                 |             |  |  |  |  |
| Results           |                      |    | This TACACS profile<br>user is part of the h | e will be sent if the<br>nelpdesk team |                   |                                 |             |  |  |  |  |
| Allowed Protoco   | ols                  |    | group  | ۰                                      |                   |                                 |             |  |  |  |  |
| TACACS Comm       | and Sets             |    |  |  |                   |                                 |             |  |  |  |  |
| TACACS Profile:   | \$                   |    | Task Attribute View                          | Raw View                               |                   |                                 |             |  |  |  |  |
|                   |                      |    | Profile Attributes                           |  |                   |                                 |             |  |  |  |  |
|                   |                      |    | shell:roles="helpde                          | sk"                                    |                   |                                 |             |  |  |  |  |
|                   |                      |    |  |  | Cancel            | Save                            |             |  |  |  |  |
|                   |                      |    |  |  |                   |                                 |             |  |  |  |  |
|                   |                      |    |  |  |                   |                                 |             |  |  |  |  |

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.

| ≡ C     | Cisco  | ISE          |               | Work Cer       | nters · Devic | e Adm  | inistration     |       |                 | 🛕 Evalua | ation Mode 2 | 7 Days | Q (0)  | Q      | ٩ |
|---------|--------|--------------|---------------|----------------|---------------|--------|-----------------|-------|-----------------|----------|--------------|--------|--------|--------|---|
| Overvie | €w     | Identities   | User Identity | Groups         | Ext Id Sourc  | es     | Network Resourc | es    | Policy Eleme    | ents     | More 🗸       |        |        |        |   |
| Policy  | Sets   |              |               |                |               |        |                 |       | Reset           | Reset    | Policyset Hi |        |        | Save   |   |
|         | Status | Policy Set N | lame          | Description    |               | Condit | ions            | Allow | ved Protocols ( | Server   | Sequence     | Hits   | Action | s Viev | w |
| Q       |        |              |               |                |               |        |                 |       |                 |          |              |        |        |        |   |
|         |        |              |               |                |               |        |                 |       |                 |          |              |        |        |        |   |
|         | 0      | Default      |               | Tacacs Default | policy set    |        |                 | Defa  | ault Device Adn |          |              |        | ŝ      | >      | ] |
|         |        |              |               |                |               |        |                 |       |                 |          |              |        |        |        |   |
|         |        |              |               |                |               |        |                 |       |                 |          |              | Reset  |        | Save   |   |

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.

| ≡ Cisco ISE |                    |             |               | Wo         | rk Ce | nters · Device Adr       | <u>▲</u> Ev         | valuation Mode 27 Days | Q                        | 0           | Q   | ٢ |        |   |
|-------------|--------------------|-------------|---------------|------------|-------|--------------------------|---------------------|------------------------|--------------------------|-------------|-----|---|--------|---|
| 0           | verview            | Identities  | User Identity | Grou       | ps    | Ext Id Sources           | Network Resources   | Polic                  | cy Elements              | More $\vee$ |     |   |        |   |
|             | + Status Rule Name |             |               | Conditions |       |                          |                     |                        | 9                        |             | Hit | s | Action | 5 |
|             | Q Se               |             |               |            |       |                          |                     |                        |                          |             |     |   |        |   |
|             |                    |             |               |            |       |                          |                     | Ir                     | nternal Users            | I           |     |   |        |   |
|             |                    |             |               |            |       |                          |                     |                        | Options                  |             |     |   |        |   |
|             |                    |             |               | ₽ Ne       | _     |                          |                     |                        | If Auth fail<br>REJECT   |             |     |   |        |   |
|             | ¢                  | Internal Au | thentication  |            | Netwo | ork Access-Device IP Add | ress EQUALS A.B.C.D |                        | If User not fo<br>REJECT | und         |     |   | ŝ      |   |
|             |                    |             |               |            |       |                          |                     |                        | If Process fai           | 1           |     |   |        |   |
|             |                    |             |               |            |       |                          |                     |                        |                          |             |     |   |        |   |
|             |                    |             |               |            |       |                          |                     | A                      | II_User_ID_St            |             |     |   |        |   |
|             | •                  | Default     |               |            |       |                          |                     |                        | Options                  |             |     |   | ŝ      |   |

Verificatiebeleid

Dit is hoe de situatie was ingesteld.

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

| Conditions Studio |       |      |                      |                        |    |      |   | Ø    |
|-------------------|-------|------|----------------------|------------------------|----|------|---|------|
| ibrary            |       | Edit | or                   |                        |    |      |   |      |
| Search by Name    |       |      | Network Acce         | ss-Device IP Address   |    |      |   |      |
|                   | 91917 |      | t attribute for cond |                        |    |      |   |      |
| EAP-MSCHAPv2      |       | •    | • 🖵                  | e 2                    | Q  | 1    | Ŀ | Save |
| 🗄 🗐 EAP-TLS       |       |      | Dictionary           | Attribute              | ID | Info |   |      |
|                   |       |      | All Dictionaries 🗡   | Attribute              | ID |      |   |      |
|                   |       | ₽    | DEVICE               | Device Type            |    |      |   |      |
|                   |       | ₽    | DEVICE               | Model Name             |    |      |   |      |
|                   |       | R    | DEVICE               | Network Device Profile |    |      |   |      |
|                   |       | ₽    | DEVICE               | Software Version       |    |      |   |      |
|                   |       |      | Network Access       | Device IP Address      | ]  |      |   |      |
|                   |       | ₽    | Network Access       | NetworkDeviceName      |    |      |   |      |
|                   |       |      |                      |                        |    |      |   | Use  |

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

| Conditions Studio          |               |        |                |                                  |       | 0       | × |
|----------------------------|---------------|--------|----------------|----------------------------------|-------|---------|---|
| Library                    |               | Editor |                |                                  |       |         |   |
| Search by Name             | earch by Name |        | Network Access | s-Device IP Address              |       | 8       |   |
| ♥☐ □ ♣ € 및 ⋢ ₽ ₪ ዸ ≣ € 1 € | ) t; 💎        | Ģ      | Equals 🗸       | <nexus address="" ip=""></nexus> |       |         |   |
| EAP-MSCHAPv2               |               |        |                |                                  |       | address |   |
| 🗄 🖪 EAP-TLS                |               |        |                |                                  |       | te Save |   |
|                            |               |        |                | NEW AND OF                       |       |         |   |
|                            |               |        |                |                                  |       |         |   |
|                            |               |        |                |                                  |       |         |   |
|                            |               |        |                |                                  |       |         |   |
|                            |               |        |                |                                  |       |         |   |
|                            |               |        |                |                                  |       |         |   |
|                            |               |        |                |                                  | Close | Use     |   |

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.

|      | Cisco ISE Work Centers - C |   |          |                  |         |                    |            | Iministration | 🛕 Evaluation Mode 27 Days Q 🕐 🔓 |       |              |               |          | )<br>2 | 1     |       |      |
|------|----------------------------|---|----------|------------------|---------|--------------------|------------|---------------|---------------------------------|-------|--------------|---------------|----------|--------|-------|-------|------|
| Over | view                       | Identi                                    | ies      | User Identity    | Groups  | Ext Id Sources     | Netwo      | rk Resources  | Policy Ele                      | ments | Device A     | dmin Policy   | Sets     | More   | e ~   |       |      |
|      | Sta                        | atus P                                    | olicy Se | t Name           | Descrip | tion               | Conditions |               |                                 |       |              | Allowed Pro   | tocols / | Server | Seque | nce   | Hits |
|      | Q                          |   |          |                  |         |                    |            |               |                                 |       |              |               |          |        |       |       |      |
|      |                            | 0   | Default  |                  | Tacacs  | Default policy set |            |               |                                 |       |              | Default Dev   | vice Adm |        |       |       |      |
|      | > Auth                     | enticatio                                 | n Policy | (2)              |         |                    |            |               |                                 |       |              |               |          |        |       |       |      |
|      | > Auth                     | > Authorization Policy - Local Exceptions |          |                  |         |                    |            |               |                                 |       |              |               |          |        |       |       |      |
|      | > Auth                     | orization                                 | Policy - | Global Exception | ons     |                    |            |               |                                 |       |              |               |          |        |       |       |      |
|      | ∨ Auth                     | orization                                 | Policy ( | 1)               |         |                    |            |               |                                 |       |              |               |          |        |       |       |      |
|      |                            |   |          |                  |         |                    |            | Results       |                                 |       |              |               |          |        |       |       |      |
|      |                            | Status                                    | Rule I   | lame             | Con     | ditions            |            | Command Set   | s                               |       | Shell Profil | es            |          |        | Hits  | Actio | ons  |
|      | a                          | Search                                    |          |                  |         |                    |            |               |                                 |       |              |               |          |        |       |       |      |
|      |                            |   |          |                  |         |                    |            | +             |                                 |       |              |               |          |        |       |       |      |
|      |                            | 0   | Default  | 1                |         |                    |            | DenyAllComm   | ands                            | 1 +   | Deny All S   | Shell Profile |          |        |       | ŝ     |      |

Sectie Vergunningsbeleid

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

| $\sim$ Authorization Policy (1) |  |                 |                        |       |      |         |
|---------------------------------|--|-----------------|------------------------|-------|------|---------|
|                                 |  | Results         |                        |       |      |         |
| 🕂 Status Rule Name              | Conditions   | Command Sets    | Shell Profiles         |       | Hits | Actions |
| Q Search                        |  |                 |                        |       |      |         |
| NEXUS HELP DESK                 | Retwork Access-Device IP<br>Address EQUALS A.B.C.D |                 | Nexus Helpdesk         | ∞ ~+  |      | ĝ       |
| 🥪 Default                       |  | DenyAllCommands | Deny All Shell Profile |       |      | ŝ       |
|                                 |  |                 |                        |       |      |         |
|                                 |  |                 |                        | Peret |      | Sava    |
|                                 |  |                 |                        | Reset |      | Save    |

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 Responsesectie, waar u kunt zien hoe ISE de waarde shell:rollen="helpdesk" heeft teruggegeven

| Paspansa | {Author-Reply-Status=PassRepl;     |
|----------|------------------------------------|
| Response | 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 from command interpreter
 exit
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)# ?
            Negate a command or set its defaults
 no
            Show running system information
 show
 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)

| No.      |   | Time  |   | Sc  De                  | Protocol                          |           | Length    | Info | ifo                      |  |
|----------|---|---|---|-------------------------|-----------------------------------|-----------|-----------|------|--------------------------|--|
|          | 66  | 22:25:08.   | 757401  |                         | TACACS+                           |           | 107       | R: . | : Authorization          |  |
|          |   |   |   |                         |                                   |           |           |      |                          |  |
|          |   |   |   |                         |                                   |           |           |      |                          |  |
| <b>`</b> | Transmi<br>TACACS+  | ssion Cont  | trol Proto  | col,                    | Src Port: 4                       | 9, Dst Po | ort: 5886 | 3, S | Seq: 1, Ack: 90, Len: 41 |  |
|          | Major<br>Minor<br>Type:<br>Seque<br>> Flags<br>Sessi<br>Packe<br>Encry<br>V Decry<br>Au<br>Se<br>Da<br>Ar<br>Ar | version:<br>Authoriz<br>ence numbe<br>: 0x00 (E<br>on ID: 11<br>tot length:<br>/pted Repl<br>/pted Repl | TACACS+<br>0<br>ation (2)<br>r: 2<br>incrypted p<br>36115821<br>29<br>y<br>y<br>: PASS_REP<br>length: 0<br>: 0<br>l<br>th: 22<br>e: shell:r | ayloa<br>L (Øx<br>oles= | nd, Multiplo<br>02)<br>"helpdesk" | e Connect | ions)     |      |                          |  |

TACACS-autorisatiepakket

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

#### CACS+

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

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.